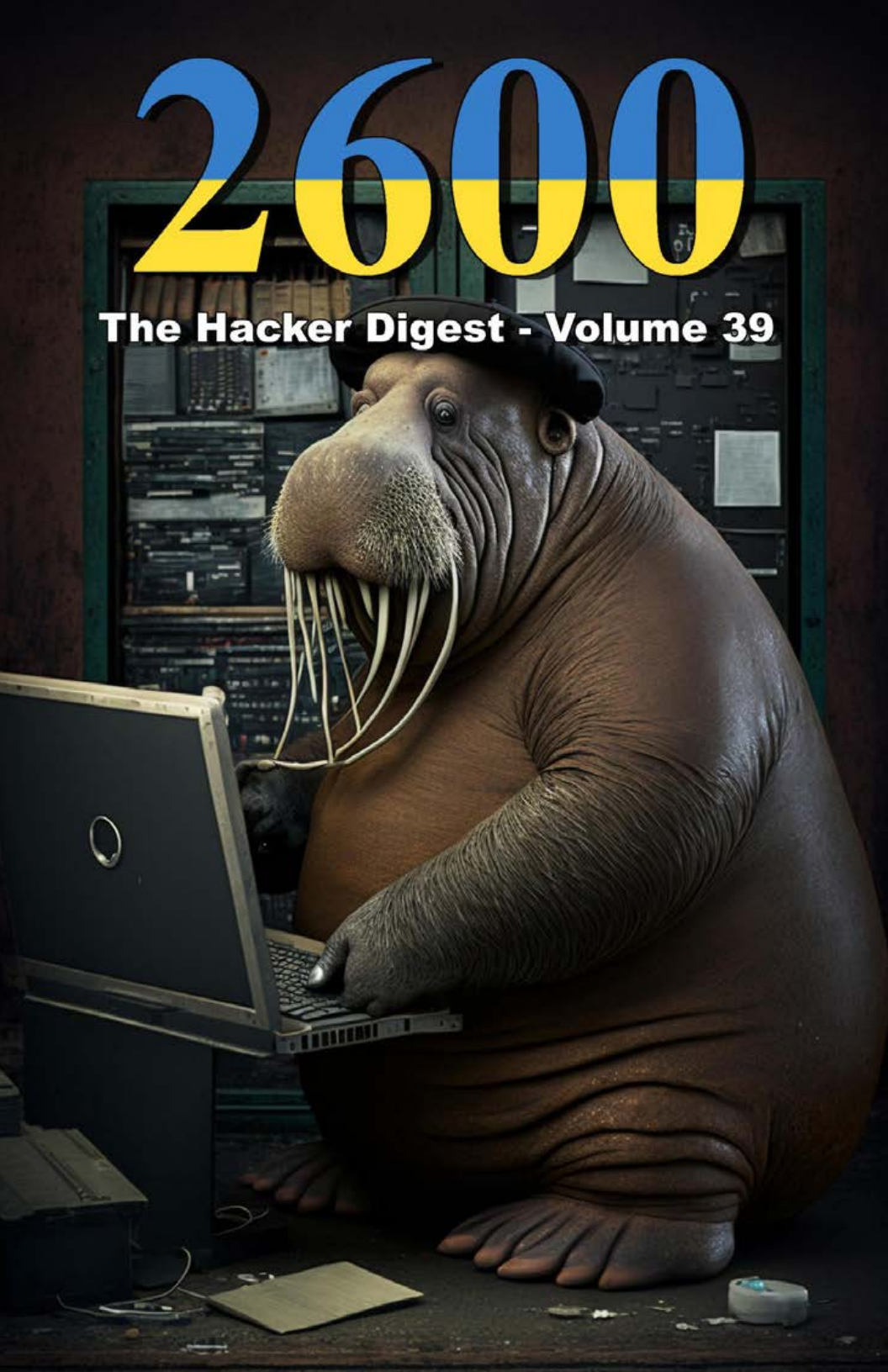
2600

The Hacker Digest - Volume 39




2 КОП.
3 2 1
4
5
6
7 8 9 0
справедливість

craiyon

AI model drawing images from any prompt!

S C O U T S

DRAW


VOTE
HERE
KHRESHCHATYK


FOXCONN
富士康科技集团
GFHG
SDGM
سیاهی لشگر نیاید به کار
یکی دُختِ جَنگی به از صَد هِزار

2022 Covers

Spring: This became one of our most popular covers ever and was the inspiration for printing cover artwork onto t-shirts.

The concept is rather simple. Ukraine had just been invaded by Russia. So we found a photo of a Soviet-era payphone in Kyiv and applied some gold and blue paint to the background - the colors of the Ukrainian flag. In the middle of the dial we added a peace symbol. If you look carefully on the body of the phone, you'll see the word справедливість - the Ukrainian word for justice.

The strength of that old telephone - and of the very concept of communications - is what stood out here. Defiance in the face of injustice was the message. And it resonated.

Summer: Artificial intelligence was beginning to get attention in the mainstream, particularly with regards to creating sometimes bizarre looking images based on descriptions. So we had a bit of fun making pictures of Supreme Court justices, who were also in the news due to the overturning of Roe vs. Wade and other controversial decisions. We used a company called Craiyon to generate the pictures. These are the descriptions we used for each justice:

- **Amy Coney Barrett** with American flag and a hand gun.
- **Brett Kavanaugh** with a beer bottle.
- **Samuel Alito** in a dry cleaner in front of coat hangers.
- **Neil Gorsuch** with a ventriloquist dummy.
- **Ketanji Brown Jackson** and **Stephen Breyer** in a swimming pool. (Jackson was in the process of replacing Breyer.)
- **Elena Kagan** on *Wheel of Fortune*.
- Neon **Clarence Thomas** with a sofa.
- **Sonia Sotomayor** in a gym on a treadmill.
- **John Roberts** at a pig farm.

And for the really sharp-eyed, we had a reference to the popular word game known as Wordle in the description bar. In Wordle style, the word SCOUTS indicated that all of the green letters were in the right place. U and T being yellow meant that they were part of the word but in the wrong place. Switching their positions would spell SCOTUS - Supreme Court of the United States.

Autumn: This was our Monty Python style cover which captured a whole lot of imagery. The giant foot coming down and the Capitol dome swinging open are pure Terry Gilliam nods. We added an ankle bracelet to the foot, along with a Jack in the Box logo to match the jack-in-the-box handle on the side of the dome. We also moved Big Ben, the Taj Mahal, and Mt. Fuji into the background and captured a bit of Abbey Road at the bottom. (On the back cover of that famous Beatles album, you see a woman in a blue dress passing by the street sign. Here we have a masked woman in blue passing a similarly placed sign that says KHRESHCHATYK, the main street of Kyiv.) There are wind turbines in the background as the battle for renewable energy sources continued to be a global focal point. We also added a rainbow coming from or going to the Capitol and had a giant "VOTE HERE" banner pointing directly at the building as the midterm elections loomed.

Inside the Capitol is Mudge, famed hacker from the L0pht and former head of information security of Twitter who had just testified in front of Congress. Being a whistleblower, he's holding a giant whistle as 24 black Twitter birds fly away. This was an allusion to Black Twitter, as well as the line "four and twenty blackbirds baked in a pie" from the famous nursery rhyme "Sing a Song of Sixpence."

A gull door Model X Tesla is in flames on the front lawn (a reference to Elon Musk's takeover of Twitter as well as some problems with self-driving cars) as a herd of elephants with Remembrance Day poppies approaches. The just-departed Queen of England is riding atop the lead elephant and away from a Buckingham Palace statue.

Winter: Our "Foxconn cover" shows a Chinese factory making iPhones while demonstrators of all sorts gather towards the front of the room. Everyone is wearing masks. The background is very stark with mostly black and white imagery while the people in the front have more color, albeit subdued. One exception to this is the bright red balaclava worn by one of the protesters to honor a departed friend of ours known to some as Jeopardy Jim and others as Red Balaclava. The latter name came about as a result of a disguise he wore while giving one of the first ever HOPE talks back in 1994 on New York City's newly released Metrocards and, appropriately, he's holding one up.

The other people in this gathering are holding different signs, including:

- **The Moroccan flag** - Morocco had just gotten further in this year's World Cup than any African team had ever been.
- **The "One Love" armband** - a symbolic gesture planned by football players at the World Cup to support the LGBTQ+ community and speak out against hatred. However, the armbands were banned by the tournament's governing body.
- **GFHG, SDGM** - initials of the romanization of the eight Chinese characters in a banned slogan that meant "Liberate Hong Kong, the revolution of our times."
- **A single sheet of white paper** - known as the "white paper protests" in China where people held these up as metaphors of news articles, social media posts, and online accounts that had been erased from the Internet for speaking forbidden words.
- **The ohm symbol repeated** - another way of showing resistance in a very literal sense.
- **A Persian protest slogan** - which meant "This massive army is useless. Indeed, a single fighting girl is worth hundreds of thousands of them." Massive protests were beginning against the Iranian regime and its policies.
- **MMIW** - for the Missing and Murdered Indigenous Women movement of North America seeking to call attention to this underreported crisis. The red hand print (color subdued here) has become a very powerful symbol.
- **Winnie the Pooh** - the symbol that's *really* banned in China since people for some reason started comparing Xi Jinping to Pooh Bear. Some leaders have *no* sense of humor.

Missiles, Operations, Explanations, Interpretations

Renewed Hope

The last couple of years have been hell for many of us. But we're cautiously optimistic that we're seeing the end of it, or at least that we've moved past the worst part.

This summer, for the first time in four years, we're having an in-person HOPE conference. That may not sound like a big deal, but for so many of us, it really is - and for so many reasons.

Let's not forget how fractured and divisive our nation has become, and how we started to see this within our own community in 2018 - and how woefully unprepared we were for that. Since then, we've spent a great deal of time improving how we respond to potential issues and in recognizing those issues in the first place. Running a conference is a series of very draining tasks, and it's essential to allocate resources in the right areas. The support we've received has been phenomenal and we've had four years to develop a terrific team. While our 2020 virtual conference was a true highlight of global coordination and a model of inclusiveness, we're really looking forward to doing all of this again in person.

We had already made the decision to leave our old home at Hotel Pennsylvania before being forced to go virtual in 2020. Greed appeared to be the predominant business model at Vornado (the hotel's parent company) when they tripled the rate for us to have a conference, which would have made it impossible for many of our loyal attendees to be there. This, after we had helped the hotel get much better Internet service and also save it from demolition the previous decade. In the end, Vornado's greed came right back at the hotel itself, as they doomed it to destruction, resulting in the loss of nearly 2000 affordable hotel rooms. It will be replaced by a luxury office tower that will benefit relatively few. It's a real tragedy, but we had many good years there - and we all did everything we could to keep it going. It's time to build new traditions and memories.

So three massive milestones are coming together at the same time: our first get-together after our nation went a little nuts with divisiveness, the first gathering since COVID-19 hit us all, and our debut in a brand new home: St. John's University in the New York City borough of Queens. It's a lot to take in. And we know it won't necessarily be smooth as we adjust to so many new ways of doing things. Those of you who were at our very first conference in 1994 can attest to this, as chaos reigned while we grappled with an overwhelmed registration system in our opening minutes. We got through it then - and we'll get through whatever lies ahead - because of the support, expertise, and patience of our amazing attendees. In this community - which goes well beyond HOPE and *2600* - there's nothing that can't be accomplished with our ingenuity and positive outlook.

While HOPE's new home is capable of much larger crowds than the hotel could accommodate, we intend to ease into things gradually so that it's not too overwhelming and so that we develop quality over quantity. If you're amongst the first attendees to this new chapter, you will be a part of history, and you'll help play a big part in HOPE's evolution.

***

As is often the case, new chapters can go in all sorts of different directions. And as we started to take the first steps towards a post-COVID world, along with the recovery came the terror of war in Europe. For the first time since the conflicts of the former Yugoslavia in the 1990s, but on a scale that was closer to the pace of the 1940s, bombs and missiles were dropped on innocent people. A massive refugee crisis was created within days, as millions of Ukrainians fled the brutal Russian onslaught. In very short order, the whole of Europe was on edge, with fears of a much wider conflict developing. Even here in the States, there has been great concern over what Vladimir Putin might do next, as he genuinely appeared to be somewhat unhinged and paranoid, perhaps as a result

of isolation due to the COVID threat.

What has happened since that fateful day in late February when the long-feared Russian invasion began is both horrifying and inspirational. While we can examine and debate how we got to this stage in the first place, what is happening in the present is about as conclusive as it gets. A sovereign nation was invaded by a neighboring superpower simply because they were getting too independent. Civilians have been targeted from the beginning. Clear evidence of mass graves, torture, and executions by Russian forces has been uncovered from multiple sources. Yet throughout all of this, the Ukrainians - both military and civilians - have refused to yield and, at the time of this writing, have succeeded in driving the Russians back, inflicting losses that were unimagined when this all began. Russian soldiers, many of whom were woefully unprepared for this war, were sent in without adequate supplies or knowledge of what they were actually doing.

Numbers and power don't always add up to victory, especially if the other side is determined, thinks outside the box, and believes strongly in their cause. This is a lesson we must never forget.

Of course, in this age of social media, facts can be thrown away simply by labeling them as fake. We've been down this road before with everything from election results to science, but this is much worse. An overtly repressive regime is successfully shutting down all opposing voices in the media, ensuring that only its version of the facts gets out. It's at the stage where even when *victims* of the atrocities in Ukraine try to tell their own relatives in Russia what's going on, they're not believed because of the programming done by mass media, reinforced by social media.

This is where the hacker mentality comes in. While risky, it's essential that the false narrative be challenged and upended. By pooling our resources, possessing an understanding of the technology, and utilizing some clever thinking, it will indeed be possible to get the truth out. Of course, as we've learned in the past few years, that isn't always enough. But it's something.

While tempting, denial of service attacks can easily wind up hurting the wrong people. A programmer recently added some code to a JavaScript library that shared a message of peace - unless the computer accessing it had an IP in Russia or Belarus, in which case all of their files got deleted. While this would have been harmful to a government official, it also would have hurt an anti-war activist in that country just as badly. Clearly, this isn't the way to help.

People affiliated with Anonymous were able to hack a state television channel in Russia and get an anti-war message out to the viewers. Banned newscasts and footage from global media sources are routinely smuggled in with the help of VPNs. The Tor browser was designed for this sort of thing and there are many people in Russia for whom the Internet restrictions are easily bypassed. But again, we're dealing with a repressive regime here and they could go as far as trying to punish people who simply *connect* to one of these services without even knowing what they ultimately use them for.

Just as we need to remember that those who disagree with us in our country are not necessarily the enemy, we must do the same in this situation. People reach conclusions based on evidence and, if they are being given faulty data, that is where the real problem lies. Our evidence has to be better and the lines of communication must stay open.

We have to continue to examine all facts presented to us with a critical eye and call bullshit when we see it, regardless of the source. Those who conjure up massive conspiracies as their default defense or who fixate on disagreeing with the right people rather than analyze what they're disagreeing about have distanced themselves from the truth. When focusing on actual evidence, you may find yourself aligned with people you're not thrilled about being on the same side with. There's simply no avoiding that and it should never affect how you process the evidence you examine. We find that too often, it does.

These are extremely challenging times. But it's precisely these times where the ability to weigh and interpret facts while figuring out ways to get around restrictions and censorship is an invaluable skill to have. If we share what we know, figure out new ways of doing things, and keep communication channels open, we have the potential to do a lot of good in this, and any, fight for freedom.

How to Create a Practical Burner Phone for the Average User

by gh057

Introduction

On January 31, 2022, the Internet Crime Complaint Center (IC3) released a Private Industry Notification (PIN) warning athletes and attendees of the 2022 Olympic Games in Beijing to "keep their personal cell phones at home and use a temporary phone while at the Games" (www.➥ic3.gov/Media/News/2022/220131.➥pdf)[1]. In essence, the IC3 is encouraging the use of what is commonly known as a burner phone. This is solid advice for anyone who is entering an untrusted environment or who requires personal privacy above and beyond basic common sense rules. However, how does one go about creating such a device?

When you hear the term "burner phone," what do you think of? Possibly some informant in a crime drama television episode phoning in a tip from the edge of the Hudson River and then throwing the phone in a nearby trash can? Burner phones are often depicted as a tool for those looking to evade law enforcement or to snitch on organized crime. However, they have many practical purposes for the average user and are legal to create and maintain. In this article, I will walk you through the steps to create and maintain a burner phone for when you need (or want) an extra layer of protection and privacy.

A Quick Disclaimer

I am in no way endorsing, encouraging, or supporting illegal activity or behavior. None of the tips and techniques that I am outlining in this article will be a major challenge for law enforcement to overcome and should not be viewed as such. The intended purpose of this article is to give the average user knowledge needed to safely and effectively create a temporary mobile device, commonly referred to as a burner phone, for those times when they might be entering an untrusted environment or require personal privacy above and beyond basic common sense rules. Use of any knowledge gained from this article is at your own risk and discretion.

So... Why Do I Need This?

The devices that we carry with us contain so much more than just a bunch of phone numbers. Unlike the phones from 30 years ago, our modern mobile devices contain our financial information, health information, contacts, likes and dislikes, and so much more; a virtual treasure trove of information which attracts both the good and the bad. When you join a social media site, a public WiFi network, or share your information at a conference, do you really know what happens with that information? Do you really know where that information is stored and who it is ultimately shared with? The reality of our modern lives is that the only person that we can trust to truly protect our data is ourselves. Protecting our data does not just mean not posting it on social media sites. It also includes protecting data that is sent along with any websites that we visit or any services that we use. Having a burner phone enables you to put one level of separation between yourself and those you don't yet fully trust by utilizing a device that is not registered to you with accounts that are not attributable to you. Remember the old adage: "trust but verify."

So how does this help in an environment like Beijing? With a burner phone, the assumption is that the phone will eventually become compromised, so you should keep your personal information off the burner phone and use temporary email addresses and social media accounts which, if compromised, will not impact you negatively; you can simply throw those accounts away and create new ones. Remember, it's called a burner phone because you can use it and then you can lose it.

Step 0: Wait, Do I Even Need a Burner Phone? Can't I Just Use an App with My Current Phone??

- *Pros:* Apps can be easily downloaded and you don't need additional hardware to use them.
- *Cons:* Apps installed on your personal mobile device have the same International Mobile Equipment Identifier (IMEI) and can be very quickly traced back to you or used to track you.

The easiest solution, of course, is to use an app (like Burner or Hushed) with the phone that you currently already have. Depending upon your needs, this may be sufficient. If you're simply looking to create a solution so that you can maintain some level of anonymity when buying and selling through local online markets or when dating via social networks, this may be all that you need. However, when it comes to untrusted environments like the Olympic Games in Beijing, this would be the worst choice. The device itself is still your personal device with your personal apps and personal usage history on it. Should

something happen to that device, it is, as they say, "game over."

Step 1: Get the Phone

The very first step in creating a burner phone is getting the actual phone! There are many places where you can obtain these devices and I outline some of them below with pros and cons.

An Old Phone You Currently Own

- *Pros:* It's free, it's immediately available, and you can start creating right away.
- *Cons:* Depending upon where you got it, the IMEI may be tied to you personally, which means there's still a chance that the phone can be traced back to you or track you.

Much like the app solution above, if you have an extra phone lying around, this is a pretty easy solution if it fits your needs. However, when it comes to untrusted environments like the Olympic Games in Beijing, this would not be the best choice. Depending where you got the phone (i.e., were you the original purchaser and was the phone purchased new), the IMEI number can still be traced back to you and if you are easily searchable online, you can still be targeted. In addition to that, many services capture the IMEI number of devices to ensure uniqueness, meaning that even if you use the same device with two different accounts for a particular service, associations can be made. The whole idea of the burner phone is to subvert electronic identification.

Purchased New/Used From a Retailer

- *Pros:* It's new so you know that it will function the way that you expect and it has a return policy if you're not happy.
- *Cons:* It's not the cheapest route to go. There is a purchase history linking you to that device.

If you can justify the cost and you don't care that the purchase history of the device can be linked back to you, then this is a solid way to go. You get the luxury of knowing that you bought a new device, one with an expected state of quality and functionality without having to risk your safety (discussed next). Phones purchased this way are typically more expensive then the next option since quality and functionality assurances can be made. However, even if you pay cash, there is a purchase history linking you to this device, whether it's a receipt of the purchase or surveillance video of you entering the retailer at the time of purchase. If that is a concern, then this may not be the best option. Remember, outside of the purchase history, unless you associate the IMEI of this device with a preexisting mobile account, this device is not associated with you. Make sure to follow the steps about purchasing a Subscriber Identifier Module (SIM) card below to keep it that way.

Local Online Marketplace (i.e., Craigslist)

- *Pros:* The device IMEI will not be linked to you, there is no purchase history if you pay with cash, and, if you use a burner phone app and/or burner email address for communications with the seller, there is little traceable sales history of the transaction.
- *Cons:* In recent years, Craigslist and other local online marketplaces have seen their fair share of crime associated with meeting a stranger in public. In addition, you don't know what was done with the phone prior to buying it.

The next better solution (and one that I have employed regularly) is to buy a device, only with cash, by way of a local online marketplace like Craigslist. The device IMEI will not be associated with you or anyone you know, unless you have the awkward misfortune of finding out that the seller is actually someone you know. However, you don't know what was done with the device prior to you getting it, meaning, you don't know if the seller is lying to you about its condition, its repair history, if it was stolen, or even if it's truly unlocked. This said, in all my experiences of buying and selling online, I can count on one hand the number of times that I've bought a lemon from someone and it's never been with a mobile device.

A note to mention here is that these local online marketplaces have seen their fair share of crime associated with the transactions occurring from petty theft (i.e., "snatch and grab") to physical assaults. When meeting a complete stranger in public, you should always follow best practices for personal safety, no matter how nice the person seems to be.

Wait, What About the Device Itself?
What Platform Should I Choose??

This is largely a matter of personal preference. In general, the rule of thumb is that if you want to make heavy modifications to the platform, then Android is the way to go. However, if you want something that will generally have a fairly secure operating system out of the box and requires little modification, then iOS may be your best bet. In either case, the steps below, unless otherwise specified, will work for either platform.

Android Alternatives -
A Quick Plug for CalyxOS

Google Android is an open source platform. Anyone can download it, make modifications, and create something new, possibly something

with a greater emphasis on security and privacy. This was the goal of the team who built CalyxOS. If you like Android but would like something a bit more privacy focused, then I recommend CalyxOS. The platform is very stable and the flashing process is virtually painless. If you want to know more, visit the Calyx website (calyxos.org/).

There are many alternatives to the standard Google Android platform out there, including Ubuntu Touch (ubuntu-touch.io/) and GrapheneOS (grapheneos.org/), which I've heard that a lot of folks like (you can find some of these alternatives listed here: alternativeto.➥net/software/calyxos/). I haven't experimented with many of these, but I encourage you all to try them out if you're curious. For the average user who prefers an easier setup process with sizable gains, CalyxOS is a great alternative to the standard Android platform.

Step 2: Obtain a SIM Card

There are a few key steps that are legitimately required in order to ensure that protection and privacy are maintained. I outline them below. The overall goal is to minimize how much association, if any, can be made between you and the purchase of the SIM card.

SIM Card Type Depends on the Phone... and Your Needs

There are two prevailing radio technologies: Code-Division Multiple Access (CDMA) and Global System for Mobile communications (GSM). Most phones these days, especially outside of the U.S., use GSM. However, some U.S. carriers, like Verizon, also support CDMA. The SIM card that you buy will have to be compatible with the technology that the phone requires. In addition, there is a difference between SIM cards intended for 4G phones and those that are intended for 5G phones. Make absolutely sure that the SIM card you buy is properly matched to the phone you are planning on using.

Pre-Pay is the Way

Regardless of what the sales person tells you about the option being "more expensive" or "a pain to maintain," this is what you want to do. For most burner phones, you only need their use for a short time, so having a prepaid solution makes sense. These solutions allow you to add more funds to them should you need to, or you can simply let that SIM card expire and buy a new one.

How Much Data? How Much Talk Time?

Remember what the intent of this device is. This is an emergency "use when needed" phone. In other words, you shouldn't need to match your current personal usage with this phone. However, there's nothing stopping you if you wish to do that; you're just going to pay a lot more for it. Typically, a few hundred minutes of talk time and a gigabyte or so of data is plenty for a relatively short-term need and, of course as mentioned above, you can always add more funds to the prepay solution as needed.

Pay in Cash

This one is fairly straightforward and it should be noted that the same technique will be interwoven throughout this article multiple times. If you pay for a SIM card in cash, then there is not an association between you, your credit card, and the purchase of the SIM card. Typically, I go into a mobile provider with about $100 in hand to make this purchase, but it ends up being around $40. The reason for the overage is that you don't want to be caught off-guard by a difference in the price and not have a cash-based means to cover it.

No, You *Do Not* Have to Give Your Name

This is one where not everyone is going to feel comfortable having this conversation. Keep in mind that it's in the salesperson's best interest, and by association the retailer's best interest, to ask for your name, birth date, or other personally identifiable information. This way they can sell you more stuff. However, there is no law that requires you to give your name, your contact information, or even show a government-issued ID. Regardless of how much they may push, you do not have to give this information. If they are truly adamant, just find another retailer who will sell you what you need; it's not worth the argument. Also, getting loud and combative draws attention to you and, if you haven't noticed, this entire article is focused on doing just the opposite. I've been everyone from "Mark Jones" to "Jesus Christy" (yes, really) just to give them a name when they wouldn't give up. Please note I've been told that the TracFones require personally identifiable information to be activated. For this reason, I typically only use the big four (Verizon, Sprint, T-Mobile, and AT&T) because they've been consistent in the past.

Definitely Make Sure the Card Works *Before* Leaving the Retailer

Using the above process, this creates an "all sales are final" situation. So to avoid burning through good cash, it's best to make sure that everything works before you leave the retailer. Simply plugging in the SIM card and checking connectivity is all you really have to do. There may be a few hours delay with the phone actually being able to make calls due to setup within the system (the salesperson should inform you of this), but the phone itself should immediately connect to the provider.

Step 3: Add Funds to the App Store

Let's face it, there are some apps that we all rely on for stability and security, and many of those are not free. The easiest way to purchase these apps is through the platform's app store, however, that requires a credit card or pre-purchased funds. It's the latter option that we are going to employ here. Simply go down to your local pharmacy, grocery store, or big box retailer and purchase a gift card (again with cash) for that platform app store. Typically, I default to $50 just to cover my needs and any services those apps may require, but this is a personal preference.

Step 4: Create New Account Exclusive For This Phone

The final step is to create new accounts for all of the services that you want to use, and this is the key: zero association to you. This means a new platform account (i.e., Google or Apple), new email addresses, new social media accounts, etc. Make sure to turn on two-factor authentication because while we hope that this device is not compromised, we should operate with the assumption that it is or soon will be. Do not allow anyone who you know in your personal or professional life to contact you on this device with their personal or professional accounts. The only accounts that should interface with you on this device should be other "burner only" accounts.

Wrap-Up/Best Practices

Congratulations! If you reached this point, then there's a high likelihood that you successfully created a customized burner phone for your privacy and security needs. However, the journey is not over. There are some basic best practices to keep in mind when using and maintaining your new burner phone so that you maintain as much of a separation between you and that device as possible.

Never Use Personal Accounts With a Burner Phone

As mentioned above, personal accounts are, well, personal (hence the name). These accounts should stay far away from the burner phone in any capacity. In other words, don't use personal accounts on the burner phone, link burner accounts to personal accounts on social media, or converse with individuals that you know in your personal life from your burner account to their personal account. Be vigilant; we're only human and mistakes happen, but those mistakes are sometimes costly.

Never Connect the Device to Your Home or Work Wireless Network

If there's simply one thing to not do, this would be it. The process of creating a burner phone takes time, effort, and funds. The hope is that when you're done, you have a tool which you can rely on reasonably well for privacy and security. However, if you go ahead and ruin that by associating it with your home or work wireless network, then your efforts will be all for naught. If you need to update it and you require a wireless network, any good coffeehouse or community center should work just fine. Additionally, if the device was just in an untrusted environment, the last thing that you want is for it to auto-connect to your home or work wireless network.

Do Not Have Both Your Personal Phone and Your Burner Phone On at the Same Time

This issue would be more of a concern for those who are going to a place where the potential hostility may be local or national law enforcement, but is generally a practice that I employ whenever I go to an untrusted environment. If you don't trust the environment enough to use your personal device, then you shouldn't trust your personal device to be on in said environment. Instead, power down your phone and store it safely in a faraday bag. Additionally, burner phones can be associated with you if both the burner phone and your personal phone are pinging the same cell towers at the same time. The covert nature of the burner phone is significantly reduced if the owner of said burner phone can be reasonably identified.

After Returning Home, Wipe the Phone

Once you return to a secure environment like your home or place of work, it's time to wipe the phone. Yep, factory wipe that sucker! Assuming that you didn't use the phone to store any sort of files like photos, videos, audio recordings, etc., your loss will be negligible. All you will have to do is set up the phone again with the same accounts you already have access to. If you did take photos, videos, or generate other types of documentation that you wish to keep, you will have to go through additional measures to ensure that those files are extracted in a safe manner, which is beyond the scope of this article.

In Closing...

I hope that this article was helpful for you. Burner phones are a common tool that I employ to keep myself, my data, and my privacy as intact as possible when I am knowingly entering an untrusted environment. While they may have gotten a bit of a seedy reputation from television and movies, they are an effective way of reducing your risk and I highly encourage their use.

[1] Federal Bureau of Investigation. (2022). "Private Industry Notification: Potential for Malicious Cyber Activities to Disrupt the 2022 Beijing Winter Olympics and Paralympics" (20220131-001). Federal Bureau of Investigation. www.ic3.gov/➥Media/News/2022/220131.pdf

Exploring the BACnet Protocol for Fun and Profit

by Teguna
teguna@protonmail.com

I have one of the greatest jobs in the world working in the field of Operational Technology or "OT." I define OT as the place where computers meet the physical world, including devices that control and monitor large infrastructures like power grids, water systems, dams, manufacturing plants, and energy pipelines. OT also includes things as mundane as the computer system in your car, your home alarm system, or thermostats that can be controlled from your phone. My OT world depends heavily on appliances like historians, SCADA servers, Industrial Control Systems (ICS), Human Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs).

OT professionals depend on a set of communication protocols that are reliable and easy to use, but severely lacking in security features. Protocols like Modbus, DNP3, and Ethernet/IP were developed before security was vogue and they focused exclusively on availability without any concern for integrity or confidentiality. Lately I've taken a keen interest in a protocol called BACnet. BACnet stands for "Building Automation and Control Network" and is the communications protocol ubiquitous with Building Automations Systems or "BAS." If you work in a modern office or industrial building that has HVAC, lighting control, access control, or fire detection systems, then those systems are probably monitored and controlled using a BAS.

Before you blow off the importance of these systems to the overall security picture, please keep in mind that the 2013 Target hack that exposed 40 million debit and credit card accounts started by hacking the store's HVAC system. Attacks on IT enabled by attacks on OT have become much more popular in recent years because of security flaws that are very common in OT equipment. Most of us in the OT industry realize we can be the "soft underbelly" of network security. Expect attacks on OT to become much more common as the demand increases for smart refrigerators, network connected litter boxes, and even Bluetooth and WiFi connected clitoral stimulators. But I digress....

As with other OT protocols, there are plenty of free or open-source tools that can assist us with exploring BACnet/IP communications to understand how BAS communication works and its inherent security problems. BACnet/IP is BACnet communications over IP networks, which is different than BACnet MS/TP that typically uses the RS485 standard for communications. This article will be an overview of two free tools for exploring BACnet/IP and a discussion of the BACnet protocol itself. This is probably an excellent time to advise you that this article has been written for educational purposes only. To use any of the techniques in this article constitutes a thought-crime at a minimum and international terrorism in the most extreme cases. The contents of this article should never be used by anyone... anywhere... ever.

The first thing we are going to need to explore BACnet is a BACnet device. This can be accomplished free of charge by visiting Contemporary Controls, creating an account, and downloading their BASemulator. It is available at the following site: `www.ccontrols.com/basautomation/bastools.php`

You'll be downloading the entire BAScontrol toolset, which also includes Sedona Application Editor (SAE) for programming Contemporary Controls devices. You can choose only to install the BASemulator when you run the install program. The software must be installed on a Windows machine. For this project, I recommend a VM running Windows 10 and using an "internal only" network.

After you finish the installation, find the BASemulator icon on the desktop or in the START menu and load the program. Select the "Start Emulator" button to begin the emulation (the default settings are normally fine). This will also bring up a web page in your browser. The default credentials are "admin / admin." What you have just installed is a complete emulation of a BAScontrol22 hardware appliance sold by Contemporary Controls. Normally a technician would use the BAScontrol22 for control and monitoring of an HVAC or other building automation system. For our purposes, we have a free software device that emulates BACnet/IP in the same manner as its hardware counterpart. If you wanted to set up a BACnet hacking lab, you could certainly set up armies of these emulators.

There are a few things we need to do for the purpose of demonstrations later in this article. In the emulator web interface, select the "System Config" button on the bottom left. At the top of the "System Configuration" page that pops up, change the "Device Object Name" to "Thermostat" and hit the "Submit" button at the bottom right of the page. After returning to the main page, select "Restart Controller" on the bottom right side (nothing will appear to happen, but the controller will reset). Select the "Virtual Points" button in the bottom middle of the page. Double-click "Virtual Point 1" and bring up the Object Configuration page. In the

middle of the page, change the "Object Name" to "RoomTempSetting" and select "Submit" at the bottom of the page. Close the window. Lastly, select the check box under our newly named "RoomTempSetting" on the Virtual Points page. This will allow you to change the value of "0.000" to "72.000". After you have changed the value, uncheck the box and close the window.

A few fun facts about BACnet/IP that you will need to know as you play with this protocol:

- BACnet/IP devices use UDP for communication and BACnet/IP is served on port 47808. 47808 converts to hexadecimal BAC0. Clever and easy to remember, eh?
- BACnet devices are always organized as a series of objects with each object having a set of properties. The device itself is an object (with an object-type of "device") with properties like an instance number and vender identification. Object types like "analogInput", "analogOutput", "binaryInput", and "binaryOutput" are very common in BACnet devices. Expect to find many different properties for each of these objects to include present-value, units, and description.
- You will interact with objects using services supported by the BACnet appliance. The "ReadProperty" service is a mandatory service in all BACnet appliances, but "WriteProperty" is supported across most devices. The WriteProperty service will offer us the most fun as a BACnet researcher.
- When we are "on the wire" with BACnet/IP packets, binaryInput and analogInput object types are read Only. binaryOutput, analogOut, binaryValue, and analogValue object types are both read and write, meaning we can use the "WriteProperty" service and change their values remotely.
- BACnet/IP makes extensive use of Broadcasts for network communications. And yes, it is entirely plausible to conduct a Smurf attack to DOS devices using BACnet/IP protocol.
- A key advantage for an attacker is that BACnet devices are blabbermouths. They just want to tell you everything about themselves to include all the objects and services they support. I'll demonstrate this in the paragraphs that follow.

Let's spin up a Linux machine with Nmap installed (Kali Linux would do just fine) and ensure that it is on the same subnet as our BASemulator machine. Type the following command:

```
$ sudo nmap -sU â€"script bacnet-
➥info -p 47808 192.168.56.0/24
```

Set the subnet to whatever you're using in your lab or just direct the scan at the IP address of the emulator. In my case, I used the VirtualBox default internal network for my devices. Your scan should come back with something like this:

```
Nmap scan report for
➥192.168.56.103
Host is up (0.00035s latency).

PORT      STATE SERVICE
47808/udp open  bacnet
| bacnet-info:
|   Vendor ID: Contemporary
➥Control Systems Inc. (245)
|   Vendor Name: Contemporary
➥Control Systems, Inc.
|   Object-identifier: 2749
|   Firmware: 3.1.28
|   Application Software: 1.2.28
|   Object Name: Thermostat
|   Model Name: BAScontrol
|_  Description:
MAC Address: 08:00:27:D7:C0:D7
➥(Oracle VirtualBox virtual NIC)
```

That is a ton of valuable information from a research perspective, which is why I enjoy this Nmap script quite a bit. Did you notice that the property of "Object Name" above for the device now has the name "Thermostat" like we assigned earlier? You should especially take note of the Object-identifier and the IP address. We are going to use both of those to learn even more information after we install BACpypes on our Linux machine.

BACpypes is a BACnet module for Python. I always keep it in my arsenal because it's freeware and can support anything I want to do in BACnet/IP. Use the following link for simple instructions to install and configure BACpypes. Download the git repository to your home directory in Linux for the rest of the examples in this article:

```
bacpypes.readthedocs.io/en/latest
➥/gettingstarted/gettingstarted
➥001.html
```

Configuring your BACpypes.ini correctly is particularly important, so pay attention to that area of the tutorial. Our network does not have a BBMD so don't sweat it. The ~/bacpypes/samples directory is chock full of useful tools for information gathering on BACnet devices and manipulating BACnet devices. I think you should explore all of them, but let's cover just a couple.

From your ~/bacpypes directory, type the following command, replacing the IP address with the one you discovered in your earlier Nmap scan:

```
$ python3 samples/ReadObjectList.
```

```
➥py 2749 192.168.56.103
```

The blabbermouth BACnet device is going to tell you everything. In this case, you are using the ReadObjectList program to get a list of all objects on device instance number 2749 at IP address 192.168.56.103 (both were passed to the program as parameters). The BASemulator has responded with a complete list of all object types, instance numbers, and object names presently on the device. In the list, you will see the "object Identifier" enclosed in parentheses. The object identifier is a combination of the object type and the instance number and we will need it later. Two stick out because we changed their object names when we set up our emulator:

```
('device', 2749): Thermostat
('analogValue', 201):
➥RoomTempSetting
```

Assume for a second that a similar device is servicing an HVAC system in a large office building. I would expect that the engineer programming the device is going to use descriptive object names in order to identify where the device is (for example, "HVAC Plant BLDG 1234") and what points it monitors ("RoomTempSetting", "ChillWaterTemp", or "OutdoorTemp"). This practice will allow technicians to better service the device during trouble calls. Object naming makes BACnet/IP a powerful tool for simplifying programming and maintenance, but it also makes reconnaissance against BACnet devices much easier than OT protocols like DNP3 and Modbus.

Let's read some values from the device using BACpypes's ReadWriteProperty program:

```
$ python3 samples/
➥ReadWriteProperty.py
```

The program will present you with a new prompt ">". Enter the following command:

```
> read 192.168.56.103
➥analogValue:201 presentValue
```

If you followed my instructions earlier, the program should have responded with "72.0" and given you another prompt. Let's pretend for a second that we are an attacker, and we want to turn up the temperature in the boss's office. Let's try:

```
> write 192.168.56.103
➥analogValue:201 presentValue
➥88.0
```

The system responds with "ack" and gives us another prompt. We were able to write to the point because analogValue is Read/Write and we can use the "WriteProperty" service to change its properties remotely. If you repeat our previous read command on the same point, you'll see that that "RoomTempSetting" presentValue has been increased to 88.0.

But what about digital? Let's choose a random binaryOutput object from our list and execute a read command:

```
> read 192.168.56.103
➥binaryOutput:18 presentValue
```

The system responds with "inactive" and gives us another prompt. Binary values, as you know, are either 1 or 0, true or false, high or low. In this device, inactive refers to false. In order to make this point "active" or true, we enter:

```
> write 192.168.56.103
➥binaryOutput:18 presentValue
➥active
```

The system will respond with "ack" and a new prompt. Repeating the read command from earlier will show that the presentValue property of the binaryOutput:18 object has switched to "active".

I have merely given you a taste of BACnet and I encourage you to explore BACnet more in your own lab. The BACpypes package has a variety of sample programs that are fun to play with and can be used to learn more about BACnet/IP. Be sure to use Wireshark and analyze the APDUs that are generated when BACnet devices communicate. Use the Sedona Application Editor (SAE) from Contemporary Control to program your BASemulator. Happy hacking!

Sources

1. Peter Chipkin. "Bacnet for Field Technicians." cdn.chipkin.com/assets/
➥uploads/2018/mar/15-19-09-42 _
➥Bacnet _ For _ Beginners2.pdf, 2018.

2. BACnet International. "Introduction to BACnet For Building Owners and Engineers.", www.ccontrols.com/pdf/
➥BACnetIntroduction.pdf, 2014.

3. Jaspreet Kaur, Jerneq Tonejc, Steffen Wendzel, and Michael Meier, "Security BACnet's Pitfalls." link.springer.com/content/pdf/10.1
➥007%2F978-3-319-18467-8 _ 41.pdf,
➥2015.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! All of a sudden, the world has dramatically changed and, as of this writing, we're suddenly back to a Cold War footing. For nearly all of my adult life, the world has been getting smaller. I have never thought twice about flying over Russia, or even through it (while I was living in Beijing, one of the best and cheapest ways to fly to Europe was via Moscow on Aeroflot). Now, quite suddenly, each option has become both impossible and almost unthinkable.

This leaves me wondering what the state of telecommunications will become. Many authoritarian countries allow open and unfettered access to telephony (while often also censoring the Internet). In fact, some such countries are even regional telecommunications hubs. They're definitely employing surveillance tactics, but these are also countries with the resources to acquire and use software (such as Palantir) to identify surveillance targets. Other countries, such as the Democratic People's Republic of Korea, sharply limit international telecommunications capacity. This is done both to limit interactions with people outside of the country and to ensure that every call can be monitored in real-time.

One of my favorite things to do in middle school during my lunch break when calling from the payphones (I was always calling something or somewhere from the payphones - often small, obscure airlines to ask for copies of their timetables to be sent) was to make international directory assistance calls. Back then, international calls were connected via satellite after analog microwave hop to the AT&T Roaring Creek Station satellite center in Pennsylvania. To call international directory assistance, you'd call an AT&T operator (by dialing "00") and request directory assistance in the given country. The operator would get you on the line with a directory assistance operator in the other country, drop off the line, and you could then do whatever.

Now, this could be a great way to blue box. You could seize a trunk in mainland China and call outbound from there to anywhere in the world, courtesy of China Telecom (of course, it was a double satellite hop and the quality was terrible, but it was possible). Although Israeli directory assistance was immune to blue boxing (they had effective countermeasures), the phone lines were apparently staffed by bored military conscripts. They were young, and they weren't strictly supervised. We would sometimes add them to a conference call full of hackers and phreaks and they'd just roll with it, telling us about their lives in Israel.

I liked calling Bulgaria directory assistance in Sofia. They put you on hold forever, so sometimes the AT&T operator would just drop off and leave you on hold with them. They'd play a recording in three languages (Bulgarian, Russian, and English) saying "Hold and operator will answer." I'd call up, get put on hold, and hand the phone to a random kid in the hallway. Of course, they didn't know that Bulgaria was a separate country, so they'd think I'd put them on the line with Russia. The "on hold" recording sounded positively Soviet. It also didn't help that Bulgarian directory assistance operators were particularly curt and abrupt.

The one country that was *really* hard to call was the Soviet Union. There were only a handful of available trunks, and directory assistance calls used the same trunks as any other call being placed to there. Although most countries could be direct dialed, the Soviet Union couldn't be. To make a call, you'd first call the AT&T operator, and you'd have to schedule a time where they'd try to get through. They'd first call you back at whatever number you gave them and, once they had you on the line, they'd make the call when the trunk was free. So, imagine a room full of KGB analysts in Moscow and a room full of NSA analysts in Pennsylvania, all listening intently while you asked a Soviet directory assistance operator for the phone number of "IP Freely" and that's probably a pretty accurate picture of what I was doing. I'm honestly surprised the FBI never showed up at my middle school to ask me to knock it off.

Through free directory assistance calls, I was able to get some phone numbers of McDonald's locations internationally, as well as some random Subway locations in Australia. It was always good fun on c0nfs to call up a Subway "down under" and quiz them about the menu. If you got them during a slow time, they were good sports about it (as Aussies always are). They'd shoot the breeze with you until a customer came into the store. McDonald's locations were harder because these were always busy and it was usually the manager answering. They didn't have time for chit chat; you'd have to pretend you were calling from headquarters with a business question in order for them to spend any time talking with you, and they'd hang up on you immediately when they realized it was a prank call.

One popular location for blue boxers to call was Scott Base, Antarctica. A phreak who had worked at McMurdo Station in Antarctica put the Scott Base phone numbers into a text file that circulated on BBSes, and one of the phone numbers was the bar at the station. McMurdo and Scott Base are adjacent to one another, and the summer population is over 1,000 people. Both McMurdo and Scott Station have a bar, and if you called the phone at the Scott Station bar on a busy night, you'd get to talk to everyone! People working in Antarctica are busy, but they were exceptionally friendly on their off hours and they were seemingly happy to talk to anyone who isn't one of the handful of people they already knew. I'm sure that the Chinese government was puzzled by all of the satellite time used to call Antarctica.

I don't often talk about the past, but it's important to realize that, not so long ago, there were real and significant barriers to being able to communicate with people all over the planet - something we take for granted today. Today's world is so hyper-connected that it's difficult to appreciate how difficult and expensive it was for ordinary people to connect with one another, just because we lived in countries with different political ideas. Long before I began exploring the world physically - visiting 73 countries and territories at last count - I was exploring it virtually by phone. There can still be significant barriers to physical travel, but even as late as the 1980s, the barriers to making phone calls were nearly as high (it could take several days to successfully get a call through to the Soviet Union).

Many readers have grown up in today's world where borders barely exist and where communication has increasingly few barriers. I'm honestly not sure what the future looks like. I do think the more that we talk to one another, the less power that centralized propaganda can hold over us. Propaganda works - whether it's Fox News, Russia Today, or CCTV. However, person-to-person communication is one of the few things that can effectively break through propaganda, and this is one of the reasons why governments try so hard to limit it. I personally hope we don't return to the Cold War of telecommunications.

And with that, I wish you a peaceful summer. I'll be at HOPE in New York in July. As of this writing, my formal participation is not yet confirmed, but I hope to see all of you in a wonderful new venue that I'm really excited to experience. Until then, stay safe, and don't forget your red box!

References

https://en.wikipedia.org/wiki/
➥Roaring_Creek_Station

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

How to Use Gmail to Send Emails From an SMTP Server That You Do Not Own

by duykham

I would like to share with you one way to set up Gmail to send emails so that they could appear as if they were sent by an SMTP server that you do not actually own, e.g. your company email. (Normally, many employers do not want you to check and send emails with your own computer so they do not give you the setting.)

In fact, the emails are sent by Google servers. I'm not talking about the services like Google 360 which allows you to achieve the same thing, but you have to pay for it. Also, Google 360 often requires you have ownership of the domain itself. What if you are trying to send emails as your company's email addresses? You do not own the company's domain.

This is a bug of Gmail; I don't think they meant to set up Gmail like this. However, when I informed them about this bug, they didn't seem to understand what the problem was and said it's intentional. Anyway, since I couldn't make the Google employees fix the bug, it is still there. Now I'm sharing it with you.

A Quick Introduction of the Bug

Gmail lets us "Send email as" external email addresses (in Settings --> Accounts and Import), e.g. someone@company.com so that you can send emails using the Gmail web interface, but the recipient will have no idea the emails were sent via Gmail. They will look as if they were sent by an independent SMTP server (such as the one belonging to your company). This is a cool feature. But, there are two big problems:

Firstly, when setting up the account, Google does not require you to enter the exact credential for that account from company.com, but any account from any (I really mean *any*) other domain could work. That's very strange, isn't it?! You are trying to add someone@yourcompany.com to your Gmail, but instead of providing username and password to show that you have legitimate access to that account, you can use any username/password from any other accounts that you personally own (e.g. soneoneelse@yourdomain1.com, whoever@yourdomain2.net,...).

Secondly, the confirmation of authentication to that SMTP account happens only once, at the time of setting up. That means, every time you send emails ("Send email as" from Gmail), it will not verify your username and password again. It just sends emails as if the account is still valid.

Thirdly, Google makes it worse by falsely affirming that the email was sent by company.com's SMTP server (via TLS, even). (You can check this info by showing the detail information of the email on the recipient's email client.) This is a white lie! They are all sent via Google's servers. All the emails are still sent perfectly even if the username/password has changed or either company.com or yourdomain1.com or yourdomain2.com does not exist (at the time of sending the emails) anymore.

Consequences? Suppose later on, you lose the access to the account (either you are unsubscribed from the service, you are fired from or quit the company you worked for, etc.), you still can perfectly send emails from Gmail as if you still own that company's email. Imagine, once you quit the company and one day you decide to scare all of your former customers with some fake and shocking news. They will believe you because they think you were still working for the company. All thanks to Gmail.

Of course, there are also other good uses to take advantage of this bug; it doesn't have to be all malicious. I will let you decide and choose what suits you best.

I will just provide some technical insight. The rest all depends on your creativity.

So here we go. This is how to setup Gmail to send emails as if they are sent from an SMTP server that you do not own.

Goal

Use your Gmail to send emails as if they are sent by someone@company.com. (This someone@company.com can be either your own company's email that you currently have access to or it's just from one of your careless colleagues that happen to leave their laptop screen on, I don't know....)

Prerequisite

You can read the emails of someone@company.com at the moment of setting up (only that moment is enough).

Setup

1. First, log in to your Gmail.

2. Go to "Settings", and then click to "Accounts and Import" tab.

3. Under "Send mail as:", click "Add another email address".

4. A pop-up window will appear. You fill in with your Name (e.g. "Someone") and the Email

address (e.g. "someone@company.com"). The click "Next Step".

5. In the next screen, you will need to fill in SMTP server, Username and Password. Here comes the interesting part, you *don't have to* use the setting of the email you entered in the previous step. Instead, you can use any of the SMTP account settings that you know, even some free ones on the Internet.

6. Make sure to check "Secured connection using TLS". Yeah, why not?! And click "Add Account".

7. Next, Gmail will check if the SMTP setting you entered is correct. Note that, Gmail *does not check* if this setting comes from the same domain as the email address you are trying to add (which is company.com). Since you own the SMTP account, I suppose you entered the correct info and that there will be no problem with the username and password.

8. Next, after verifying the SMTP setting, Gmail will send an email notification to someone@company.com with the "Confirmation code". This is when you need to check someone@company.com and read the email from "Gmail Team" and get the code. Normally it's nine digits. Fill that in at "Enter and verify the confirmation code" in the next screen.

9. Click "Verify".

10. If you follow exactly what I said, you should be done by now. You can verify it by going to "Settings" and "Account and Import" again. You will see that someone@company.com has been added to "Send mail as".

How To Use

It's straightforward: every time yo want to send an email with someone@company.com address via Gmail, just select it from the "From" drop down menu in the "Compose" window.

Happy "cheating" - I meant, hacking!

FOIA as Weapon

by Radar Lock
radarlock@protonmail.ch

FOIA - the Freedom of Information Act - is a citizen's most powerful tool in the fight against government corruption. This federal law, and its state level counterparts, are (in the right hands) a battering ram for breaking down government secrecy and shining a spotlight into places bureaucrats do not want anyone to look. I spent four years as a newspaper reporter and, much like a hacker, I was always looking for new exploits in the way the law could be applied for investigations. Eventually I grew tired of the dog-eat-dog world of journalism, learned how to code, and jumped ship for the tech industry. But I learned a few tricks along the way (and developed a few of my own) that might be worth sharing.

Tip One - Everything They Have is Fair Game

Most FOIA users ask for conventional items: letters, emails, documents. Don't limit yourself to these, because the interesting stuff lies elsewhere. If, for example, you have reason to think that the county prosecutor is up to shenanigans, ask for his entire web browsing history. His complete phone records can usually be found on his phone bill. Asking for all his emails would be considered excessive, but asking for the metadata for an extended period - subject, recipient, timestamp - is not and may point you in the right direction. And if our prosecutor is unlucky enough to be the user of a government-issued cell phone, or is receiving a government stipend for his personal cell phone, every record therein contained is yours for the taking, up to and including the official's voicemails and Spotify playlists.

Tip Two - Format Your Request as a Question

Government officials are rarely under any obligation to answer your questions, and they do not have to create new records in response to your FOIA requests. However, if you word your FOIA request as a question, it can force them to provide the answer through documentation. For example, if the municipal dog pound is not releasing data on how many animals it euthanizes, you might word a request thusly: "I request such records as would demonstrate how many animals were euthanized in the third quarter."

Tip Three - File a FOIA on Your Own FOIA

This is called a Meta-FOIA. It lets you know how the government processed your FOIA request - who was talked to, where they looked, and oftentimes exactly what they think of you.

Tip Four - Blackmail Their Lawyers

A lawyer values nothing more than they value their law license. This is an Achilles' heel that can be used in your favor, and it is my favorite trick. *Always* try to get a governmental body to handle FOIA requests through their lawyer. When they deny your request for some invalid reason, you can leverage the "Rules of Professional Conduct" (which most states have adopted as their code of ethics for lawyers) to force them into fulfilling your request.

For example, I was once on deadline for a major story, and an agency's lawyer denied my request for critical documents. I was faced with months of delays if I challenged this the conventional way when the story was needed immediately. Luckily, this lawyer had broken a state FOIA law, which I pointed out was a violation of the "misconduct" section of the ethics code. The ethics code also has a rule called "Respect for Rights of Third Persons," which states that "a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person...." Finally, I contacted the managing partner of the firm where this lawyer was employed, explained the violations, and pointed out that a managing partner is just as responsible for the violation under the code of ethics as their subordinate.

All I had to do once I had laid out the ethics violations was threaten to file a formal complaint against their licenses. They emailed me the documents I wanted the next morning. Learning the rules was boring, but once I knew them I was able to wield them with great power. If anyone tries this technique on an NSA lawyer, please let me know how it goes.

Final Thoughts

Since so many of *2600*'s readers bring politics into their submissions, I - a rare "little l" libertarian reader - cannot resist doing the same. Many seem especially concerned about January 6th, which was an event where a group of people who were largely unarmed trespassed on the Capitol, took some selfies, and stole Nancy Pelosi's dias - mostly while remaining between the guide ropes. And who knows if any of this would have happened if undercover FBI agents hadn't infiltrated these groups and apparently goaded these people on?

The fact that this event looms so large in so many imaginations is a reflection of how media distracts us from real issues. I am watching in real time as Biden's 16 percent inflation rate is destroying the wealth of my older relatives. This is not as sexy as January 6th, but it is an actual systemic problem, rather than a distraction. Never forget that BLM sucked all the oxygen out of Occupy Wall Street - and that is exactly what our corporate overlords wanted.

Instead of worrying about "systems of oppression," realize the oppression is built on individual instances of injustice. Go out, find some of those instances (evil is hiding in plain sight, I promise), and use the FOIA toolkit I have provided above to go out and slay some dragons. In my career, I brought down two prosecuting attorneys - one who let a dangerous rapist go despite having a substantial case against him, and the other who indicted a man he knew was innocent. Their scalps are a source of immense pride. You too will find that rooting out corruption is endlessly more satisfying and effective than marching down the street with a placard addressed to no one in particular.

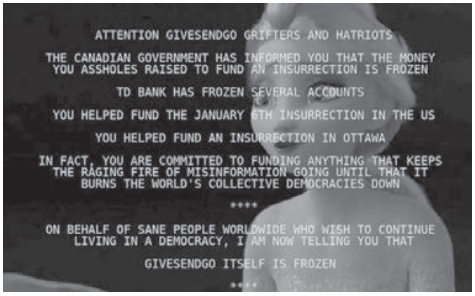
Data Analysis as the Next Step

by Tim R

In *2600,* you see a lot of pieces about reverse engineering, systems knowledge, phone phreaking, and other interesting things a curious person can learn about. In this piece, however, I'm going to advocate for a broadening of horizons, and suggest that data science and data manipulation get added to this list of topics. Take a moment to think through all of the data leaks that have forced important changes in culture and brought about world changing events: the "Collateral Murder" video, the diplomatic cable leak, details on PRISM, the Panama Papers, the Paradise Papers, and the list goes on and on. While it's great that these pieces of information make it into the hands of journalists and academics who take the time to research and find the proverbial needle in the haystack, have you ever attempted the same? Perhaps you've taken the time to actually download these troves of data, but have you taken the time to sift through them yourself to see what speaks to your community or what poses danger to what you find important? I think the time is right to suggest that examination of data at scale is the next step you should be taking in your pursuit of the hacker ethos.

An anecdote might help motivate the discussion. In January of 2022, a convoy of disgruntled citizens established an occupation of downtown Ottawa as a way to protest what they believed to be unfair restrictions on freedoms through the implementation of vaccine mandates and enhanced procedures at border crossings. This occupation of Ottawa was a real mess, both figuratively and actually. Daily life came to a standstill and the government, both federal and provincial, as well as police, seemed reluctant to do anything about the situation. Taking a step back for a moment, clearly the lead-up to the convoy's appearance in the capital city of Canada required a buildup of people, support, and enthusiasm. It can be said without any surprises that creating such a moment as this requires commitment of all sorts and undoubtedly money to make it happen.

As is common today, the organizers of this movement took to crowdfunding to get the word out and to solicit donations. As the motivations of this group were a bit dubious, or at least not apparently clear where motivations fell, the initial crowdfunding campaign using GoFundMe was frozen. Looking to find a viable alternative, the organizers of the group moved to a lesser known, and probably poor choice, of GiveSendGo. If you've been paying attention to the news, GiveSendGo has a known history of poor security and a lax approach to site updates. Quite suddenly and with great surprise, suddenly the site redirected to an alternate domain, `GiveSendGone.➥wtf`, and, instead of a page outlining ways to give and totals to date, a page was presented stating that "GiveSendGo itself is frozen," and also presented on this page was a link to a 40 megabyte spreadsheet of leaked donor information: name, email address, donation amounts, IP addresses, and anything else you could think of that would identify and provide insights about who contributed.



Here is where curiosity got the better of me. This development happened fast and, by the next morning when I finally realized something was up, I attempted to find the dataset. However, the hacked website was gone as was the spreadsheet. Curious and interested to see what was in that spreadsheet, I attempted to retrieve it by a generic web search and only found a series of different results analyzing portions of the data, all of which were very insightful and clever[1]. In the days that followed, a veritable flood of analysis pieces were published. While all these works were great demonstrations of data journalism, I still felt compelled to continue digging to get exactly what it was that I wanted. The next step I followed was to find the wiki page for the leak on Distributed Denial of Secrets[2]. Once there, I was greeted with a message saying that those interested in the information would need to contact DDoS directly to request access. The presumed purpose of this step was to ensure that responsible use of the information was adhered to. I respect the rationale and motivation for such a move, but I was still curious. I wanted to see if anyone at the same organization as me contributed to the group by foolishly using their work email address. I

also wanted to see if the funding was in fact coming from foreign bodies.

Enter the next step in the process, something that should be in the toolbox of anyone who spends time online: the Internet Archive Wayback Machine[3] This invaluable mechanism of Internet history is able to take snapshots of web pages over time and present these snapshots fully rendered in a sensible interface. The Wayback Machine is extremely useful for so many different venues of research and, delightfully, it throws a little bit of a wrench in the usual operation of the Internet, which usually functions as an actual memory hole. Within minutes, I was looking at a capture of the .wtf domain mentioned previously and was also in the possession of the spreadsheet I was so compelled to find.

Armed with the data, the next step, of course, comes down to how to analyze it. Here, yet another tool came into play. Simply put, the Jupyter Notebook, made available via Anaconda[4] or through various other means, such as Google Colab. If you've spent time using Python for traditional programming projects or for scripting, this represents yet another paradigm that you can use your skills for. In short, it is a web page that allows you to embed chunks of Python code and render their output by executing the code in a specifically deployed virtual environment. A search for "Python Pandas" will provide the broad strokes of how to interact with data using this suite of tools. Another site worth consulting is Kaggle[5]. It provides interactive tutorials on data manipulation using the Notebook paradigm. As an alternative, another platform worth considering is R, or more specially a cloud hosted platform called RStudio. While just as powerful, it isn't my default as I spend so much time with Python that I don't want to lose my fluency with that language.

Now, armed with the data and the proper tool to explore it with, the fun could begin. Some simple first things to explore: comparing donation amounts based on postal codes in my community (think the Canadian equivalent of a ZIP code) , analyzing the full-text of donor comments to see just how seditious they might be, and finding out what IP addresses associated with government agencies might be on the donor list.

Bringing it back to the original thread, I hope this narrative compels us all to think of the full story of how a leak should play out. Not just the discovery and distribution, but also the analysis and evaluation. The hacker mindset is about discovery, curiosity, and ingenious thinking. Often we see this come to life by circumventing roadblocks imposed by DRM, or by helping disseminate information acquired by whistle-blowers at great risk to larger audiences and to the mainstream popular media. How often have you spent the time systematically working through a leak, or providing someone the tools and know-how to do something similar? I'm hopeful that the answer is something non-zero.

If this isn't compelling enough an example, I encourage you to dig into this idea of operationalizing leaks by looking at the technical tools that the International Consortium of Investigative Journalists[6] have developed that are used to comb through terabytes of documents in order to find meaningful information that takes down despots and fights fascism. These are marvelous tools built on top of large scale data analysis platforms, all open source, that allow you to use your command line knowledge and Python skills to sift through vast amounts of data. Better yet, what about helping a local journalist or community group utilize these tools to make meaningful discoveries? There is a steep learning curve for people not acclimatized to working with computer systems, let alone large caches of files, to even make sense of how these tools can be used to serve the greater good, let alone to have the wherewithal to bootstrap these systems and to seed them with data. Imagine handing over a refurbished machine, now air-gapped, running an instance of Ubuntu on it preloaded with gigabytes of data and an intuitive web interface as the way to interact with it to a person who is just waiting to be given the tools that will allow them to crack open a very important investigation.

Platforms like SecureDrop and end-to-end encrypted communication channels do wonders for allowing those who are vulnerable to get in touch with trusted organizations so that they can provide information on nefarious dealings, but what about the last mile? What about enabling and performing the analysis in the first place? This is a step that I hope is part of the hacker ethos that will continue to be important as inevitably more and more leaks surface.

Links

[1] www.cbc.ca/news/politics/convoy-➥protest-donations-data-1.6351292
[2] ddosecrets.com/wiki/GiveSendGo
[3] archive.org/web/
[4] www.anaconda.com/
[5] kaggle.com
[6] github.com/ICIJ

Web 3.0 is Bullshit

by aestetix

Every so often, a new buzzword permeates through the tech world, inspiring endless blog articles, conference talks, and empty corporate announcements. The most recent of these is "Web 3.0," which is being hailed as some kind of "decentralized Facebook using the blockchain." From both a technical and a conceptual view, Web 3.0 is bullshit, and in this article we will attempt to explain why.

Let's quickly cover the framing that tech pundits are trying to use to delineate between Web 1.0 and Web 2.0, and then look at the actual turning point. In many discussions (and on Wikipedia), we can see people making the argument that Web 1.0 started in 1991 and lasted until 2004. This is mostly reasonable.

They then proceed to say that Web 1.0 was "read-only," static pages with no user interaction, and wasn't capable of showing ads. This is completely wrong, and only establishes that the pundits making this arguments never *used* Web 1.0. In the mid 1990s, we had sites like GeoCities, which allowed people to log in and create their own web pages, and sites like Slashdot had - and still have - massive post interaction; in fact, Slashdot gave us the term "Anonymous Coward," used to describe someone posting comments anonymously. As far as advertisements, technologies like pop-up blockers and ad-blockers were a direct response to the constant barrage of advertisements from websites. And all of this was happening long before 2004.

A better marker for Web 2.0 is at the protocol level. With Web 1.0, while we could do all of the things that tech pundits now claim we couldn't, viewing updates *did* involve refreshing the page. That is, the browser would make an HTTP request, get an HTTP response, and that would be the end of it. Web programmers came up with ways of making websites seem interactive, using tricks with hidden divs, as well as JavaScript and CSS elements; however, the real innovation came when we realized we could use a JavaScript object called XMLHttpRequest to make a new HTTP request from the browser, grab the response with JavaScript, and parse it back into the page *without refreshing the page*. This fundamentally transformed the web. It enabled things like real-time updates without the need to click an "update" button, and opened the door to a lot of drag-and-drop web technologies we now take for granted.

We also realized that because JavaScript - like many programming languages - is Turing Complete, we could use it to recreate almost all of the software we used on the computer, such as email clients and word processors, in the web browser. We now take tools like Gmail and Google Docs for granted, but in 2004 such an idea was revolutionary. In many respects, these uses of JavaScript brought us into the modern Web 2.0 era.

Defining Web 3.0 is a lot trickier. As soon as the term "Web 2.0" was coined, tech pundits were trying to slap the label "Web 3.0" on every new craze. Some said that Web 3.0 was Big Data systems like MapReduce. Others suggested it was the advent of mobile devices (iPhone vs. Android). Still others ensured us it was the walled gardens of Big Tech itself. It's a bit ironic to watch the same pundits who once said that Web 3.0 was Big Tech now announce that Web 3.0 is the technology that will help free us from Big Tech.

But let's take the pundits at face value and assume that Web 3.0 is what they claim: using blockchain technology to allow people to set up applications in decentralized systems that are free from Big Tech. The problem with this claim is that both Web 1.0 and Web 2.0 were already decentralized, without needing a blockchain. In addition, questions that many tech pundits are now posing regarding how to curb censorship while preventing crime with Web 3.0 have

already been addressed, as the same issues have arisen time and time again over the last 30 years.

Web 3.0 purports to enable data ownership, but we can already do that. All we need to do is set up our own websites on our own servers, which is now easier than ever. If the issue is interoperability, we have all kinds of technology to do that. If we want to find a list of open systems and protocols, we can simply look at technologies that Big Tech companies initially embraced and then abandoned to force everyone into their walled gardens. It might be worth asking why Google killed off Google Reader, which used RSS; or Google Talk, which supported XMPP.

Regarding the questions of censorship and free speech, this is not a new debate. In the early 1990s, we had the debate on whether there should be an "Internet Driver's License" when the Internet was known as the "Information Superhighway." We then saw the advent of laws like the Digital Millennium Copyright Act and the Communications Decency Act, both passed in 1996, attempting to address issues of digital ownership and speech. We also had websites like WhiteHouse.com (a porn site), and Nissan.com, a small family owned computer company which has been fending off lawsuits from the massive car company since 1994. And, for that matter, consider the decades of debates within ICANN about whether to create a .XXX top level domain.

In conclusion, Web 3.0 is bullshit that simply revives old ideas, and the only new insights revealed by the current "discussion" are the level of absolute ignorance of tech pundits and the depth of greed of venture capitalists who are probably trying to recoup losses from bad investments into crappy cryptocurrency startups. Slapping a blockchain onto a website is not going to magically solve everything. Then again, what more can we expect from the ruling class that is attempting to usher in the "metaverse?"

Book Review

***Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Andy Greenberg, 2019, ISBN 978-0-385-54440-5**

Reviewed by Br@d

I received a free copy of this book back in late 2020. The author and senior writer for *Wired* was the keynote speaker at a virtual user conference for a security vendor that I was working with at the time. I was one of many attendees who won a free copy of this book by taking part in the conference's gamification. This involved attending various sessions as well as visiting the virtual exhibitor's hall to interact with sponsors. Not only did I win a free copy of the book but with some basic enumeration, I was able to upgrade my prize winnings to a higher level (the details which will be left for another time).

Around late 2021 I finally got around to reading this book. It had been on my to-do list for a while; I just never had the urge to dive in. Once I finally did get to it, I was pleasantly surprised at Andy's flow of information. It was very easy to follow (regardless of your technical background) as it took us through more than a decade of the world's most well-known cyber attacks. More important to current times, this book covers a lot of background information that better put in light the current political and technological struggle that is happening between Russia and Ukraine (and the world).

This book is filled with various references that go into extensive detail, yet is still an easy read for the tech and non-tech savvy alike. Not only was this an informative and enjoyable read, but it was also scary at times, bringing the hard realities of how acts in the digital realm can have a significant (and even fatal) impact on our physical world.

WHY YOU NEED TO SELF-HOST

by Byeman

On December 14, 2021, Google published an article titled "New Notifications When Drive Content Violates Abuse Program Policies"[1]. This rolled out to all Google Workspace customers, as well as G Suite Basic, and Business customers. What does this mean? Whether you're a small business, an activist community, a Fortune 500 company, or an individual, Google is monitoring your data, data that you're paying Google to store, and deciding for you what you can and cannot save. There is no admin control for this feature.

Google doesn't know, or care, about the context of the files stored. Let's assume you run a non-profit fighting racism in your community. You collect the hate mail you receive, the threats, pictures of the people protesting you and your work. All Google sees is a bunch of hate speech stored in your account and, presto, your files are locked down.

If you're a Fortune 500 company, you clearly have resources to fight this. And hopefully your legal team and IT department can advise you about what you should and should not store in the Google cloud. Once again, the little guy is the victim. What can be done?

Self-hosting!

I could use every single page in this magazine to tell you a fraction of what you need to know. I haven't approached the folks at *2600* HQ about this, but, wait, wait, no they're shaking their heads, can't do it. And honestly, I'm not qualified to do it. What I am qualified to do is encourage you to dust off your hacker caps and get to work.

I hang out on several forums related to self-hosting and the various platforms that can be hosted. I see people making the same, even worse, mistakes than what I made. I'm new to this. In the early months of the pandemic I needed a distraction. I screwed up. Oh lordy, I screwed up. But you know what? It was okay that I did. I was learning. And secondly, I chose to learn using a Raspberry Pi and a virtual private server (VPS). Why was this important?

Rule One: You're a student, not a master. Choose an inexpensive gateway to the drug that is self-hosting. VPS hosting can be had for as little as $5 a month and a full blown Raspberry Pi setup can be had for well under $100. If I had decided self-hosting wasn't for me, I wasn't out much money. But there's a second much overlooked benefit. It's trivially easy to do a hard reset. If you've completely hosed your server, just destroy it and create a new one. This process takes about 15 minutes on a VPS and about the same on a RPi. Which brings me to...

Rule Two: Don't make any of this your daily driver. You're not ready. Continue to use Google Drive, OneNote, Dropbox, and Gmail. I really feel bad for people when I see their pleas posted at 2 am saying they had moved all of their photos into their Raspberry Pi and now the Pi won't boot and when they pop the SD card into their laptop, all it can offer is to format the memory card. Before you migrate, be sure you're using robust hardware and have a backup strategy implemented before you move your data.

Rule Three: The community will help you if you help yourself first. It was rare that I had to post a question to any forum because I was not the first person to have the issue. Use the search function first. If you find a thread and still have questions, ask on the existing thread. If you can't find it, start a new one, but in both cases you need to help us help you. Asking for help on a poorly described problem will get you ignored and following up with "isn't anyone going to help me" will only make you a pariah. At a minimum, we need to know your operating system, your hardware, what you were trying to do, what were you doing when the problem started. Before you even think about asking for help, search the error message. Review your logs and search on the error codes and descriptions you see. You'll be amazed what you'll find. If you show the community you did your homework and provide them with enough information, they'll be happy to help you.

Rule Four: Give back. If you post a problem and find a solution, tell us about it! Please. The next person with that problem will want that information. As you learn, browse the forums and jump in to help whenever you can. Believe me, the community will get to know you, will trust you, and will be more willing to help you as you continue to grow and get more advanced in your self-hosting journey.

How to get started? Pull up your favorite search engine and ask "how to get started with self-hosting" or something along those lines. Some of the better resources include:

```
cyberhost.uk/getting-started/
www.reddit.com/r/selfhosted/
docs.standardnotes.com/self-
➥hosting/getting-started/
```

I hope this inspires someone. My next article will discuss cool tools you didn't know you needed that can be self-hosted, solving problems you didn't realize you even had.

Happy hacking!

```
[1]  workspaceupdates.googleblog.
➥com/2021/12/abuse-notification-
➥emails-google-drive.html
```

Should I or Shouldn't I? Ransomware Negotiation

by lg0p89

Ransomware's successful use as a malicious tool is growing. Way back when this began as only encrypting files and systems, the affected party or business would receive the usual message to pay for the decrypt key in Bitcoin. If no payment was made in a reasonable amount of time as determined by the attackers, you generally were out of luck. There was no appealing to any level of moral fiber, but only "pay me." At times, people would get lucky and find the decrypt key in code or a file left somewhere on the system. This was not the norm, but occasionally the person/company would be fortunate.

This evolved with additional forms of encryption and, as a tangent, instead of only having the option of encrypting, the attackers added exfiltering the data and threatening to publish it unless the ransom were to be paid. Now the targets had two issues to possibly contend with.

As ransomware has become much more profitable with an ROI (return on investment), the attackers operationalized this into an industry. This is so prevalent that it even has its own acronym: RaaS (Ransomware as a Service). Gone are the days of the lone attackers targeting businesses from his own system. The bad actors have businesses set up and working with ransomware attacks as the corporate goal. As the ease of use continues, this is only going to get worse until a robust, reliable set of tools becomes available to combat this directly.

If there is any doubt on how expensive ransomware can be, just do a quick Internet search.

- The CNA insurance company dealt with a ransomware attack in March 2021 that cost $40 million.
- Acer had a $50 million ransomware demand that same month.
- In June 2020, the University of California at San Francisco paid $1.14 million.
- In early 2020, Travelex paid $2.3 million.
- In May 2021, the North American division of Brenntag paid $4.4 million.
- Colonial Pipeline in 2021 paid $4.4 million.
- CWT Global, a U.S.-based travel services company, paid $4.5 million in July 2020.

These are only the large and published payments. Adding to the attackers' revenue are all the other smaller successful compromises and payments. This line of work can be lucrative, which is what continues to drive this forward.

The question is, if you happen to be infected, what is the next step? Do you pay or not pay? If you don't pay, get ready to spend a lot of money on new equipment. If you pay, you may be a victim of BOHICA (Bend Over, Here It Comes Again), as they know you will pay.

The choice boils down to economics. When there are viable backups which are recent and go through periodic checks, you may not need to pay. If, on the other hand, the backups are done quarterly and the system has never been checked other than to look at the record when the backup was last done, the company and their insurance carrier may want to get their checkbook out. If you choose to pay, you may ask yourself if you can negotiate with them. Maybe you could pay a little less and still get your files back or they'll promise not to disclose the files.

The attackers have lofty goals for the revenue generation from ransomware. The amounts they are seeking are probably not in line with what the business and/or their insurance company, if they have the coverage, are able or willing to pay. In the attackers' minds, you have a massive treasure chest of gold, when you have enough for a month or two of cash flow. This perception has been furthered by the large payment mode by companies who really didn't have a choice. This is where the ransomware negotiator comes into play While the attackers still need to maintain a planned revenue level, there is no blank check for them. With ransomware being so prevalent in the last two years, the negotiator role is relatively new. This role may be used more as the attackers who already have compromised your system ramp up the pressure to pay them with calls of threats and intimidation.

In this case, when you have no other choice but to talk to them, the negotiator is there to mitigate the amount and talk to them, focusing on the relevant points.

Social Engineering Attacks Out of Control

by Stephen Comeau

Before the pandemic, social engineering attacks were prevalent. I used to get calls on them once a week on a regular basis. Who would have thought we would wish we could go back to that once-a-week scenario as being relatively favorable? Social engineering attacks have since taken on a life of their own. Now, I deal with 20 to 30 calls *per day* on this issue at minimum.

Social engineering attacks have not only grown more frequent, they have become more sophisticated. Not only are regular users having difficulty separating the false from the true, but career IT people are having the same problem. And this is particularly troubling, for it directly affects our overall ability to adequately respond.

To focus on the specifics, one out of ten adults falls victim to social engineering attacks every day. Currently, the most prevalent of these attacks is the phishing scam. Phishing scams target email and phone communications alike. There are also plenty of new attack vectors - less common but likewise troublesome. Some involve text messaging. These have come naturally to the fore with the development of emerging technologies within the larger IT realm.

Looking back in time, we see that phishing attacks are not new, and have posed a problem of longstanding duration. However, since the pandemic, these types of attacks have increased exponentially in a way that had not been properly predicted, causing them to occupy center stage in modern efforts to keep communications systems secure. Phone scams (or phone attacks) have increased by more than 150 percent since the start of the pandemic. In fact, phone attacks have become so problematic that the Federal Trade Commission has taken particular and serious notice of them, putting the weight of the federal government behind a larger national effort to mitigate them.

Over the summer (July 2021), the FTC began enacting statutes requiring providers to implement Caller ID authentication. This new regulatory focus represents one of the most extensive campaigns undertaken by the federal government to combat the phone scam epidemic. This overall effort has been particularly aimed at reducing the growing number of robotic phone attacks.

While this federal-level effort is reassuring, it is at best a temporary Band-Aid solution. It will undoubtedly help to stem the overwhelming tide of phone attacks for a short time. But, as we know, the "game of cat and mouse goes on," with bad actors becoming ever more sophisticated in their own efforts. As expected, new software has already been developed to evade the FTC countermeasures. Some of it involves a novel implementation of traditional cloning technologies, making use of cloning software that is readily available and simple to use. All that remains to do, upon utilizing such software, is to dial the first unwitting victim's number. Beyond that point, it takes only two seconds after the individual accepts the incoming call for his or her phone number and device identity to be acquired. This device identity, or IMEI (International Mobile Equipment Identity), is a 15-digit identifier that links the phone with a specific phone number.. On the victim's end it looks like the scammer's call is coming from you. All this occurs with your active participation, yet without your knowledge of what has actually occurred - and the FTC countermeasures are evaded. Scarry, right?

As previously noted, cloning software like Dr.Fone and CLONEit is nothing new, I remember messing around with similar software for learning purposes a decade or so ago. I further remember some of the troubling discoveries I made. It was scary then, it is scarier now. In the old days, you needed to be physically near the victim's phone to compromise it. Nowadays, such attacks are far easier to implement and with more sophisticated software that is more readily available. You don't have to be an uber-hacker to run a cloning phone attack on the average phone user anymore. Anyone with enough knowledge to run a kiddie script level attack could easily deploy one nowadays. This accessibility highlights the need for preventative measures to be adequately employed. Some such basic measures are as follows:

- Always keep your phone software current with the latest updates
- Always keep you phone properly locked down

A minimal level of security on any phone

should always include:

- Having a passcode lock on your phone
- Encrypting your phone to protect your information, especially your IMEI number (Encrypting your phone in this way makes efforts to steal a copy of this critical number vastly more difficult.)
- Never leave your phone unattended, especially in a public place
- Do not leave Bluetooth on when you're not using it

Protect yourself by educating yourself as to the sophistication and diversity of modern cyberattacks. Attackers will often use several different techniques to get what they want from you, some of which we have covered, and others of which we will cover now.

The first of these techniques is the social engineering attack, by which you pose as someone else, likely someone important, working for ether a regulatory agency, key vendor, or authoritative management team within one's own company. So, if you are ever unsure of the legitimacy of a call, hang up. Then call back the specific agency or company on their known public line to verify their identity.

Another technique phone attackers or scammers will often use is to create a sense of urgency. They will create a scenario where you will need to do something or give them something right away to keep something else bad from happening. Note that nothing is ever urgent enough for you to avoid properly verifying their claims. Never provide any personal information or financial data to anyone who calls you whose authorization to receive such information remains in doubt. To emphasize, you can always hang up and call back the agency or company's legitimate known number for verification.

Also know that official government agencies like the IRS will never call you randomly. Doing so is a clear indication of a scam. Always verify any call you get from a party you would otherwise hope to trust, especially if what you are hearing sounds too good to be true. I can't emphasize this point enough!

Another sure sign of a scam attack is a demand for immediate payment. No company or agency will expect you to respond on the spur of the moment without adequate thought. Additionally, if they demand a specific form of payment, like a gift card or Western Union payment, this is a sure sign of a scam. Hang up.

Also, never let anyone you don't know have access to your personal devices. You have no idea how many times I have heard the same story. "Oh Mr. (Blank) called me from (Blank) Company and asked for access to my computer to fix (blank) issue I was having." No! Wrong!! Do *not* give anyone unauthorized access to your computer or personal device without first verifying the legitimacy of that access. A legitimate company, without a partnership or vendor relationship, will never ask you for access to your device. Remember, as before, to verify this request by phoning the company on their main line as the best way to handle any access issue about which you have significant concerns.

Another method of dealing with scammers is to record the number you were called from, and then to block it on your own phone.

Finally, you should always report any phone scams or phone attacks to the FTC (Federal Trade Commission). It is very important that you remember to fill out the pertinent - and simple - form at the FTC website. By reporting the scam attempt, you are helping the FTC keep track of changes in and frequency of different attacks. You are, in the process, keeping others from being victimized. The FTC has the power to flag compromised numbers through phone companies and to place those numbers under review. By this means they can hope to apprehend those who have compromised phone identities. You can report any such issue to the FTC here: `reportfraud.ftc.gov/#/`.

I do hope this article serves as a needed wake-up call (no pun intended), adequately informing the public on how social engineering and spoofing attacks occur, and in particular from a phone attack perspective. It was also my intent to describe what should be done to prevent this form of attack from occurring on such a large scale in the future. My hope is that with some effort and better public security education, the attacks I have enumerated in this article will finally start to, once again, become few and far between. We may even return to that more-desired point where we are getting just one social engineering attack inquiry per day. It's a nice dream, right? Either way, it is now clear just how big of a problem social engineering attacks have become, and that something effective needs to be done about them now. Stay tuned for further updates.

The Hacker Perspective

by Rick Swords

Growing up, my father was the director of electronics for a large, cash heavy medical center campus. This meant that he and his crew were responsible for sourcing and maintaining every piece of technology in the place. Sometimes in the summers I would go to the electronics lab with him on the lower level of the hospital and the techs and engineers would let me solder, and tinker, and tolerate my begging for food.

Sometime thereafter, my father would ask me to help him get some things out of his car that would change my life... forever. After some heavy lifting, sitting in our dining room which became an office after he and my mother divorced, there was no more china cabinet, fancy seats and table settings - just an IBM PC XT with dual 5.25 inch floppy drives, 640k RAM a 10MB hard drive, keyboard, IBM amber monitor, dot matrix printer, and a Hayes 300 baud modem. For those of you who don't go back this far, 300 baud is about .3 kb/sec which equals... infinitely faster than nothing. Huge technical books about the PC, DOS, Basic programming, Lotus 1-2-3 (you may know this as some form of spreadsheet), and other floppy disk applications.

My father was keen to get his entire budget and spending practices into Lotus and hand them to higher ups as a signal to back off, give him what he wanted, and generally make his job easier. So the first thing he did was to teach me to load the application; open the proper file; enter the data and formulas in their correct cells, columns, and rows; and save the file. This may not sound like much, but this entailed teaching me the DOS command line for creating, saving, and manipulating files. I caught on pretty quickly - not because I was some sort of financial wiz, but finishing the tasks he assigned meant I had the whole setup to myself until I couldn't keep my eyes open anymore. Then do it all over again.

It was on. I was dialing up BBSes to chat, play games, try to break things, and other fun and mischief. I connected with other kids and adults who taught me tips and tricks of all sorts. My first real game was *Zork*. I quickly learned that I sucked at games and was more into just exploring and learning new things.

Thirty-five years later, my friends still joke that they only knew I was home if they saw the amber screen glowing through the window of our dining room. A yell meant "Yo, u good?" A whistle meant "Pause that shit and get outside - we got some gangbangin' to do!" That was me. Part time geek, part time street kid. This dichotomy of interests would continue to shape my life for a long time. The older kids in the neighborhood knew I was generally smart, and encouraged me to nurture my intellect, and not to get caught up in the street life. I loved my fellow Vice Lords and they knew it. I eventually was given the rank and role of "Minister of Lit." My duties included maintaining the "literature" or rules, regulations, and *creed* of our organization, and maintaining copies of this for new and old recruits. I also kept minutes of meetings and assigned security details. Sounds fancy for some 12- to 21-year-old street kids, but back in those days we had order and maintained it. Period.

Maybe you can see where this is going. Soon all the Lords in my hood had *printed* copies of our Lit, prayers (yes, we prayed), meeting minutes, roll calls, etc. This would eventually get us very high praise when we would attend the larger meetings of groups of neighborhoods to "check in" and generally assemble. We became known as a group that had our shit together, and I became known as the "go to" for teaching other MOL officers to keep tight records. Please note, although there was plenty of unlawful action going on, record keeping was strictly from an organizational standpoint. Internal and clerical - same as any other private social club or similar group.

I was young, smart, tough, chubby, wore glasses, and I was honest. These traits were unique in the body politic, and I was cherished and protected by the older members. I felt the love and returned it. I needed it to survive outdoors.

One day in eighth grade science class, the principal got on the PA system and asked if I was present. My teacher answered in the affirmative, and she responded by saying that I need to come to her office immediately because "we think his house is on fire." It was. My school was one block away and I could see the smoke as I left the schoolhouse. I made it there to a scene of fire trucks, police cars, smoke, water... *lots* of water, and the bottom half of my childhood home dripping and smoldering.

The other thing I saw was my father. He was leaning on his car, smoking a cigarette and talking to the Red Cross and firefighters. My father grew up in the Bronzeville area of Chicago, was a Navy veteran, and was a cool customer. He was like me, but better. He was smart, tough, and well respected. I'm saying this to say, we didn't exchange too many words. "What happened, Dad?" "They don't know yet" was enough for both of us. We were more interested in the next plan of action.

First thing was two brown paper sacks from the Red Cross that contained underwear, t-shirts, and socks for the both of us. My father finished some business with the firefighters - they left. Then the insurance company chatted with us and gave me a thick stack of lined paper, and gave my father a check. You get three checks when your life burns down and you're insured. That was "check #1" right there in front of the dripping house.

Some of you reading this may have seen homes burn down on TV or something similar. When it happens to you, the finality of it is staggering. Your forks and spoons, couches, secrets, clothes, sundries, photo albums, your *history*... is gone. It hits you in waves. As you think of something to go get, or use, or equip yourself with, it's gone. But that night, my father and I cashed the somewhat large check, hit the mall, locked down an arms hotel for a month, ordered food, and hunkered down with the stacks of lined paper to write down *every* single thing we had in the house to claim for its monetary value. My father was an honest dude, so we stuck to reality - no hacking the insurance system. This was the necessary duty to get "check #2."

The next day I went to school in my ill-fitted jeans and NGO t-shirts. I answered all the questions about the fire and, it being close to the end of the school year and time for high school, I graduated and made it through the summer. My father meantime got check #3 and ordered the contractors to finish our house by the end of summer. They did, and we moved into a brand new house on the same land and filled it with brand new stuff and, most importantly, we went absolutely crazy with new computer systems. By this time (I'm terrible with dates), I think the IBM PC AT 3.5 inch disks was the hype. The hard drive was 100MBs, the modem was 9600 baud, and the monitor was RGB... for god sakes *R...G...B!!!*

I was back at it. Geeking like crazy at home, gangstering like crazy outside, and failing miserably in high school. My mother wasn't having it. She made an executive decision that I should leave Chicago and live with my ex-Marine, self-made millionaire uncle in the suburbs of Maryland to finish high school.

It was great for me. While I was there, my father got remarried, and I spent my time reading from my uncle's vast library of books and teaching myself more computer skills. The town I lived in was full of miscreant ex-pats from Brooklyn, New York, D.C., Virginia, New Jersey, and other places. We were all good/bad kids that needed a change of pace. My background was a good fit with the east coast teenagers. They believed in mental and physical fitness, knowledge of self and being generally a civilized being... with some super rough edges. After a couple scuffles, I was accepted as the Chicago kid. Country as hell to them, but cool.

I got great grades, lost lots of weight, started a videography business, and grew mentally. But there was one problem. Because of my utter failure in gaining credits back in Chicago, the school wanted me to graduate a year late. Class of 1991? Not an option. I was in the class of 1990. Period. My uncle understood, and I dropped out and got my GED and attended University back in Chicago. The *same* university my father worked for on the medical center side. So while I hacked my high school graduation with a General Education Diploma, my father's clout hacked my college acceptance. I was in.

It was 1991 and the Internet was becoming ubiquitous to those in the geek set, and to normies email and instant messaging were the killer apps. I did a couple years and dropped out from party exhaustion and, to be quite honest, I missed the streets. This section I will redact because I was older, nowhere near as smart as I thought I was, and the middle 90s were crazy. Let's keep it at that. I eventually went back to school and discovered they had a computer science degree offering. In 1999, I had an interview with a Fortune 100 technology company and was told by the interviewer that I didn't need the degree, I should finish the classes I was taking, and he would give me a job in his research lab. I knew what this meant: fun, freedom, and an unlimited budget. I was in.

I was having a ball. I worked for an absolute genius, and he gave me all the room I needed to explore *after* I handled the tasks he assigned me. I was used to this dynamic and handled it well. In the early 2000s, I worked on wireless high speed Internet, bluetooth, touchscreen tech, and smart appliances. My boss saw this future we live in now, and let us do what we wanted and needed to create it. My boss has since passed away, but some of my fellow engineers have since formed a great company some of you may know: Ubiquiti Networks, Inc.

During my tenure, I traveled quite a bit. During my travels, I met a young lady. She

was a recent hire at Microsoft. We became fast friends and she began to tell me that her previous job was at GE Capital. She was competitive and, while I bragged about hacking and tech work, she would tell me that I didn't know how to hack the most important thing... *money*. This got my attention.

Before long, she was teaching me how companies were built on paper: from the employer identification number; to aged shelf (not to be confused with shell) companies (companies that were formed in years past and put on the shelf to let them "age"); to financial documents and what underwriters look for; down to a corporate website and virtual phone, fax, and office services to give a company a real world presence in an emerging virtual landscape. Before long, we put together our first multi-million dollar company and began to socially engineer every creditor we knew. We were quickly getting credit lines, travel accounts and cards, auto loans, and whatever we wanted based on these *shell* companies.

Within a few years, we both quit our jobs and began to hack the credit system full time. We both had luxury cars and condos, six figure corporate credit cards, and a money supply from my street connections that required everything from restaurant furniture at 50 percent on the dollar to farm equipment. We would take a little and pay our bills, and travel and have fun with the rest. I thought I was the smartest guy in the world while simultaneously knowing I wasn't.

In 2004, at the height of my powers, my mother, father, and one of my best friends all died within 60 days of each other. Liver failure, lung cancer, and murder by police respectively. I was silently devastated. I did what I could to help bury them and help their other survivors, and put my nose to the grindstone to make as much as I could and get out of the game.

By 2008, we had built a network of shell companies that did business with one another like a pyramid. At the top was me. One day, when I was picking up a truckload of electronics from a location I used for such things, I was quickly surrounded by federal agents. They identified themselves as members of the U.S. Postal Service, Secret Service, and Chicago Vice. I was charged with theft and questioned. I kept quiet and was let go, but the jig was up.

My federal case was hard to indict because the place they interrogated me was being exposed publicly for being an inmate torture site (the feds wanted nothing of this), and I had an all female staff (no male voice, or handwriting, or witness recall) that was pretty stoic. Soon though, the feds kicked in my home door, guns drawn, to find loot and weapons I had for home protection and gave me a state case for them. They seized, froze, and demanded all I had. The federal investigation ripped through my money until I was in tatters, and the state case lingered like a gray cloud over my remaining pennies and self-made hell.

My state case went on for three years. During this time, I started a business consulting firm helping people to put together *legal* companies with the skills I acquired in the fast life. During this time in 2010, I kept my eyes and ears to the street. And the word on the geek streets at this time was Bitcoin (the code). I was sucked in instantly.

I thought to myself, now *this* is how you hack money.

Over time, I began to mine and acquire and see the elegance in the code for what it was. I was also broke and in a unique position to see my future with a money that was unconfiscatable *if* I was careful.

In 2011, I was sentenced to the minimum three years for unlawful possession of a weapon and had to do half of that. During my time in prison, I taught GED classes, wrote a patent for music streaming, and read *The Best of 2600* (*wink*). Upon my release in October 2012, I came home to a few bitcoin (the money) on an Apple Time Machine drive and submersed myself back into the code and community. On my date of release, the exchange rate for Bitcoin with USD was around $13. Despite a few slip-ups and clown maneuvers, I have pretty much been dollar cost averaging since then. I cannot believe how far it has come. I now teach Bitcoin security and monetary policy to friends, businesses, and non-profits.

As I write this, the world is in the midst of a global financial crisis and a viral pandemic. I'm seeing many people start to crack. Some of their belief systems and trust are being broken. Their governments are printing money from thin air, and can't protect them as they once believed. This makes me feel for them... and be grateful. Grateful I can teach myself new skills with primitive tools, survive being a child of divorce, having my home burn to the ground, bury both my parents and loved one back to back to back, the streets, time in prison, and starting again with nothing. The world is in chaos at the moment. But it won't break me. I don't see chaos. I see problems to be solved collectively. I see things from a Hacker's Perspective.

Rick Swords (@rick_swords) is a Bitcoin professional and educator. Rick is now spending his time investing in Bitcoin-only startups and running a Bitcoin ATM network with the help of his daughters and young son. "It is my wish to empower all the human families with the only cryptographic money with street credibility: Bitcoin."

Sleuthing Google Apps Part 1: Google Calendar

by Estragon

In a pair of articles, I will describe straightforward but non-obvious ways to see what other people have been doing in an organization you have online access to. In this first article, we will see how Google Calendar can be utilized to see what meetings are occurring, even when you cannot see any meeting details. Then, in a second article, we will look at how the change-tracking mechanisms within Google Workspace applications for spreadsheets and documents can reveal intention and coordination among those who wrote them.

These techniques may be of interest to *2600* readers in organizations that make use of the Google suite of online applications (Google Workspace and related names), or similar cloud-based document management and editing platforms such as Microsoft 365.

The Google suite of applications, like any modern cloud-based software, changes from time to time. I tested the methods described here while writing this article and found that some things had changed since I first observed the behavior - and things can be expected to change again in the future.

About Google Calendar

This article is about Google Calendar. This is the calendaring application in the Google suite, and it is typically accessed via a web browser or a native app on a phone or tablet. The techniques described here have only worked for me via a web browser, at the time of writing. Google Calendar (sometimes shortened to GCal) lets you keep track of your appointments and contacts. It also lets you send and receive calendar invitations to other people, get reminders of appointments, set your working hours, and so forth.

Google Calendar has great interoperability with other calendar apps, which facilitates scheduling of meeting times with attendees in multiple time zones. It also interoperates with other Google suite elements, such as Meet (for audio/video calls), Drive (to share documents), and others.

There are millions of people who use Gmail and can utilize Google Calendar with their regular Gmail login. My focus in this article is on the many thousands of organizations that have adopted the Google Workspace suite of applications. These organizations typically use some of their own Internet domain space to point to Google-operated systems so that their email addresses, documents, etc. are within a Google-hosted enclave, but with their own organizational name, branding, policy, etc.

First, let's get a general description of how Google Calendar is used within organizations. Then, I will share two personal stories, along with an illustration. This first article concludes with some advice on how to avoid information leakage via shared calendars.

Google Calendar Use Within an Organization

The basic scenario, which is typical of organizations that have adopted the Google suite, is that default settings hide your calendar from outsiders. For example, people who are not part of my organization will not be able to see my calendar or calendar events, and even if they are signed into Google with another organization, they won't be able to see my free and busy time.

Within my organization, by default colleagues will still not be able to see details (such as the title and description of an event in my calendar), but they will be able to see my free or busy time - that is, a view on what parts of my days are booked with calendar entries, and what parts are free. This is a very useful feature, since it helps find a meeting time that is open for all parties.

An "organization" in this context is usually associated with one or more Internet domains or departments that have chosen to adopt the Google Suite. For the scenarios I'm describing here, consider a fictitious organization like 2600meetings.net.

To adopt Google Workspace for the organization, the domain administrators of 2600meetings.net might set up Google as an email handler for the domain (by assigning MX records in the DNS and a few other setup steps). Organizational employees or designated members/affiliates would get a Google login to the 2600meetings.net application space in Google.com: mail, document sharing (via Google Drive), the

suite of productivity applications (documents, spreadsheets, presentations, etc.), and a plethora of available add-ons, including some from non-Google providers.

The result is that employees of 2600meetings.net, and anyone else assigned a login to the Google portal for the organization, will be able to utilize whatever Google services are set up for them. They can even utilize the Google login to authenticate to other services (this also works for people using the regular free Gmail.com service).

The administrators of the organization's Google domain can choose which extra applications are available to their organizational users, as well as some default settings and restrictions. For example, document sharing with outside parties might be prohibited. Or a company-wide email signature might be added to outgoing emails. Or a company might even use their own authentication system (via OATH2 or a similar protocol) rather than letting people login with a Google credential - thereby tying that Google identity more closely to the organizational identity. Options like these help an organization customize the Google Workspace experience to meet its needs.

For the Google Calendar app, what I have seen is that calendar sharing within organizations allows anyone to see free and busy time by default. Sharing of additional details, like the event description, location, and other attendees, must be done intentionally by the calendar owner. No calendar details at all are visible to outsiders.

This set of defaults makes great sense for setting up meetings within the organization. There is even more granularity available, such as to assign rights to fully manage someone else's calendar (for example, an office administrator might need to set up meetings for the unit's head, and assign meetings to others in the group).

Here's the thing: Visibility of free and busy time can disclose information about who is meeting together. When physical rooms are scheduled via the calendar (which is another feature), even more inferences may be made.

Example 1: Sleuthing to Find Out When Meetings Occurred

I'll tell two personal stories where unintended information disclosure via Google Calendar happened. In this first story, I had applied for a job in the same workplace my spouse is employed by. It's a large organization, with over 10,000 employees, staff, and others who all utilize the same Google-managed application suite.

My job application had been languishing. I had been interviewed but didn't know whether another candidate had been selected. We knew who was on the search committee, and the name of the hiring official, but none of them were in the same department as my spouse. The search committee members worked in different departments, including the human resources (HR) department.

Google Calendar sleuthing to the rescue! Might we see indications through free/busy time whether the search committee had met after my interview? Or whether there was a meeting that included the hiring official?

In this situation, one of the people who might have also been a candidate already worked for the organization. Could we find out whether they had been interviewed?

We found that just by my spouse's viewing of free and busy time, we could get insights into the communication among search committee members.

There are two ways of doing this in the Google Calendar application. For quick investigations, just set up a test meeting and invite the people you are interested in. When you view "More Options" (or similar) in the test meeting, select "Find a time" (or similar).

You then get a side-by-side view of available time for whoever you invite - as many as you invite.

You can even see free/busy time in the past. This is key: if you want to find out what people did in the past, take a look at past meetings. If you want to find out who they were meeting with, just invite all those people to the test event and GCal will happily show where calendars were aligned in the past.

Of course, you should not actually *send* an invitation to those people. You just want to see when they were all scheduled at the same time, in the past or in the future.

Another way of sleuthing calendars is to use the Google feature to "Add a calendar" to your calendar view. Instead of an individual meeting, this lets you see a group of calendars, all color coded, for whatever range of times you select. Within the web interface to the calendar app, you can navigate backwards and forwards in time just like if you were trying to make a new calendar event invitation, looking for alignment of the calendars you are interested in.

In my situation, we found that the top administrators, and all the HR people, had

their calendars set to be non-visible to others within the organization. Their calendars could not be viewed, and there was no indication of free or busy time.

However, other people on the search committee had their calendars available for viewing. We looked back in time to the day of my telephone interview, and could see them all lined up, in the same "busy" block of time, for my interview.

It was then easy to look for other times they were lined up and make an educated guess that those were the days/times for the other interviews. Scan forward a week or so, and we could see when the committee had likely met to discuss the candidates.

Did they interview the inside candidate? It looked like they didn't - the inside candidate only had occasional overlapping meetings with some search committee members.

What about meetings involving the administrative team, when a candidate would be presented to the hiring official? Well, we could not see the top administrator's calendar, nor anyone in HR. But there was someone who reports directly to the top administrator on the search committee, and their free/busy time was available. Also, we found that the room where the search committee met was in the calendaring system - so that people could book the room for their meetings.

We were able to infer the search committee had met, that the internal candidate was not interviewed, and that the search committee had not yet had a meeting to present their recommendation to the top administrator. All of this was simply by looking at the alignment of free/busy time for those people who had made it viewable across the organization.

Example 2: Sleuthing Collusion

Another example of sleuthing via shared calendars occurred when I and some other people in my workplace suspected that a group of coworkers was colluding on ways to damage the broader organization. Without going into detail, the basic situation is that we had a big membership organization, in which people from multiple other organizations collaborated.

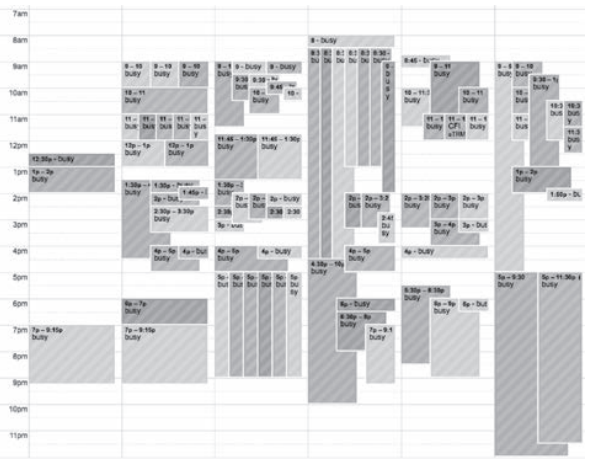
We had a neat Google Workspace setup, where everyone in all the constituent organizations had access to the same shared platform: calendaring, documents, etc. But everyone had a login and email associated with their own organization (functioning as a sub-organization within the Google space).

Here's a made-up example to illustrate. In the *2600* context, you could imagine a single Google domain for 2600meetings.net, and then people in Austin would have austin.2600meetings.net or austin2600.2600meetings.net (or even weareaustin2600.org - they don't need to share the same top-level domain).

This type of setup, in my situation, let people create invitations via Google Calendar with people from across the whole broad organization. We could also share documents and other activities on the Google platform. Very convenient.

When my coworkers and I suspected there had been some meetings among people working against the broader organization, we used the same method as above to look for alignment in calendars, across several people. We didn't have access to see all the calendars, but we could see enough. This also served to discover a few people who we were not sure were part of the collusion or not, and rule out some others.

Since one of the collusion meetings occurred right after an in-person meeting that was publicly known, we even knew where this took place - all without being able to see details of anyone's calendar events. Some people's calendars were completely unavailable, just like the top administrator in my earlier example, so we couldn't know for sure whether they were involved or not.



Aligned free/busy time for a group of people

All this sleuthing yielded precious insights into what had been happening. Rather than old-school surveillance (following people around, secret cameras, phone taps, looking through trash cans...), it was easy to make reasonable inferences of what had been happening simply by using the Google calendar to see free/busy time.

Preventative Steps

Shared calendars are very useful, and the sleuthing I described doesn't involve using calendars in a way they were not intended for. No privilege escalation is needed, and no workarounds.

However, using calendars as they are intended within an organization results in information leakage that may be unintended. Did the search committee want it to be possible for meetings and deliberations to be inferable across the organization? Including whether the incumbent candidate had received an interview? Surely not. Similarly, the collusion meeting mentioned above was in fact a secret - its very existence was withheld from close colleagues who attended an earlier meeting. But by looking at calendar alignment for those who made their calendars visible, the existence and partial attendee list became visible.

This creates a situation where the convenience and utility of making free and busy time visible is offset by the need for basic operational security: where people are and with whom they are meeting. Those with higher needs for operational security, such as administrators, human resources personnel, and others in sensitive or leadership roles may well choose to lock off their calendars from others in the organization. This makes it harder to schedule a meeting or other event; emails, phone calls, etc. will be needed to ascertain when all parties are available.

Whether this tradeoff is worthwhile depends on the role of the people involved, the size of the organization, how spread out people are, sensitivity of organizational activities, etc.

All that said, there are clearly some implications that anyone using a shared calendar, or managing an organization's calendar settings, should consider.

The domain administrator should select defaults deliberately and ensure everyone getting an account is informed of these defaults and how to change them.

Domain administrators should utilize an explicit off-boarding process for people who leave or change roles, so that any access they have to the calendars and other applications is disabled.

Individuals should not open sharing across the whole organization, unless they are sure that is desirable. Consider the number of people within the broad organization, and then consider how many have legitimate need to access any of your calendar details.

Consider a "least privilege" approach to calendar sharing:

By default, no sharing or visibility of a calendar to anyone.

- Free/busy time viewing should be enabled on a need-to-know basis for correspondents and close organizational members (i.e., same department, boss, etc.).
- Full calendar details should only be available to trusted individuals.
- The ability to make edits/changes to a calendar should almost never be granted, except where it makes organizational sense (such as an administrative assistant who needs to schedule meetings for other people).
- Calendars for rooms or other resources should only be available to people with a legitimate reason to use that room.
- Review your calendar sharing settings from time to time. Perhaps sharing was enabled with individuals for particular projects or collaborations and should be removed after the collaboration is done.

I hope this overview of Google Calendars has been helpful to readers. I've been using Gmail and associated tools for 20 years and have been a domain administrator for several large and small organizations, as well as an end-user in organizations I worked for. Information leakage via shared calendars is something I've observed frequently.

The convenience of online calendars is undeniable. The risks of unintentional sharing are important considerations for anyone utilizing such a service and, as with all tools, it's important to consider these risks when making decisions about how to configure and use the tool.

I LOVE SMART WORKING

by blue_elk934

"Raise your hand if you want remote working to last forever."

This question could be asked to pedestrians paying attention to their smartphones or in a post where an elaborate answer is replaced by a heart, a bulb, or a clap. In 2020, I read a LinkedIn post that listed all the advantages of remote working. In 2020, COVID severely affected Italy and, for this reason, one of the first measures enacted was the massive implementation of smart working. It is not surprising that most people happily approved of this decision.

Together with the numerous advantages of smart working, it must also be considered that the pandemic was a tempting opportunity for some bad guys. I want to imagine these guys as if they were in a restaurant. I'll give an example:

Starter: understanding the victim's network infrastructure

Main course: entering the victim's infrastructure network by phishing email for the employee

Second dish: once inside the victim's network, launching an SQL injection to disclose the employee's ID

Side: finding out the managers' emails, telephone numbers, and those of other important people

What about the dessert? There you go: a ransomware that could knock out the enterprise!

My example could be funny for most people, but it's an unfortunately true story. In 2020, the information technology attacks increased by 12 percent. In particular, there were attacks with impacts of "high" and "critical."

In a large part of this alarming percentage, many attacks were caused precisely by:

- The use of personal and non-corporate devices (laptops, smartphones, etc.) (the so-called BYOD - Bring Your Own Device)
- Naive employees attracted by phishing emails who downloaded dangerous attachments or entered company login credentials
- The inadequate security of home routers played a fundamental role (for example, using WPS and WEP ciphers)
- Employees exchanged emails containing top secret data without using cipher email plugins.

Some people may think that this situation was due to the naivety of the employees. However, the companies should have invested more into areas concerning security.

I came up with some ideas:

- First of all, it is important to give companies the opportunity to invest (with tax advantages) in secure fields in order to train employees and enable them to protect themselves from these cyber threats. If companies do not have enough resources to invest, the government should intervene through state contributions.
- Have employees use only company devices, avoiding the so-called BYOD.
- Also involve schools in the training process, because students are more technologically literate than their parents (the employees). It could be an opportunity for discussion, dialogue, and greater awareness of cyber threats.
- Employees should be allowed to report safety issues quickly and easily - every minute counts!
- The use of IDS (Intrusion Detection System) that monitors the behavior of the corporate network.
- Also, simulating calls to employees (social engineering) and ad hoc phishing emails would be useful to understand the degree of "naivety" of employees.

If smart working is the method of working in the future, we need to intervene immediately with awareness and tenacity!

After these years of the pandemic, I think the time has come for the so-called renaissance of cybersecurity to occur in the world. This is a great opportunity for a profound dialogue on this issue that can lead to greater collaboration between computer experts avoiding vanity and popularity, that popularity existing just because you have a resume full of semi-series computer certifications and 5000 connections on Linkedin!

EFFecting Digital Freedom

by Jason Kelley

Filter Bots Stifle Your Speech

Filters are common on online platforms. But anyone who's been put in "Facebook jail" or had their Twitter account dinged knows that these automated filters can't easily determine whether a post actually breaks community standards; they can't check for irony or humor, they miss context clues, and they simply aren't cut out to understand the nuance of written language. What's more, revelations from the "Facebook Files" have shown that at least that platform has a special program, dubbed "cross-check," which gives some "VIP" users a near-blanket ability to ignore the community standards entirely.

Unfortunately, filters are having a bit of a moment in Washington DC. Though not explicitly calling for filters, the "Kids Online Safety Act" would require platforms to limit certain types of legitimate speech - like conversations around substance abuse - from being shown to people below a certain age. Companies that can afford to - the big players - will no doubt use their filters to comply, and either ensure that users who are affected by the law see little to no discussion of the topics that are verboten. The types of content targeted by these bills are complex, and sometimes dangerous - in addition to substance abuse, the law lists discussions of suicide and eating disorders - but discussing them is not bad by default. It's very hard to differentiate between minors having discussions about these topics in a way that encourages them, as opposed to a way that discourages them. What's perhaps worse is that the bill vaguely lists "other matters that pose a risk to physical and mental health of a minor" as content that should be limited. As we've seen in the past, whenever the legality of material is up for interpretation, it is far more likely to be banned outright via oversensitive filters, leaving huge holes in what information is accessible online.

Likewise, Congress is considering a filter mandate bill that would task the Copyright Office with designating technical measures that Internet services must use to address copyright infringement. Right now, sites like YouTube, Facebook, and Twitch use filter tools voluntarily, to terrible effect, but they are not doing so under any legal requirement. But corporate copyright owners complain that filters should be adopted far more broadly. They point to one of the conditions of the legal safe harbors from copyright liability included in the Digital Millennium Copyright Act - safe harbors that are essential to the survival of all kinds of intermediaries and platforms, from a knitting website to your ISP. To benefit from safe harbors, sites must accommodate any "standard technical measures" for policing online infringement - essentially, they have to implement an agreed upon mechanism for removing copyrighted material.

These measures were meant to be "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process."

As a practical matter, no such broad consensus has ever emerged, partly because the number and variety of both service providers and copyright owners has exploded since 1998, and these industries and owners have wildly varying structures, technologies, and interests. What has emerged instead are what you see today: privately developed and deployed automated filters like YouTube's ContentID, usually deployed at the platform level. For decades, influential copyright owners have wanted to see those technologies become a legal requirement for all levels - and the "Strengthening Measures to Advance Rights Technologies Copyright Act" is the latest in a string of bad proposals that would do so. The law would require service providers to adopt "designated technical measures" to police potentially infringing activity - i.e., in many cases, filters - approved by the Copyright Office - despite the fact that these filters aren't able to distinguish between lawful expression and copyright infringement, and that they regularly punish both people who make their living sharing videos online and everyday users.

There are tens of thousands of examples of these oversensitive and inaccurate automated takedowns. Some highlights, which we've memorialized in our Takedown Hall of Shame, include YouTube's system flagging *static* as copyrighted material *five separate times*. Another ironic example: the company flagged video from a New York University Law School panel where *the point* was to explain how song similarity is analyzed in copyright cases. The flag was eventually removed, but only after NYU Law reached out to YouTube through private channels, attempting to get an answer to its questions about how YouTube's filter system, Content ID, and takedown policy worked.

The problem isn't just on YouTube: Facebook heeded a takedown request from Sony and muted a musician's own video performance of Bach, because the platform's filters can't tell the difference between different classical musicians playing public domain pieces. The company only backed down when the musician took his story to Twitter and then emailed the heads of Sony Classical and Sony's public relations.

The problem isn't just copyright filters, of course: in an attempt to battle COVID-19 misinformation, Facebook also kicked the page for Oakland-based punk rock band Adrenochrome offline. (Adrenochrome is a word popularized by Hunter S. Thompson in two books from the 1970s, but which gained recent popularity amongst conspiracy theorists.) The site renewed, then removed the page again, and only restored it after we reached out to them.

Twitch has also had its filter failings: when the live streaming site hosted Blizzard Entertainment's gaming conference BlizzCon on its official gaming channel, it replaced a live performance of Metallica with something resembling the music from an ice cream truck - all while leaving the music intact on Blizzard's own Twitch stream. Given that Metallica put themselves on the frontlines of the fight against digital music downloads in the early 2000s, launching high-profile lawsuits and testifying in front of Congress, it's no surprise Twitch was so twitchy.

So if filters can't tell if one thing is just a copy of another thing, how can they tell if something is definitively hate speech, or a promotion of substance abuse (for example)? What we've learned from the long, painful history of automated copyright filters is that *filters don't work*. And mandates for filters don't just stifle speech, they also have downstream effects on the potential for new providers and platforms to challenge the big incumbents. If a filter mandate were made law, the largest tech companies will find it easy to implement whatever the standard technical measures are (likely using something akin to their current measures, but turning the "filter" knob up to 11). The burden of laws like this falls mainly on users, and small and medium-sized services.

Faced with these criticisms, government officials and politicians ought to back away from these ham-fisted plans to regulate online content through mandated technical measures. But it will take people like you to convince them. We hope you'll join us at the Electronic Frontier Foundation in fighting back against the filter mandates - before the Internet gets remade to serve the whims of today's politicians and the entertainment industry.

The Phreak's Field Guide to Identifying North American Phone Switches, Part Two

by ThoughtPhreaker

DCO

The red-headed stepchild of the switching world; there's really no other way to put it. Siemens bought it, discontinued it in the early 90s as an end office (it survived a little longer in production as a long distance switch), and gave the EWSD the capability to interface with DCO line frames and remotes. Genband bought the DCO and EWSD designs, and made their softswitches do the same thing!

- To this day, the maintenance processor for every DCO in the network is a DEC LSI-11, as were the original call processors for the system. As a result, Siemens kept an original PDP-11/70 in service for software development until 2000 before replacing it with a Mentec clone. At some point, newer call processors (as in, the ones you get when you pick up your phone rather than hit a key on the switch's serial consoles) were ported to a more recent hardware architecture. Given the lifespan of telecom gear, it's likely that in some parts of the U.S., you can pick up your phone and still get a PDP-11 at the other end.
- Won't support GR-303 loop carrier without a third party add-on.
- Early incarnations supported the strange coin detect feature the ESC used without pulling line current. For whatever reason, this was dropped later in its life.
- Commonly (almost exclusively) does AIS-style announcements.
- There's two different models of DCO: CS (toll tandem) and SE (Small Exchange). Both are relatively low capacity switches, so for that reason, you'll most likely find the DCO-SE when you're wandering around the very rural parts of ex-Contel/GTE territory. As for the CS, a lot of small long distance carriers bought these in the 90s. If you can dig up some small toll providers, they might still be using them.
- DCOs have a stutter dial tone with six bursts of dial tone instead of three.
- Has a tone used for confirmation, partyline ringback, etc. consisting of short, 100 millisecond pulses of high tone. No other switch type seems to use this.
- When pulsing your first rotary digit, there's no burst of dial tone when you're done.
- Completely ignores fourth column (A, B, C, D) tones.
- Much like when dialing with the switch's predecessor - the ESC - dialing * in certain places lends itself to odd circumstances. As the final digit as a CAC+0 call (as in, say, 101-0288-0-212-555-121* - it's important that it be the last digit), it appears to put the call through! What it's sending isn't entirely clear. In SS7, a destination phone number is sent using binary-coded decimal, as opposed to plain ASCII in ISDN-derived protocols, so the only possible combinations to send are 0 through 9 and A through F. With a * as the final digit of a local call, strange recordings will occasionally play, such as permanent signal (if you'd like to make a call, etc.).
- Like the GTD-5, its processing of the # key isn't entirely clear. For example, 101-0288-0# won't tell a DCO to stop waiting for digits and to put the call through. Instead, it generally seems to keep waiting for digits, as if considering it part of the destination. Unfortunately, this makes CAC + # (as in, just the carrier access code; no called party number) impossible to call, severely limiting some fun things that can be done with long distance tandems.
- Flash behavior on coin (and possibly home) phones isn't entirely clear either. For example, on a CO-controlled coin line, flashing after the switch releases a call will make it send coin return voltage, but only keep someone on silence.
- Really hard to find! Playing with a DCO up close is a rewarding experience for anyone keen on introducing unorthodox input into the phone network. Considering many of them only serve far-flung rural areas, this requires planning, the willingness to drive a considerable distance, and the ability to find a payphone once you get there. Street View is your friend, kids....

Ringing number: 337-666-9009 (CNAM returns CENTURYLINK; likely unused pair in the central office)

Remote call forwarding prompt: 218-834-9934 (ETC Digicept providing voice samples)

Unknown dialtone: 815-537-0006 (beware that this doesn't supe. Being able to transmit over the toll network before supe is a whole other topic, but a carrier like MCI/0222 (read: not Worldcom/0555) is ideal for this. What it's looking for isn't entirely clear, though; the switch will wait for a seemingly infinite amount of digits before inevitably throwing you to an error recording. At the recording (and this isn't a hardware fault, they all seem to do this), the switch will arbitrarily hang up and call the recording back - or sometimes just throw you off the call entirely. Given how long it waits for so many digits (this would really make more sense

with a passcode rather than a destination), it's possible this is another way the switch has of handling call forwarding.

EWSD

Outside the U.S., the EWSD, Siemens' pride and joy, is everywhere - from Argentina to Iran. Inside the U.S.? It just comes up here and there. What it's like depends pretty heavily on who runs it, though. AT&T has trouble understanding *how* to run it, and it's occasionally poked at by their techs for that reason. In any case, their dialplans aren't exactly bulletproof. Verizon tends to be a little better about dialplans (some of them even have custom prompts on their Cognitronics machines!), but they have their own weirdness; in this case, a CAC - 0110. Instead of sending you to a long distance carrier, it originates whatever you put next locally.

- In a strange gesture of switch apathy, AT&T's EWSDs do pretty much no checking of your destination numbers. As a result, you can route calls to almost anything of your choosing like 0xx codes, and it'll put it right through! No weird routings, no CACs needed, no workarounds. Let it be known that nothing good ever came from talking shit about your phone switches.
- The 0110 CAC seems to be a thing on all North American EWSDs, even the independent ones. Curiously, on most other switch types, the ability for someone to take advantage of this is hit and miss at best.
- The EWSD stands as one of the only switches (the DMS-100 being the other) to have two different types of ringback tones. As far as I can tell, this has to do with the generation of hardware. Paul Timmins, the guy who runs Telcodata, was nice enough to post the install dates for most of the Ameritech EWSDs in Michigan. On that list, one clear pattern starts to come up: all the Type 1s were installed sometime before 1995, with the first Type 2 showing up in 1993. Unlike some of the more common switches, the EWSD never really became popular until the mid 90s, so the vast majority, partly thanks to DCO conversions and CLECs, are Type 2s. Type 1s only seem to occasionally show up in RBOC exchanges near the Midwest and eastern parts of the U.S.
- While EWSDs seem perfectly capable of generating milliwatts (they can all do more complex 105-type tests), almost none of them do. Instead, they have a test set that sits on an analog line, and answers with a 102-type milliwatt. In between the silence, if you send it touchtones, you'll get all sorts of weird tones.
- When getting an error recording, the default behavior is to let an announcement play once, and quickly hang up.
- The digit "D", typically rejected by most switches in one way or another, will translate to 0 on an EWSD.
- Like the DMS, some EWSDs have been noted to make soft clicking noises as calls progress. In this case, they tend to be less subtle than the DMS's. While nobody seems to know for sure what causes this, I have a pretty strong suspicion it's caused by how the EWSD handles lines on loop carrier systems.
- Our resident EWSD resident, JmanA9, was kind enough to get some information on the EWSD's test functions. The ringback circuit, surprisingly, is an actual, physical test device that physically removes you from the line card, and takes over the function of running your phone line. This function is used very rarely, but is especially unusual on a switch that's preferred for all-ISDN networks, like some in Europe.

(Type 1) Ringback tone: 203-453-0994
(Type 2) EWSD Milliwatt: 541-384-0100
Ringback tone: 608-663-0126
Reorder tone: 608-663-0130
Remote call forwarding prompt: 888-345-8672, pick any switch from the IVR.

AXE-10

Like the metric system or a sensibly-sized pickup truck, what's common to the rest of the world is somewhat uncommon to the United States. The AXE-10 is no exception. While it holds the title of being the world's most popular phone switch, it's little more than a footnote in the North American network, with many being replaced by their more popular counterparts as quickly as the early 90s. In former US West and Southwestern Bell regions however, a moderate but persistent crop of AXE-10s stands firmly in place.

A certain Greek AXE-10 running part of Vodafone's network holds a particularly unique place in telephone folklore, having been host to a rootkit written in PLEX, the switch's proprietary programming language, that concealed the wiretapping of the Greek prime minister and several other officials. Wikipedia's write-up of the story gives an air of mystery to the incident, as well as the cringeworthy opsec failure that led to a suspect being identified in the case.

- Quite a few of the ones in the U.S. are near the Mexican border. This may be because Mexico uses so much Ericsson gear; AT&T will occasionally call on Mexican switch techs to help them fix stuff.
- Unlike other manufacturers, Ericsson appears to have stuck to developing in-house CPUs until a relatively late date, with off-the-shelf components being introduced into APZ (main CPU) designs towards the late 90s.
- Like the DMS-100, it seems to be married to an announcement machine. As far as most non-softswitch designs are concerned though, they stick out like a sore thumb. Unlike a lot of the non-AIS announcements, they never, ever ring, and they're always very clean sounding. Ericsson

made it fairly easy to let you directly upload recordings.
- Impatient! Only has a five second waiting time for partial dial conditions.
- Reorder timing is slightly faster than most American switches, but not as fast as a DEX-450/600, one of the toll switches occasionally found in the ex-MCI (0222; the non-Worldcom one) network.
- When dialing, the fourth column DTMF digits A, B, and C mostly seem to react as if you dialed a *, depending on where it's inserted. D, however, is another story.
- Can drop you to an announcement *fast*. In the fraction of a second that most switches can bring you to reorder, the AXE-10 can start up a recording.
- Typically is filled with a bunch of strange tones in its test ranges, like out of spec milliwatts (next to real ones, no less) and seemingly arbitrary 815 hertz tones.
- AT&T AXE-10s allow NPA-0xx-xxxx.
Ringback tone: 970-887-0051
Busy tone: 405-382-9154
Announcement: 405-382-9137
Weird tone: 325-235-0500
Off frequency milliwatt?: 325-235-0514

CS-1500/C15

What do you get when you put a DMS-10 CPU in a 2U rackmount box and slap some ethernet interfaces on it? A CS-1500! Not much more to say really.
- Like the GTD-5 and the EWSD, this switch is married to an AIS; pretty much all installs come with an Innovative Systems APMax. The increasing number of APMaxes being paired with DMS-10s has made an already tough exercise of telling the two apart even harder.
- Telling a DMS-10 and a CS-1500/C15 apart can be really hard; they use very similar software, CPUs, and even the same line frames. As far as I know, the only way to tell them apart is to try finding a 105 type test, or possibly a loop; independents, where you'll most likely run into this scenario, will likely put a 105-type test in a place like 9105 or 1105. 9108/9109+1108/1109 is a good place for loops.
- The stutter dial tone you get on a CS-1500 when dialing *67, *82, etc. will be normal speed; the DMS-10's is noticeably slower than the speed most switches play it at.
- Does not have the offhook tone with the weird modulation sound in it like the DMS-10's.
- Cannot support dialpulse trunks, among a few other trunking arrangements the DMS-10 does.
Remote call forwarding prompt: 828-297-9999
Reorder tone: 906-524-9966

CS-2000/C20

The CS-2000, as Nortel's internal hardware guide puts it, isn't a new product, but effectively a new hardware revision for the DMS-100. The software was ported from SOS (Switch Operating System; Nortel's proprietary RTOS) to Linux, and a virtual machine layer took the place of some of the hardware. The CS-2000 also runs on PowerPC 750 and 7410 CPUs, much like the newest DMSes. The C20 is a redesign of this hardware by Genband to fit into an ATCA blade chassis, along with a completely different source of call progress tones.
- In ATM mode, this switch is quite literally indistinguishable sounding from a DMS-100. Supports many of the line frames and peripherals of the switch as well. Despite being ATM, internal signaling channels will still be done via IPoATM cells.
- In IP mode, the CS-2000 uses the same tone set as the DMS-100 in three-way mode. While it still supports DMS-100 hardware, some installations will do weird things, like fade out as it disconnects, as if there was some sort of packet loss concealment. Other installations have a subtle, but still noticeable level of latency.
Remote call forwarding prompt: 610-799-9900 (this isn't the best reference; the exchange itself is a DMS-100, the CS-2000 seems to be for an affiliated cable company)
Non-working number recording: 620-371-6111 (uses DMS-100 EDRAM circuit pack, stock announcement)
Non-working number recording: 702-722-6222 (uses CS exclusive Audio Server, stock announcement. Note that very new Genband C20s may use a different announcement, as evidenced by the very last of the AT&T 1AESS to C20 cutovers in 2016/2017)

Safari C3

This switch pops up occasionally in small patches. Some west coast Comcast, some Charter, some Atlantic Broadband. The switch is optimized for voice over PacketCable networks, and can be identified by a fairly distinct ring, and its breathy voiced stock announcements.
- This was very hastily thrown together by Cedar Point, a headend equipment manufacturing company, before eventually being acquired by Ribbon/Genband. This will occasionally result in weird feature limitations. For example, it'll support ISDN PRIs natively, but only NI-2 flavor PRIs. Or, as its manual cautions, if you insert a high density media gateway card into the last slot on the chassis, the switch will overheat.
- As of 2021, while Ribbon appears to fully back the product, it's unclear who continues to run these. Changes in LERG, audible ringback, recordings, and other factors appear to suggest major cable companies are phasing these out. This would be consistent with the relatively short lifespan (less than 20 years, whereas some DMSes have continually run since the 70s, albeit with severely evolved/upgraded hardware) softswitches seem to encounter. A cursory search

for some press releases suggests South American cable operators might still be using them. A search on Shodan revealed one on the public Internet operated by TV Rey (as in, TV King. I can't say it with a straight face either), a Mexican cable operator.

When I first started writing this, this is where I put numbers for the C3. Today, any secrets these awkward boxes of overheating breathy voices held were taken to the grave along with the example numbers I wanted to give out.

Taqua T7000/OCX

One of the many designs from the telecom boom (and bust) of the early 2000s. The switch was initially embraced by small companies, but seems to have fallen flat on its face, like a lot of other switches introduced at the time. What differentiates it from products like the Coppercom CSX and Gluon CLX is it survived, still retaining an audience within Sonus/Ribbon's halls.

ANAC: 229-236-0102

Remote call forwarding prompt: 760-928-5900

Remote call forwarding prompt: 806-350-0099 (alternate prompt set)

- The call forwarding prompt sounds very close to the DMS-10 and CS-1500 call forward dial tone, but listen closely to the way it comes on. There's two bursts of stutter dial tone, a (relatively) long pause, and another of those two bursts. There's also a few other differences, like stock recordings and its reaction to keys like *.
- Stock recordings sound weird and fucked up for some reason. Some iterations of this switch seem to have a completely different prompt set.
- Incorporates a SPARC machine running Solaris, though its role isn't entirely clear.
- Really hard to distinguish T7000 and 5ESS ring.
- Architecturally, all cards on the T7000 (or OCX; same thing) are designed to be functionally independent of each other - the resources needed for billing, features, switching, etc., are all self-contained.
- Typically run in small patches by Paetec/US LEC, Allstream/Electric Lightwave CLEC properties (the former apparently only for IP traffic; they appear to be run alongside 5ESSes), but relatively rare overall, with a handful already being replaced by the early 2020s. Getting a chance to fondle T7000 dial tone has been anything but easy.

MDX384/IGX/HDX/SLICE

Built to be very modular, and because of their unusual design, wind up in very strange places. Their very low capacity (IGX supports 96 lines per shelf, MDX384 supports 384 lines) is ideal for places like ghost towns, and fanless operation makes them ideal for extreme parts of Alaska and the Yukon. They're popular as military PBXes as well, having survived a number of tours in Iraq. The SLICE, seemingly a 1U version of the IGX/HDX - or at least running the same software, has gotten its rite of passage into the U.S. military. In some places where HDXes have historically been used, they've been swapped out with SLICEs for portability reasons. Some FTTH deployments in the middle of nowhere are done with SLICE hardware too.

- Despite their age and different generations of CPU cards (the IGX is believed to run on a 68k), the IGX, SLICE, MDX, and HDX appear to be all be running ports of remarkably similar software.
- Card stock between the HDX, IGX, and MDX are interchangeable.
- Each shelf in an HDX switch can have a maximum of 512 timeslots assigned to it, with additional shelves being connected together with a ribbon cable to allocate up to 4096 channels on the system's TDM bus to up to 32 shelves. This limitation is suspiciously similar to the H.100 bus used in hardware-accelerated telephony cards for computers, with its maximum of 4096 timeslots, 32 independent serial data streams, and its big, IDE-like ribbon cable used to link cards together.
- The HDX has been described as both a softswitch and circuit switch before. Redcom's marketing tards need to make up their damn minds. Both generations work on circuit packs, the 90s generation of which look like they're using a few *very* old designs with hand-woven PCBs. It appears the presence of a TRANSip (media gateway) card is what qualifies it as a, uh, "soft" switch, an increasingly hilarious misnomer that switch manufacturers seem intent on abusing. By definition, a softswitch, such as Asterisk or CallManager, runs on off the shelf hardware. Nothing here, carrying a "next-generation" moniker for over 20 years or otherwise, meets this definition in the slightest.
- Has a BASIC interpreter on it! No, seriously.
- One of the few switches in the world to still support magneto phones.
- The integrated AIS sounds like the voiceover person had a stroke. This is apparently a design choice associated more with newer Redcom systems, though not absolute. While an IGX can still sound like it lost all feeling in its throat, it's far more common to use a scratchy sounding announcement card, more often than not with the voice of the switch tech in some far flung place with an equally scratchy carbon mic.

Supervision test: 831-389-9103

AIS report: 831-389-9108

Loop: 907-293-1108/1109

Announcement via older IGX hardware: 907-293-9990

GTD-5

What do you get when an obscure phone company designs obscure hardware? The GTD-

5 EAX! That's a "General Telephone Digital #5 Electronic Automatic Exchange" for those of you who actually pay attention to acronyms. There's a certain saying in telecom: "one is good, two is great." Just to show they really were a phone company, GTE duplicated *everything* in the processor complex not just once, but twice. A single card has two processors running the exact same instructions and comparing them, while an identical card does the exact same thing. All the digital trunk cards on the system are likewise duplicated. Internally, the system communicates using 12-bit PCM words over a parallel bus, and runs on software written in a custom version of Pascal. Like some of the other designs such as the EWSD, the system has no announcement cards, and leans entirely on external equipment to generate any recordings. For that reason, most of these were sold with units from the Cognitronics company to make this happen.

Random facts:

- Around 2000, Lucent completely redesigned the GTD-5 switching network. Little is known about it other than, well, it exists and it's different.
- Like any good obscure switch, the GTD-5 will almost always let you dial 0xx codes. You don't need to put a CAC in front, unlike on a DMS-100, but probably won't be able to dial nine digit numbers. The tradeoff is the alternate dialplan for vertical service codes such as *67 on GTD-5s *will* generally block 0xx.
- The GTD-5 is more or less married to an AIS to provide any recordings in most configurations. Typically, these are run of the mill Cognitronics machines, but occasionally will be an ETC Digicept, a really old Cognitronics machine, or in some really recent cases, an Innovative Systems AP or APMax. However, some very old GTD-5s have actual, drum-style announcements. Mount Olive (217-999) is one of two I've ever heard equipped this way, and is living proof that the hardware even allows this.
- Some switches, most notably the GTD-5 in Logan, Iowa (712-644), seem to have strange, newer retrofits used to generate recordings with text to speech. This is incredibly rare, but might be a sign of things to come if more of the older Cognitronics boxes fail.
- Sometimes this switch will have a noticeable pause between certain tones, like offhook or stutter dial tone, even during off-peak times like four in the morning. It's unclear what causes this, but it might imply tone cadences are generated by non-dedicated hardware.
- Has a strange way of handling permanent signal (not dialing anything at the dial tone) conditions. Some have the announcement machine play something, some just give reorder, others a solid high (480) or low (480+620) tone, or even just silence. Sometimes you'll get a combination of all four. Always stay on after the reorder to be sure.
- According to Chuck, a seasoned GTD-5 tech, it may be possible to gain some insight into what software version a GTD-5 is running by the way it handles someone leaving their phone off the hook. It can be any combination of reorder, high tone, low tone, offhook tone, or all of the above. Supposedly though, there is no way to change what combination of these it uses in software. The most common way of doing things currently is to use all four (reorder, low tone, high tone, offhook tone).
- Outgoing voicemail system trunks, some of the most locked down outgoing trunks you'll find, tend to get ANAC, directory assistance, and other things most switches never, ever allow. This switch is *not* good at toll restricting! Some GTD-5s have adopted the peculiar behavior of sending offhook tone down voicemail trunks when presented with an SS7 message indicating all circuits are busy.
- The behavior of the # key as the first digit of a phone number is unclear. Where most switches assume you're using a speed calling code, the GTD-5 seems to wait for an unusually long string of digits, so long as the first or second digit isn't 1 in most cases. Notable exceptions to this are 0, 2, 3, 6, and 8; with 1 as the second digit, they'll keep listening.
- One of the few large CO switches to be designed (at least originally) for fanless operation. Newer hardware doesn't necessarily follow this trend.

Unknown older hardware generating offhook tone for a GTD-5: 712-374-1256

Feature recording via weird TTS thing: 712-644-1275

Remote call forwarding prompt via ETC Digicept: 906-341-9983

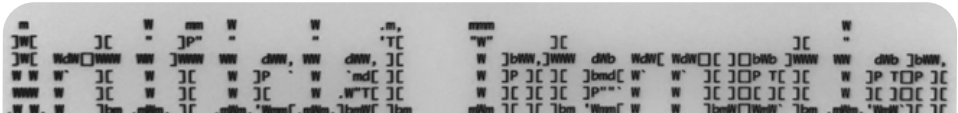
Remote dial tone: 231-773-9996 (for unknown purpose; doesn't look for a destination phone number)

Softswitches I Know Nothing About

Metaswitch [early/mid 2000s ATM + IP core Compact PCI softswitch: popular with the rural telcos who change their switch as often as their underwear. Later systems use an ATCA chassis rather than cPCI. Very common within larger LECs as a voicemail system or for IP trunking]: 406-347-4800 (voicemail), 503-266-1021 (ANAC)

Coppercom CSX [early 2000s softswitch design. Few survive now]: 517-436-9000 (ANAC)

Special thanks to: Scott from the Socal bridge, Scott from the not Socal bridge, the people who wrote the Wikipedia switch articles, dmine45 (maintainer of telephoneworld.org), Evan Doorbell, Paul Timmins, JmanA9, Jim Somerville's LinkedIn profile, Shadytel for keeping it as real as it gets, trmg. You guys seriously know your stuff! This article would've been a lot less interesting without your bits of wisdom to stick in here.



by Alexander Urbelis On the Signal-to-Noise Ratio Concerning Ukrainian Relief alex@urbel.is

This column left off discussing a humanitarian disaster that was ongoing in Myanmar and the need for empathy among strangers. Since then, Russia has invaded Ukraine, there is a full-blown war on European soil, and the world's nations, including finally the United States, have accused Russia of perpetrating war crimes.

The world has become familiar with the heartbreaking images of fathers pressing their hands to the windows of trains as a final valediction before their families, now refugees, are carried away and they must return to the frontlines to fight the Russians. We have all the seen the horror of a mother and her two children killed in plain daylight while crossing the street, we've seen images in the aftermath of a woman nine months pregnant injured by a bomb before her death and the death of her unborn child, and there are untold and unspeakable horrors happening to the people of Ukraine on a daily basis as Russia continues its siege and its indiscriminate and persistent bombing of civilian targets and areas.

As of the writing of this column, despite the supposed sophistication of Russian operators, the war has hitherto had very little to do with cyber operations. Though Conti, a ransomware gang known for both its excellent customer service and connections to the Russian government, vowed to support the Russian incursion by breaching and encrypting the data of Russia's detractors, this notorious bunch of threat actors quickly walked back that threat less than 24 hours after its utterance. Before they could, however, a Ukrainian security researcher released for public consumption nearly 100GB of Conti chat logs, training materials, and other internal documents.

On *Off The Hook* in March, we had the pleasure of hosting Emma Best of Distributed Denial of Secrets. DDoSecrets has published close to a terabyte of leaked Russian materials, from official documents of the Russian censorship agency (the Roskomnadzor) to troves of documents that relate to oligarchs' oil interests and Russian state-affiliated companies such as Transneft and MashOil. Also on *Off The Hook* as a guest was Karina Shedrofsky, head of research at the Organized Crime and Corruption Reporting Project. Karina and her colleagues have been tracking the assets of Russian oligarchs for years, and put together an interactive Russian asset tracker that sheds great light on the hidden assets of Russian oligarchs and the jurisdictions that provide them haven.

A concerning trend, however, is for the target of hacktivism or leaks to claim that the hacktivist groups responsible for the attacks are actually operating at the behest of a hostile foreign nation. Branding hacktivists in this manner is not simply misinformation or deflection - it could signal that those responsible for the actions are being classified as enemy combatants. When dealing with a country like Russia which has had no qualms on multiple occasions with targeting enemies of its state for poisoning and assassination, that is a scary classification for anyone to carry.

Indeed, from saber-rattling with nuclear weapons to clamping down on news media and protesters, Russia has been trying exceedingly hard to discourage individual or collective opposition to its illegal war and to prevent actively supporting Ukrainian relief efforts.

Around the globe, we are all wondering how we can support Ukraine, and our inability to do so has left us wanting. With this in mind, I have observed a curious trend in the Domain Name System (DNS) since the outset of the war. Right around the time that the hostilities commenced, I began to monitor and track domain names that contain the string, "ukrain*." That word stem would capture "Ukraine' as well as "Ukrainian" and other variations. Since the beginning of the war, I have identified thousands of new domains, with daily registrations peaking at around 500 at the outset of the invasion and then tapering off to about 125 new domains appearing every day in April 2022. Nearly immediately, however, I noticed a very significant spike in domain names about donating to Ukraine.

By way of our steady, old friend grep, it was easy to identify domains that pertained to donations, aid, relief, NFTs, and, of course, cryptocurrency. As of writing this column, there were nearly 800 new domains that incorporated strings relating to aid and relief together with the string "ukrain."

This is very much the type of gray area in which Russian operations thrive. Indeed, an often overlooked yet critical piece of understanding Russian politics is the role that Vladislav Surkov plays in advising Putin. Surkov was and is a manipulator who came from the world of the theater before rising to political power, holding the position of deputy chief of the Russian Presidential Administration from 1999 to 2011. Turning Russian politics into a shapeshifting mess of coalitions and ever-changing alliances and conflicts - and then letting it be publicly known that Surkov himself had artificially generated these coalitions and conflicts - was the Kremlin's tactic of keeping the masses confused, distrustful, and always questioning what was real and what was artificial.

Not surprisingly, on the heels of the invasion, there has also been an uptick in reports of donation fraud concerning Ukraine. Though many of these scams may originate on social media or via text message, much of the fraudulent activity will

eventually rely on a domain name to host content, harvest credentials, siphon credit card details, or otherwise act as some form of pass-through for data or communications.

From the perspective of Russia, these domains and the fraud associated can be beneficial to their war efforts on several levels.

On one level, decreasing the signal to noise ratio (or increasing the noise to signal ratio) serves Russia because this type of fraud, and the media attention that it generates, will cause ordinary persons to have misgivings about donating to Ukrainian causes or relief efforts out of fear of being defrauded. From a policy perspective, given so much may be riding on the Ukrainians' ability to withstand sieges and sustained shelling and urban onslaughts - which would require aid and relief to withstand - it is not inconceivable that Russia could be encouraging this type of behavior under the table or turning a blind eye to criminals who engage in such fraudulent activity.

On a deeper and more sinister level, if Russian actors were behind the fraud themselves, they would be accomplishing the goal of deterring others from donating resources to Ukraine while also absconding with the funds and resources that well-meaning persons from around the world intended for Ukrainian relief.

And on yet another - albeit less - sinister level, there are many domains that track to Russia, either by registrar, registrant, NS records, or IP addresses. And if these domains relate to ordinary Russians, as some of the Whois data indicates, and those domains are not fraudulent, then given the authoritarian crackdown on dissent - or even contrary dialogue to the Kremlin's official position on the invasion - then those domains and the persons behind them should be lauded as heroic.

But then again, going back to Surkhov's playbook, how do we know what is real and what is fake, what is charity and what is fraud, what is a legitimate humanitarian effort and what is a dangerous honeypot of a brutal regime? It is one thing to talk about the dissonance and difficulty of ascertaining fact and fiction and another thing entirely to see it. For that reason, I am dedicating some space in this column to listing Ukraine-focused domains with Russian connections. And while I encourage readers to exercise caution and discretion if they intend to visit any of these domains, I am also very curious about what information from and connections between these domains can be derived.

To that end, I encourage readers to reach out to me directly via Twitter (`@aurbelis`) if they would like to receive the full list of all newly registered and aid-focused Ukraine-related domains, and I wish you all, in the meantime, happy hunting.

Domain	Name Server	IP Address
Aboutukraine.info	ns1.beget.pro	87.236.16.73
Aidforukraine.site	ns2.reg.ru	194.58.112.174
Aid-ukraine.info	ns2.webhost1.com	91.236.136.57
Airdpukraine.shop	ns1.reg.ru	31.31.196.22
Cats-dogs-ukraine.com	ns2.fozzy.com	88.212.244.12
Charityforukraine.org	ns14.domaincontrol.com	178.248.234.146
Chernobylukraine.com	ns05.domaincontrol.com	178.132.201.54
Diplomukraina.org	ns1.eurobyte.ru	46.30.41.23
Donate-to-ukraine.world	ns4.nic.ru	195.24.68.29
Donate-ukrain.com	ns1.mchost.ru	185.105.110.4
Donateukraine.charity	curitiba.porkbun.com	78.40.217.96
Donateukrainenow.online	ns1.reg.ru	194.58.112.174
Donateukraine.online	ns1.nethouse.ru	185.84.110.85
Flowers-ukraine.com	ns2.beget.com	87.236.16.9
Forukraine.world	ns2.lighthosting.net	62.122.190.67
Freeukraine.site	ns10.uadns.com	185.165.123.36
Goodsfromukraine.com	ns45.domaincontrol.com	185.129.100.113
Handofukraine.online	----------	23.105.244.169
Helpsukraine.xyz	----------	23.105.244.169
Help-ukraina.space	blocked2.nic.ru	194.85.61.76
Help-ukraine.auction	pid2.srv53.org	94.103.188.153
Helpukraine.icu	ns1.he.net	81.28.13.179
Help-ukraine.website	ns2.reg.ru	31.31.196.4
Hosting-ukraine.com	ns.parktons.com	46.8.8.100
Iherb-ukraine.com	ns2.timeweb.ru	92.53.96.18
Ilyaukrainets.com	ns1.reg.ru	194.58.112.174
Interview-ukraine.com	ns3.nic.ru	89.104.84.244
Jewsprayforukraine.com	ns4.zomro.su	81.91.178.41
Legal-support-ukraine.com	ns25.domaincontrol.com	185.165.123.36
Lifeukraina.online	ns8.nic.ru	195.24.68.8
Market-ukraine.xyz	ns1.reg.ru	194.58.112.174
Much-ukraine.xyz	ns2.beget.pro	185.50.25.57
News24-ukraine.store	ns1.beget.com	87.236.16.13
Newukraina.com	ns2.masterhost.ru	90.156.201.101
Ngchildrenukraine.net	ns2.ukit.com	185.129.100.127
Osteology-ukraine.org	ns116.inhostedns.com	185.165.123.36
Polandviza-ukraine.com	ns2.parktons.com	46.8.8.100
Prayforukraine.space	ns2.hosting.reg.ru	31.31.196.4
Razonforukraine.com	ns1.hosting.reg.ru	31.31.198.124
Razonnforukraine.com	ns2.hosting.reg.ru	31.31.196.230
Russia-ukraine.com	ns2.beget.com	87.236.16.254
Saveukrainenow.company	ns3.nic.ru	91.189.114.21
Saveukraine.site	ns2.beget.pro	87.236.16.247
Saveukrainetoken.com	ns4.timeweb.org	92.53.96.222
Saveukrainewarefare.com	r.ns.arvancdn.com	91.218.247.43
Saving-ukraine.com	ns3.digitalocean.com	141.8.195.65
Sendflowersukraine.com	ns2.netangels.ru	185.93.109.240
Setukrainefree.com	ns1.hosting.reg.ru	37.140.192.220
Slavaukraine.fun	ns1.justhost.ru	185.22.155.64
Slavaukrainegeroyamslava.xyz	ns2.hosting.reg.ru	37.140.192.82
Slava-ukraini.site	ns1.beget.com	5.101.152.161
Smile-solutions-ukraine.agency	dns1.registrar-servers.com	185.129.100.113
Ukraine-save.com	ns2.hosting.reg.ru	31.31.196.42
Ukrainewarvideo.com	ns2.beget.pro	87.236.16.75
Ukraineweek.com	ns2.reg.ru	194.58.112.174
Ukraingood.com	ns1.reg.ru	95.191.131.143
Ukrainian-analyst.com	ns3.timeweb.org	92.53.96.12
Ukrainianparty.com	ns2.beget.pro	87.236.16.251
Wikirusiaukrainewar.com	ns.parktons.com	46.8.8.100

Has the CIA Cloud Service Become More Secure? Negative

by Duran (Hong Kong)

Lately, the U.S. intelligence community has been gradually migrating their business to cloud services. The CIA already did cloud work with Amazon several years ago. The CIA's former chief technology officer for the chief information officer Gus Hunt also revealed in an interview four reasons for the transition to the cloud: "speed, efficiency, innovation, security." Of course, the first three reasons aren't in doubt, but the last one - security, really?

The answer is in the headline. Security is not a good reason for migrating to the cloud, at least in my perspective. Why do I say this? Hmm.... You need a pre-knowledge list here:

- James Clapper Jr.: "'Double-digit' cuts coming for intel budget" (washingtonpost.com, October 17, 2011)
- "What to Cut and How to Cut? Historical Lessons from Past Reductions in the Intelligence Community" (Capstone Project, RAND IPC, 2012)
- "Transparency Takes a Hit in CIA Budget Cuts" (sunlightfoundation.com, 2013)
- "The Details About the CIA's Deal With Amazon" (theatlantic.com, 2014)
- "Securing the Cloud" (www.jinfowar.com, April 2014)

Once you have read the above materials, follow my analysis on them.

First, in the book *Permanent Record*, Edward Snowden told us he was building some cutting edge technology for the CIA's private cloud with his contractor partner in 2011 when he was in the U.S. Please take note of the time period. It was the moment when the U.S. government made a decision to cut the intel budget. Director of National Intelligence James Clapper said that "he was going to try to 'protect people' and that he hoped to find 'one half the savings' by reducing overlap among the myriad computer systems now operated by the 16 intelligence agencies that make up the community." Clearly, the CIA had already made a plan for budget cuts, using cloud services to solve the "silos" problem - "the problem of having a billion buckets of data spread all over the world that they couldn't keep track of or access."

Second, the Bush School of Government and Public Service made a capstone report for RAND IPC. In its "Recommendations" section, it says "A decrease in manpower without corresponding reductions to the tasks assigned to the IC creates ineffectiveness, as evidenced by the Korean and 9/11 case studies." and "Policymakers should be aware of the danger of exacerbating the collection-analysis balance. Personnel reductions must be accompanied by corresponding cuts to intelligence missions. If this prioritization does not occur, the IC will be overwhelmed with data, and will lack the ability to process the data in a timely and actionable manner." and "When policymakers cut personnel, they should be wary of the assumption that analysts are completely fungible. Technical and regional expertise is highly valuable, and assuming an expert in one field can move to another field and perform effectively is unrealistic." Overall, we can see this report does not advocate personnel reduction, so the IC have to turn to seek efficiency from science and technology. This represents "speed, efficiency, innovation."

Third, the more secure cloud is *not* real. Why is that? Everybody knows the safest way to store something is to lock it in a vault, whether it's gold or information. We usually make a paper copy of important files in daily life; people always think that virtual things are unreliable. The ultimate object representing the wealth of a country is gold bars.

"The Amazon-built cloud will operate behind the IC's firewall, or more simply: It's a public cloud built on private premises." The saying from the article "The Details About the CIA's Deal With Amazon" from *The Atlantic* actually told us the IC data center facilities were located in a safe place, which can be verified from the paper "Securing the Cloud:" "C2S is housed in a private data center on government premises." Obviously, the agency is very concerned about the physical security of the facility. Besides, according to the description in "Securing the Cloud," it seems that the task of cloud security is left to NSA: "NSA's Information Assurance Directorate (IAD) is heavily involved in projects related to security for cloud architectures to meet the future computing needs of the Intelligence Community. NSA is leveraging this technology for optimum advantage while providing confidence in data security." and "As part of its

IAD mission, the NSA will continue to provide expertise for protection of U.S. National Security Systems whether the data is stored in traditional physical computing systems or cloud-based virtual systems." It is funny to read the word "confidence" in that sentence, it can be seen that the security of cloud services is indeed a complex and severe problem. In this article, the author enumerates various security issues, which is worth reading.

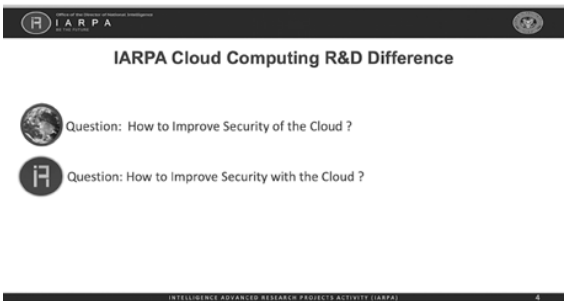
Current Incumbent	Acquisition Description	Estimated Dollar Value
AMAZON WEB SERVICES, INC.	IGF::OT::IGF The purpose of this action is to award a Task Order to Amazon Web Services under a Central Intelligence Agency IDIQ contract for Commercial Cloud Services.	$1,247,284

FY21 Budget

Contract Awardee Name	NAICS Description	PADS Orig Award Date	PADS Ultimate Completion Date	PADS Total Award Value	ITD Obligation
AMAZON WEB SERVICES LLC	Data Processing, Hosting, and Related Services	24-Jul-2015	30-Jun-2019	428,328.00	352,372.00

period budget

Additionally, Intelligence Advanced Research Projects Activity (IARPA) from DNI's Office also tries to convince the public about the cloud security problem. Its explanation mainly illustrates a question "How to Improve Security with the Cloud?" More interestingly, they proposed a concept "Defining Protection Benefits/Costs as a Function of Time" in the slides.



Slide snapshot from IARIA 2018 Cloud Computing Conference

Finally, let's look at some evidence that was obtained from the Department of Energy.

Description of Requirement	Vendor Name	Action Obligation
IGF::OT::IGF THE PURPOSE OF THIS ACTION IS TO AWARD A TASK ORDER TO AMAZON WEB SERVICES UNDER A CENTRAL INTELLIGENCE AGENCY IDIQ CONTRACT FOR COMMERCIAL CLOUD SERVICES.	AMAZON WEB SERVICES. INC.	$44.372.00

FY14 Budget

Numbers tell it the best. The cloud service budget increased from $44,372 in 2014 to $1,247,284 in 2021. This is just the budget of the CIA. It shows the CIA cloud business growing rapidly and this will increase in the future. The government can slash the budget through data center integration, even at the expense of being criticized for cutting off some units (such as the CIA's Historical Collections Division). However, they still have to pay larger costs on cloud security, including hardware and software, as well as "Redesign the Legacy User Environment Leveraging AWS EC2."

Snowden wrote in his book that "The aim was to unite the agency's processing and storage while distributing the ways by which data could be accessed. In plain American, we wanted to make it so that someone in a tent in Afghanistan could do exactly the same work in exactly the same way as someone at CIA headquarters." It is true that the United States can use its super technical power to do something, but the strongest fortress was broken from the inside. More advanced and intelligent things do not mean more security. Legacy systems are often reliable, which has been proven with countless facts. Besides, if an employee can access it from Afghanistan, so can the enemy.

The Author Does Not Exist

by Variable Rush

It started years ago, around 2010 or 2011. I was a big fan of *Final Fantasy XI*. I played Yugdaba on the Valefor server. At some point I discovered there were a series of novels based on the game, but they were only available in Japanese, French, and German. There were no plans for an English release.

I had a German-to-English dictionary and thought I could read at least one of the books by translating each word individually. It was the summer, school wouldn't start for another few months, so I bought a German language edition from, you guessed it, Amazon.

In the few days before the book arrived, I thought of Google Translate. Could it translate faster and make more sense than me translating using a book? To test this idea, I found a German language fairy tale on Project Gutenberg - a German translation of a Japanese fairy tale, as luck would have it - and translated it using a combination of the dictionary, Google Translate, and a friend online who knew German and English. It worked. Within a couple of days, I had created a translation of a short story that had never been translated to English before, if Google was to be believed.

When the *Final Fantasy XI* book came in, I set to work on it right away. I felt great about my translation. I eventually contacted Square Enix's marketing department (I didn't know where else to go) regarding them paying me to translate the whole series. They said no.

I next made a mistake. I translated the entire book of fairy tales and sold it on Amazon. This was a mistake in that some of the fairy tales had never been translated to English. My selling the lot on Amazon counted as them being published, so I was unable to monetize the translations further by having them published in literary magazines.

I translated several more books this way. I also discovered Babelcube. Babelcube is a site that connects authors to translators. I signed up as both a translator and a writer. Several of my translations were translated to other languages by other people, and I myself translated several works to English from German using my tried-and-true method.

That was it for a long time. The intervening decade has been a strange decade for me. I got married, lost close family members, moved, changed professions, went back to college, moved again, and so much more.

So for most of this time, I added nothing to my translation empire. Each month I would be sent a royalty check from Amazon for ten or 20 dollars. Most of the sales were from a translation of an erotic fiction novel written by the same man who wrote *Bambi*. Yes, that Bambi.

Since one erotic fiction novel was about 80 percent of the money I was making in royalties, I sometimes thought how to increase the amount I received, figuring that if I increased the amount of stories I was selling that I could increase the 20 percent on the other side.

I tried using a site like Fiverr to pay people five dollars to write more erotic fiction, but after hiring two people who then sent me the exact same story, I stopped using the site.

During the summer of 2019, I came across a site called "Talk to Transformer." It was a demo of using an AI to write text. Fast forward two years and I find that demo has become something called InferKit. I tried it out. You can just press "generate text" and it will write off the cuff or you can feed it key words to make it write in a particular direction. So for my first pieces, I filled it with the kinds of keywords you would expect to find in a piece of erotica.

Those early pieces I made with InferKit are more, "wham bam, thank you ma'am" than the more nuanced, somewhat story-focused pieces I would later create with it. Granted, editing still has to be completed on each output. Sometimes characters change genders or do things that are impossible or say things that do not sound right or get hung up on a word or phrase (yesterday I had to edit the phrase "all of the colors" out at least a few dozen times as one of the characters in this LGBT story the program generated had a vibrator that contained a light that changed color). Each work comes to 2,000 to 5,000 words.

These new AI-written books make money for me in three ways.

1. Each costs a reader $0.99, so I get $0.35 on each one.

2. They're all in the Kindle Unlimited program, so for each 100 pages read, I get somewhere around $0.04 (more books equals more pages).

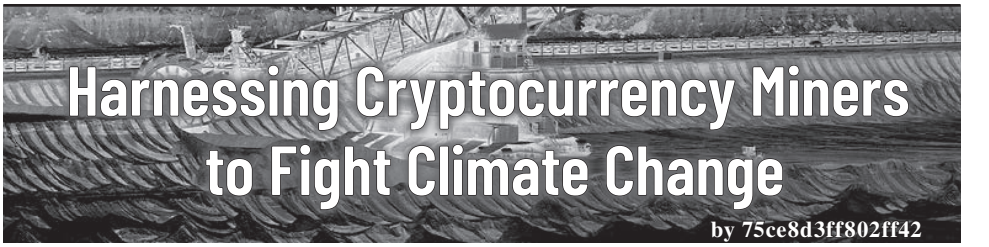
3. They each contain a sample of the original German-to-English erotica book to entice the reader to purchase that book at $2.99 and, of that, I get $2.

Since starting this new venture, I have not broken $40 per month in sales, but it's getting there. I recently broke $30 for the first time. I have

opted to, so far, only publish so-called vanilla erotica. I have not moved into Chuck Tingle-esque territory or anything more risque. The AI gets confused very easily at this stage.

I have two author names going right now for the erotica. I have one with a male name, for those stories that are told from a male perspective, and a female name for the female perspective stories. The pictures for the authors came from a site that makes AI-created faces of people that do not exist. Those names are Samantha Cherry (so named because I don't know a Samantha, yes, I laughed too much at that) and Benedict Urlaub (Urlaub is the German word for Vacation, what I hoped my foray into erotic publishing would net me). I have toyed around with the idea of "writing" other genres.

The InferKit program I have been using has been extremely fascinating. I can see how in the future it and programs like it will constitute the equivalent of duct tape in books, that an author who can't write action scenes or love scenes will use it to piece aspects of their stories together. And yes, I know that by using a program I am technically what is known as a "script kiddie." But as the ninth of the Ferengi Rules of Acquisition states: "Opportunity plus instinct equals profit."



Harnessing Cryptocurrency Miners to Fight Climate Change

by 75ce8d3ff802ff42

One of (if not the) biggest obstacles facing the widespread adoption of renewable energy (wind and solar) is the lack of a way of efficiently storing electrical energy at scale. We can store small amounts in battery packs, but large-scale storage is still a trillion-dollar problem. This leaves electrical grids with several unattractive options:

1. Overbuild so much wind and solar farms that there's still power available even on calm nights.
    - Extremely expensive and wasteful 99 percent of the time
2. Build expensive and inefficient energy storage facilities.
3. Supplement wind and solar energy with fossil fuel energy when necessary.
    - Often *less* green than 100 percent fossil fuel systems because on-demand fossil fuel generators are less efficient than always-on generators

I would like to propose, as a thought experiment, a way to harness the money behind cryptocurrency mining operations to expand green energy production. Yes, I know that I just proposed cryptocurrencies as a solution to a serious problem, but please hear me out on this.

My proposal: Designate 90 percent of surplus green energy produced at any given moment to a pool that is distributed to cryptocurrency mining operations in proportion to how much of the grid's production capabilities each operation has contributed. Contributions to the grid can be in the form of wind and solar farms or cash payments for the grid to spend on building/expanding wind and solar farms. As an added measure, consider adding an additional tax on all cryptocurrency mining operations that rely on fossil fuels for electrical energy.

Such a setup would give every mining operation an incentive to assist in building out the grid's wind and solar capabilities; an operator could invest in the grid and reap the rewards of effectively free power indefinitely (a small fee for maintenance may be required long-term). Some operators may choose to run their own wind and solar farms, but buying into the grid's system gives operators two advantages:

1. Geographic diversity provides more reliable power.
    - It may be calm where your operation is situated, but the odds are that it's windy *somewhere* on the grid's footprint
2. The option to simply pay the grid to expand wind and solar production saves mining operators the trouble of building actual wind and solar farms.
    - Just "let the professionals do it"
    - This also has the benefit of allowing for smaller mining operations that don't have the large capital required for building wind and solar farms

In my humble opinion, the jury is still out on whether cryptocurrencies are a net good or ill for humanity. Hopefully, a setup that encourages miners to contribute to green energy production would move the dial towards "good."

An Atavistic Freak Out, Episode Four

by Leon Manna

This story is a work of fiction.

5:43 AM on a Monday. Typing furiously into my laptop as the sun starts to rise, realizing that I intended it to be a late night and it ended up turning into an early morning, another maniacal, amphetamine-fueled organized keyboard mash which, by some ridiculous odds, turned into something that you could comprehend, or maybe even *read*. If you wanted to, that is.

I'm not Leon Manna. He was always just an idea when they stack the cards which, of course, are stacked against me. Leon Manna.... The name sounds like a stranger to me. Some barrier was crossed, a bridge to a terrible life filled with excitement, after declaring myself dead to escape The Machine. There was something funny about it. Your, no, *my* whole life destroyed in an hour long funeral service, nobody in the casket as they lower it down. Never again.... Now it's just checks and guns and cheap CVS cell phones that I drop into puddles. After the whole thing was over, I became Leon Manna. I lied to you, and I am truly sorry. Take the back door on your way out. The show goes on. It won't ever stop! Never! Don't count on it! Ride the wave! Mindfulness! You wouldn't like it!!!

So let's get back to my story. There I was, sitting on my couch like an idiot, waiting for the blotters to kick in, watching a mosquito fly around my room. Someone was knocking. They were like gunshots, Vietnam flashback to my old neighborhood, KDY at night, putting my nerves on edge, electrocuting my brain, 110 volts, neurons firing too fast to comprehend anything as my pupils dilated from the blotters and I saw the world in full color, not one, not three, but the entire range the human eye can even process.

No thoughts, just open the door. It was Lenny. His shirt was stained red. I stared at him for a second. The way he was just standing there, staring at me with this possessed, demonic look on his face was amusing. I knew I was supposed to be scared, but it was almost like he was trying to amuse me. I laughed and said, "Jesus man, are you okay?"

He groaned and his face turned red. "You left me on that beach! I'll brace you for this!" He swung his arm at me, missing by what, a foot?

"Hahaha.... You shat on a five-year-old and punched me in the chest! What else did you expect me to do?" I cackled a couple more times.

He let out a guttural noise and started staggering towards me. I backed up and pulled a switchblade out of my pocket. "Lenny... heh... I'll stab you! I swear to... *hah*... I swear to god I will! Please man! Hahahaha...." My organs were starting to hurt. I couldn't stop laughing.

His eyes were glazed and unfocused. Red spot, he missed his vein. Telltale signs of the type of junk addict who *wants* you to stab them. Maybe I should, for his own sake.

"You wouldn't do that.... You're gonna have to stab me.... Hehehehe.... Don't you live above the landlord? You spent too much time in drug dens as a teenager. Your mom was right about you! I had a whole talk with her last night over dinner. Bitch! Haw!"

"My mom went missing and is assumed dead, Lenny."

We stood there for a second and made eye contact, both totally silent waiting for the other to say or do something. But neither of us did; we just stared at each other. Then I chuckled, and so did Lenny. Now, rolling around on the floor, unable to control ourselves at all, a tenant peeked out of her door and then promptly slammed it shut. I laughed so hard I pissed myself. Is Lenny my friend? I'd hope not.

SECURE MESSENGER:

2600 Magazine: Yo
leon_3k: what's crackin goldstein
2600 Magazine: Why do you call me Goldstein?
leon_3k: Goldssten.
2600 Magazine: HOPE this weekend
leon_3k: hope for what
2600 Magazine: The conference. You coming?
leon_3k: Yes, of course. I'm gonna write about it, in your magazine, and I will be smoking crack the whole time. Then I'm gonna let a coyote loose inside the building.
2600 Magazine: do you have a job?
leon_3k: I am self employed, I invest in imaginary encrypted money and the stonks markets.
2600 Magazine: How high are you
2600 Magazine: Oh, the other thing I had to tell you is that we got a letter from the FBI about you, they don't appreciate some of the things you write about.
leon_3k: Kyle better be there.

2600 Magazine: No seriously, don't write anything crazy. We got subpoenaed last time.
leon_3k: F

Hackers On Planet Earth! How could it have slipped my mind? Why would it? And it was that year, so once more I would atavistically make a trip to New York no matter the distance I had to go, just to dive right into the very center of The Machine, all while being far too deep into some second life with too little correlation between the two to ever be able to turn back. I can see the point of no return through my rearview mirror, the exit I never knew I had to get off at until it had passed.

Me and Lenny started the trip. He loaded around three suitcases, which was strange considering we'd be there at most four days. He wouldn't tell me what was in them, but they seemed way too light. All I brought was some weed. I'm done with these research chemicals and the only thing I was researching was how high they would get me. Right as we got on the road, Lenny took out a needle.

"Put that shit away man! Not in the car! You need to drop that before it's too late. Have you ever read William Burroughs? I bet you can't even read and some sort of idiot algorithm in your heroin brain calculates it for you...."

"Shut up, shut up! I need it! You fucking nerd.... My chest hurts! *Uuaahhhh!*" Unhinged.

Idiot! I lit up my first spliff as we were driving. It was high quality weed. I felt very calm as my attorney suffered from a borderline opiate overdose next to me. It was nice to *not* be on some crazy psychotic chemical. Things felt peaceful.

And here I am now, flying down Interstate-95 in light blue denim pants, cuffed up twice, waterproof Vans, glasses hanging onto my face by a thread. The car was going about 70 MPH on a highway in SC. My shirt was in the back seat, because the AC didn't work and the heat in Charleston was reaching 94 degrees Fahrenheit. Lenny had his head back with his eyes shut, sweating and groaning every now and then.

I was focusing on the road when suddenly it all made sense. The FBI asked me to sing them a song yesterday... or maybe it was right at Sawtooth when they asked. Three letter agencies are better than no audience at all. Do I sing to them? I don't think I'm even capable of knowing when I am.

26 was the number on my shirt. What did it signify? I didn't know. I had thrown a suitcase together in a hurry at the last minute, a mixture of Khaki pants, shorts, white shirts, and socks. The amount of days we would be there outnumbered the clothing items by 26. And that somehow matched the number on my shirt, which matched my age, which matched the date. Was there a meaning? Or was this magical thinking? Did Lenny agree? Did Goldstein? Do you?

I looked up. I was standing outside of Hotel Pennsylvania in New York, not moving, with a dumb look on my face. This was where HOPE was (at the time) being hosted. Me and Lenny were staying in a shitty motel across the river in Hoboken, New Jersey. The parking was better out there, and we took a train to get into NYC.

My daydreaming was cut short by Lenny. "Stop staring at the hotel and let's get started. I wanna interact with these freaks so goddamn bad...."
"They aren't freaks. They're actually great people."
He laughed, and said, "If they're anything like you, they're freaks."

There was a journalist sitting at a table near an auditorium. I don't consider myself a journalist, but something *like* it. Still, that's giving myself too much credit. I just write stories. We started talking, and he asked me my name.
"Ocha. I go by my last name."
"Alright Ocha, you okay being in a story?" He looked at me intensely.
"I was going to ask you the same thing." Crooked grin.
"Who are you writing for?"
"I'm doing a story for La Palma Tech."

He said some random online publication I'd never heard of. Then he mentioned that he had some cocaine, and asked if I'd like to do a line with him.
"I'm supposed to be in that talk."
"Let's just go to the bathroom real quick." He grinned at me.
"I don't think that's wise. I heard they're going through people's bags while they're in talks. Hotel rooms too, the ones who are staying here! They're looking for drugs and weapons. Intel says there's about three firearms in the building right now. They already caught eight people for coke, and seven more for psychedelics. Didn't you see them taking people out?" I tried to look concerned.

His face changed. He got scared. Everything I just said was completely false. I don't really know why I was fucking his brain up the way I was. I think I just wanted to see if I could. He was pissing me off anyway, and besides, anybody who offers random people cocaine

deserves it. They weren't actually searching anybody's bags, I just wanted him to be in a constant state of fear that they would.

I don't remember what the talk was about, because I was too focused on trying to spot FBI agents. I wasn't able to, because all the FBI agents were dressed in normal clothes. I declined the journalist's offer of cocaine. He decided he was just going to snort it right there in the auditorium, and was taken out by security ten minutes later. I remembered the lie I told him warning him about this and wondered what was going through his head as they took him away. I pretended I didn't know him and stared straight ahead.

Then I heard a scream, and turned to the back of the auditorium. I saw Lenny's silhouette standing in the doorway. He rushed over and sat down next to me. The dude on stage let out a very wet fart.

"I gotta go man, I'm freaking out. They're taking people away left and right! We have to leave." He sounded afraid.

"Hold on, just wait it out. We'll be fine, we didn't do anything," I whispered.

"Cmon, let's go!"

"Alright, alright, we'll leave. You have a point. I saw the pigs take some poor nerd away 30 minutes ago. Then security kindly had a journalist escorted away."

"I saw him on the way out.... They didn't look happy. As your attorney, I advise you to leave so we don't end up like him."

We got up and exited the auditorium. We chose not to take the elevator, but rather go down a restricted stairway. Neither of us were allowed to do this. We made it downstairs and into the lobby, when I heard a shout.

"Stop! Don't move!"

I looked behind me and saw a U.S. Marshal, some fat, middle-aged walking handlebar mustache. He looked like a freak cartoon version of Hulk Hogan after drinking beer and smoking cigarettes for 15 years straight. I looked at Lenny and we ran. Lenny barreled right into some silver-haired kid with a guitar, knocking him over in an instant. I dashed out the front door. We managed to outrun him, because he was about 240 pounds, and got into a nearby subway station.

TRANSCRIPT ISSUED AT REQUEST OF LAW ENFORCEMENT VIA SUBPOENA

[Dial tone]

Goldstein: Did you get away?

Leon: Oh yeah.

Goldstein: It's gone to shit. Someone burglarized our hotel room and stole two passes. We still don't know who did it, and they won't share the CCTV footage with us.

Leon: I'm sorry, what?

Goldstein: Yeah, someone got one of our staff to disclose our hotel room, and then somehow got in and took a pass.

Leon: ... I'm gonna have to call you right back. [Phone call ends.]

So *that's* how Lenny got our passes!

We saw the first palm tree at the bottom of North Carolina. We made it to Charleston, and Lenny said he needed a swim. We got to a beach and went down to the water. I smoked out of my hash pipe quickly and we got into the water. After a moment, I said, "that was crazy...."

"You're telling me? How long were we there for anyway?"

I laughed. "One day. It was supposed to be three. It was pretty funny when you let that scream out and burst into the auditorium."

He chuckled. "Yeah, I did that on purpose. Did you see their faces? The nerd on stage looked like he shat himself!"

"He did shit himself! I heard it! We outran a U.S. Marshal. We must be extremely lucky."

"No, we're extremely smart." I noticed he was talking about both of us, and not just him. I'd never seen him as relaxed and friendly as he was.

"You proved yourself," he said.

I was shocked. "What?"

"You're someone I can respect and view as an equal now. And why? Because you actually listened when I told you we had to leave. I'm your goddamn attorney, and for the first time you actually listened. You're an idiot genius who doesn't know what's good for him. A lot of my clients don't listen. But when someone does, they've proved themselves. Besides, the pig could hardly keep up with you."

I didn't say anything for a second, just smiled. Then I laughed and asked, "What was in those suitcases anyway?"

"Hah! A couple servers I stole out of a server farm, seven laptops from the editor's room, a bunch of HOPE passes, four USB drives I stole out of a police station, and then one very very sensitive government document I really needed to get rid of."

My smile disappeared. Awful jackass....

What will happen next? I don't remember, so we will both find out when I read my notes next time.

Social Media Is Neither

Let's be honest. We've all benefited in some way from social media. Whether it's staying in contact with a select group of people or being more tied into what's going on in a particular community or movement, we cannot deny that through social media we have the means of connecting in a far more efficient and accurate manner than ever before.

But it's this very allure which draws us in and helps to set us up for a nightmare that eclipses all of the good. Virtually every negative aspect of society has become orders of magnitude more amplified owing to the ability of instantly rounding up a huge number of like-minded people - as well as artificial constructs that can often carry the same weight as real individuals.

Mob rule is never a good thing. The least common denominator becomes the default and any signs of independent thought are quickly quelled. Forums like Twitter and Facebook make it really simple to whip up outrage and shut down an opponent or even an entire opposing line of thought. There are occasions where this is warranted, but there are many others where it is not. Hatred, racism, bullying - these are easy to understand concepts that shouldn't be tolerated in any forum. But then the tables get turned and, through social media, people are told that up is now down and 2+2=5. Because of the mob mentality, few dare to question what is obviously wrong. Most are content with being in a group where they feel they belong and where there's a target of "others" who are the threat and who must be stopped.

Nobody is immune from this. We've seen it happen on all sides of the political and social spectrum. Just as we once told ourselves that fascist rhetoric could never take hold in our country, we now make a similar miscalculation in concluding that whatever side we're on is safe from undue peer pressure through social media. While there are certainly perceptible differences in the degree that we're all affected, a seed is still a seed. As long as we hand over this much power and influence to this means of communication, we risk losing a great deal before we even realize there's a threat.

When "alternative facts" become legitimized through over-tolerance or by convincing people that they're constantly being lied to, almost everything can be turned into reality for a significant part of the population. This is how a fair election can be seen as a stolen one by huge numbers of people; those saying otherwise are lying and making up facts - and simply saying so is enough to convince those who have signed on to the right social media faction. We saw the same thing with vaccines and how all kinds of easily disproved "facts" were being spread and believed, despite what health experts worldwide were saying; the health experts were in on the conspiracy, after all. Suspicion and mistrust, coupled with instant access to millions of believers and sharing legitimate-looking stories, made actual facts no longer necessary. As Russia continues its brutal onslaught in Ukraine, its citizens continue to believe the official version of events, despite what on-the-scene journalists, witnesses, and actual unedited footage are saying. This is actually an older strategy of simply shutting down the independent voices and only permitting state propaganda to be heard. It's historically how populations have been controlled and it continues to be an effective means of manipulation across the planet. Control of social media only makes this tactic easier.

When we say that social media is neither, what we mean is that there is nothing social about blindly following and never questioning what you're told by the people you find yourself allied with. We know this is not how everyone uses the tool, but a significant percentage of the population does. And as for media, let's just say this is not the kind that you should rely upon to tell you the truth or to uncover actual facts, particularly those you may not want to hear. *That* form of media is comprised of people who spend their lives pursuing facts, questioning what they're

told, often putting themselves in danger, and reporting what they find - regardless of who benefits and who wins or loses. Yes, we can still "become the media" and uncover those truths that mainstream media overlooks for one reason or another. But this is an earned position, not one that you get simply because you want it. Unfortunately, the lines have been blurred to such a degree that it's almost impossible to tell true journalists from entertainers - or even highly delusional individuals.

The risks to all of us if this continues are great. In the past, we've warned of the potential abuses of new technology by asking readers to imagine what might have happened had the Nazis had such tools at their disposal. Now try to imagine what they would have done with the power of social media. And realize that there are many regimes that are at this moment refining their skills in that particular realm so that their message becomes the only one that spreads and weaponizes. In the past, you simply had to have a dictatorial form of government where the population and the media were controlled in order to turn lies into truth. But now, all you need is a way of reaching susceptible people through social media, along with a message of suspicion and fear that will motivate them to follow you and do whatever you say. And once that's perfected, the dictatorial power will inevitably follow, as the mindset for it has already been established.

It's a scary prospect, but it's not an inevitable one. We have the ability to fight back. We just have to believe in ourselves as individuals who aren't desperate to win acceptance. We don't have to keep going down this road.

This means taking social media a whole lot less seriously. It means actually *talking* to people one on one and not just going with what's popular or trending. It means not being afraid to speak your mind and to not feel the need to punish others when they do so. Arguing is great. Shaming is a tool often used by bullies who can't win an argument with words, so they turn to mobs. We can do better.

It may seem comical and almost fun to watch how crazy things can possibly get. We used to believe that to a degree years ago. But if the nonsense leads to the wrong people being in the wrong positions and making the wrong decisions, it very quickly stops being funny. And it's damn difficult to untangle the ensuing mess.

We're living through a lot of those consequences today and the situation may seem hopeless at times. It's not. It just requires that we work together so that a degree of sanity can once again prevail. That means being able to distinguish fact from fiction, to respect the words of those who have devoted themselves to true research, and to always continue questioning what you're told. That latter part should apply to everyone, not just those you don't trust. Most of all, we have to learn how to communicate with people again, not just usernames.

Social media started with such promise. We gave it too much power. It's well past time we took that back.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2022. Annual subscription price $31.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	21063	20000
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	5442	5389
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	14169	12880
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	19611	18269
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	123	122
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	920	914
E. Total free distribution	1043	1036
F. Total distribution	20654	19305
G. Copies not distributed	409	695
H. Total	21063	20000
I. Percent Paid	95	95

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.

Phishing in 2022

by Jeff Barron jeffbarron@protonmail.com @_jeffaf

Phishing remains the most effective way to penetrate an organization from the outside. The Verizon 2021 Data Breach Investigations Report (DBIR) states that a median average of 3.5 percent of users click the phishing link. This was a median; some organizations had clickthrough rates of greater than 40 percent. It's funny, even if you don't follow the tips in this article and your phish ends up in spam, you still have a chance. Phishing is alive and well in 2022. In this article, I will show you how to do it. No more cloning websites. Two-factor authentication? We can beat that.

OK, so you have your target? Well, there is a bunch of OSINT to be done before you can even set up your domain. A sock puppet account on LinkedIn is really good for mapping out relationships inside of the target organization. Other social media can reveal useful things for the target as well, but I mostly stay with LinkedIn.

Using the website `phonebook.cz`, I discovered 307 email addresses for `2600.com`. Now, I have no interest or intention of phishing the good folks at *2600* or anyone that isn't paying me to do so. However, it shows how effective `phonebook.cz` is at quickly displaying email addresses by just providing a domain name. Another commonly used tool is "theHarvester" which is available on GitHub and packaged with Kali.

OK, so you've got emails and maybe some information for pretexts from your OSINT analysis. This is the point where you should search for breached credentials for your target. If you haven't been collecting breach dumps and don't know anyone who has, then I recommend an awesome service: Dehashed. You can get an account for $5 at `dehashed.com` and it's well worth it. You can also check for the existence of breached credentials without paying anything. Once you have obtained your breached creds, then it's time to try them out. If you can send an email as someone in the organization, then that will add credibility to your phish.

It's time to register a domain. The first thing we want to do is examine our target domain name. Can we get a different TLD? Using a tool at `dnstwist.it`, one can see that there are some shady *2600* domains like `2600.cn` and `2600.eu` that are likely not related to `2600.com`. You may get lucky and get the .ORG or .NET version of your target. It is also worth checking for expired domains. You can find those on `expireddomains.net`.

As far as registrars, I don't really have an opinion. The cheaper the better. I've used Namecheap in the past and it's done the job. After you register your domain, the next step is to sit on it for at least seven days. If your domain is less than seven days old when your phish goes out, it will be sent straight to spam.

The next thing you'll want to do is to get a VPS for your domain. I use Digital Ocean droplets, but there are probably better and cheaper options out there. On your Linux-based VPS, you'll want to install Postfix and Mailutils. (Mailutils is the package name for Debian/Ubuntu-based distros.)

Setting up Postfix is out of the scope of this article. I'll include an awesome reference at the end of this article for those who want to learn more about how to do it. Essentially, it boils down to adding your domain to three files (/etc/postfix/transport, /etc/postfix/virtual_domains, and /etc/postfix/virtual_regexp). Remember to configure hostname and mailname properly in /etc/ as well.

We need DNS entries! You'll want to configure your DNS to have an A record pointing towards the IP address of your VPS. You'll also want an MX record pointing at mail.evildomain.tld. Unfortunately, there is still more DNS work to do. We must have SPF, DMARC, and DKIM records for our shady domain! This is fairly easy to do and, again, I point you to the first reference at the bottom of this article for more details from `Hacktricks.xyz`. After you have set up SPF, DMARC, and DKIM records, then you also need a Reverse DNS entry or rDNS PTR record that resolves the IP address of the VPS to the domain.

So we have finished our setup. It's time to *test* our mail and see how well it will do with spam filters. `Hacktricks.xyz` recommends a website called `mail-tester.com`. You can send an email to it and similar services from the command line with Mailutils.

```
echo "my test message" |
➥mail -s "My test message"
➥generatedAddress@mail-tester.com
```

After testing the email, there is one more thing I do on my VPS box. I use iptables to block AWS, Azure, and GCP. I don't have good data on this, but I strongly believe this allows my evil domains to live longer without getting burned by threat intelligence companies scanning the Internet for bad domains like ours.

Pretexts! So what are we going to say to get the user to click? I have two trusty pretexts that are effective. They are "Hey, I'm (insert name of IT person found on LinkedIn) and I noticed some unusual activity on your o365 account. Would you help me out and check and see if this is you?

Thank you so much! (insert link)" and "Hey, we are resetting all passwords as we integrate our new vendors. Please go to (insert link) and follow the prompts as soon as possible. Thanks! (Insert name of IT person you found on LinkedIn.)" It's good to personalize the email as much as possible and say Hi (name of victim), but that can be tedious so I usually just make it generic for all, then send the phish to everyone (except the IT department).

At this point, we have most of what we need to begin this engagement. But what are we linking to? We haven't cloned any websites! The reason we haven't is that we are going to use evilginx2. From the GitHub page, the project self describes as follows: "Standalone man-in-the-middle attack framework used for phishing login credentials along with session cookies, allowing for the bypass of 2-factor authentication."

Evilginx2 is amazing. Imagine our victim uses o365. We can generate a link with evilginx2 that when the user clicks it, will be redirected through our site and get proxied to the actual site itself. So on one side we have the victim user, in the middle is our VPS, and on the other side is o365. It looks identical because it *is* the actual site. Because of where the VPS sits during this attack, you can also capture session cookies generated if the victim user gets a push notification or enters a code - since we are proxying the connection, we will get that cookie too and be able to bypass multi-factor authentication in this way. Evilginx2 will also download TLS/SSL certs for you when you run it. I prefer running it from docker as it's quick and easy. The evilginx2 GitHub page has great videos explaining how to use it and how it works under the hood.

All right, so if you've gotten this far, you now have everything you need to conduct a modern, MFA-bypassing, phishing attack. Please use this power for good. I recommend reading through the references for more detailed information on some of the areas I glossed over. If you want to talk more about offensive security, please feel free to shoot me an email.

A big shout out and thank you to the folks who helped teach me this stuff: Critical Path Security, Black Hills Infosec, the amazing folks at hacktricks.xyz, Kuba Gretsky of the evilginx2 project, and *2600 Magazine,* which inspired a 12-year-old version of me to build a red box.

So long, and thanks for all the phish.

References

- book.hacktricks.xyz/generic-methodologies-and-resources/phishing-methodology
- github.com/kgretzky/evilginx2

Plain Text in Plain Sight: Smaller Alternatives to the World Wide Web

by Colin Cogle

What's wrong with the World Wide Web? You open a browser, connect to a server (usually securely), and interact with content. With a few clicks, you can get news, sports scores, movies, inane updates from people you may know, cat pictures, hacker magazines, dinner... what's not to love?

Sir Tim Berners-Lee published the first website in December 1990, where he described his new document management system, hypertext, and the markup language for it. Though he continues to shape the incessantly-evolving ecosystem as the head of the World Wide Web Consortium, there are problems with the modern Web which will likely outlive us: ads, trackers, megabytes of JavaScript bloat, DRM, cookies, nonconsensual data collection and analytics, pop-ups, pop-overs, pop-unders, autoplaying music, commercialization, compartmentalization, autoplaying video in the corners of news articles, top-ten lists spread across 11 pages, ugly Facebook share buttons everywhere (even on PornHub for some reason, in case someone out there thinks their family and friends will love this video). And that's just off the top of my head.

It's easy to be an old man yelling at a cloud. It should surprise no one that the World Wide Web is here to stay. However, that doesn't mean we can't come up with alternatives. In fact, we already have - and I'm not talking about mobile apps or Tor Browser.

Go For Gopher

When you strip away everything superfluous, you're left with plain text. No formatting, no scripting, just words on a page. That was the idea behind Gopher. Named for the University of Minnesota's mascot (in case you were wondering), Gopher is a filesystem-

inspired protocol to make your computer "gofer" information online.

Gopher sites (sometimes called Gopher holes, because why not) are typically presented as a text-based menu. You have words, and you have links to folders, files, or other sites. That's it. Unlike the Web, all Gopher sites look the same and navigate identically. It's truly a product of a time when NFT stood for nice fucking Tamagotchi.

This forced simplicity is part of the reason why it failed. While HTML is forgiving of mistakes, Gophermaps are strict and make you follow RFC 1436 to a "T." Needless to say, once customizing your MySpace pages became a thing, Gopher was looking very long in the tooth. Browsers eventually removed support for it, getting rid of it like an unwanted rodent.

Somehow, though, Gopherspace isn't dead. In the past 15 years, the number of Gopher servers online has tripled. Servers, clients, and (ironically) Web browser extensions continue to be developed. Most notably, the Playdate handheld gaming system had its release notes only available via Gopher, leading to [some news coverage for the plaintext protocol] (theregister.➥com/2022/05/23/the_return_➥of_the_gopher/)!

Gopher is more than nostalgia for the days when the Internet made noise when you turned it on. You can find news, weather, search engines, home pages, phlogs (the equivalent of blogs), and more. Perhaps this little rodent living under the Web isn't so dead after all.

Blast Off With Gemini

Fast-forward to 2019. A person by the handle Solderpunk was frustrated with the WWW and how crazy things were getting. In an interview, he said, "Visiting websites is basically a matter of downloading and running software, without any way to know in advance what that software might do, and very little ability to pick and choose which things you let it do." However, he also thought Gopher was too rigid and restrictive. The community sat down and thought up something like "'the web, stripped right back to its essence' or as 'Gopher, souped up and modernized just a little.'" The result was something these outer space buffs called Project Gemini.

Like Gopher, it's another simple text-based protocol that was designed to be intentionally difficult to expand, to avoid the feature creep that the WWW underwent. However, Gemini sites (called "capsules") are more modern, featuring Unicode, free-flowing text, gemtext (think: Markdown), virtual hosting, TLS 1.3, and more.

In three short years, Gemini has gone from IRC discussions to something implemented by over 2,000 servers, and it shows no signs of slowing down. More capsules and gemlogs (again, "blogs") are rocketing off into Geminispace every day.

So the Web Is Dead, Right?

No, and far from it. For general browsing, the World Wide Web is going nowhere, and that's fine. I've spent this article trashing it, but the good still vastly outweighs the bad. My bank will never implement Gopher. Amazon won't be selling products on Gemini anytime soon. Despite the big Web, there is definitely a place for the "small web" these days.

Consider:

- Has your computer gotten too slow to run Google Chrome? Is that old Android tablet struggling? Did Apple cut off macOS updates for your perfectly good laptop? Don't fork over your hard-earned cash and make more e-waste. A Gemini browser would make that old device feel like new - and put less strain on the old battery.
- Perhaps you want to get your vintage computer or old cell phone back online, but good luck using a 25-year-old Web browser. Gopher was made for retrocomputing!
- Traveling out to the boonies and stuck with dial-up or a 2G phone signal? It's rare, but it happens. You could spend an hour watching one web page open, or use Gemini and get it done in seconds.
- Do you prefer the command line? Text-mode web browsers can be cumbersome, but Gemini and Gopher were *built* for the terminal.

If you feel like everything online is getting bloated, and everyone wants to track you and sell you their crap, there are thinner alternatives. We can chat on IRC, talk on newsgroups, send email instead of signing our lives away to Meta - and now, we have some alternatives to the ever-expanding Web. However you choose to do it, happy browsing!

BATTLE FOR BETTER BATTERIES

by Hydrolycus

Rechargeable batteries are found in all the things, big and small, that make modern societies tick. Thanks to their ubiquity, it is easy to take batteries for granted, but in doing so we ignore the undeniable fact that our choice of rechargeable battery is a choice that has real-life consequences in environmental, financial, as well as geopolitical terms.

So let's start at the very beginning, allegedly a very good place to start.

The Heavy Metal Era

The lead-acid battery was the first practical rechargeable battery. Invented by the Frenchman Planté in the late 1850s, it's inexpensive to manufacture and capable of delivering plenty of current features that have led to it still being the most widespread battery used in internal combustion vehicles and stationary installations.

In spite of its popularity, it's not without problems. First of all, it has a poor power-to-weight ratio. Lead, one of the battery's principal components, is as heavy as - well, lead actually, a fact that makes it unsuitable for portable devices.

It gets worse. The other principal component is sulfuric acid. In practical terms, a leaky battery in your phone could give you a one-time free dermabrasion. The charge/discharge cycle of a lead-acid battery releases highly combustible hydrogen gas, creating a potential Hindenburg scenario in poorly ventilated spaces. And then there's the disposal problem. Lead in all its forms is poisonous to humans and many other living organisms, necessitating strict disposal and recycling protocols for the batteries.

Nickel Ain't Worth a Dime

Nickel is a much lighter metal than lead. It's relatively inexpensive, and nickel oxide hydroxide also happens to be a good material to make battery electrodes from. Several different chemistries have been developed, and such batteries can be made quite small, making them viable in portable devices.

But as you probably guessed, nickel-based batteries have their own set of problems. The batteries have very real limits on the number of times they can be fully recharged from a partial discharge, the "memory effect" we've all come to hate. They also have problems with polarity reversal if they are discharged too deeply, a phenomenon that can kill sensitive electronics along with the battery. The trick would be to discharge the batteries fully but not too fully before recharging. And even if you are astute enough to pull that off, there's a gotcha: self-discharge through internal leak currents.

Although nickel isn't very toxic by itself, it is often partnered with cadmium in batteries, and cadmium is an extremely toxic metal that you don't want in your local landfill, unless you have a fetish for kidney failure and spontaneous bone fractures.

A Cure for the Blues: Lithium

So far we've painted a pretty depressing picture of rechargeable batteries (pun intended), but for the longest time it was all we had and we learned to live with it. Then the 1980s came upon humanity, bringing with it blessings like big hair, Members Only jackets, boom-boxes, ferns, and *Full House*. And lithium.

Lithium is the lightest of all the metals, juxtaposing it as a Barry Manilow to a heavy metal like lead's Iron Maiden. It is also happy to give away and accept back electrons, with none of nickel oxide hydroxide's fussiness. Put those facts together and we could have a recipe for battery chemistries suitable for portable devices as well as electric vehicles. And, sure enough, there are dozens of battery types based on lithium. So all's well, then?

Hardly. Lithium is a poisonous metal, posing a danger in humans to the kidneys and the nervous system. Somebody might protest that the small quantities used in, for example, a cell phone or a music player aren't a big deal in the overall scheme of things. But imagine the day when discarded lithium-based batteries of tens of millions of electric cars and other vehicles end up in landfills across the globe.

Disposal is not the only problem associated with lithium. The mining and refining process of lithium consumes mind-boggling amounts of another scarce resource: water. It takes two million liters of fresh water to make one ton of lithium. One ton of lithium is a lot, right? Actually, no it's not. One ton of lithium is barely enough to make batteries for perhaps 90 small passenger cars.

Then there are the financial considerations, and those include more than just the high cost of

extraction. Lithium is a relatively rare metal. The worldwide reserves are on the order of 20 million metric tons. Most of the reserves are located in China, with other extractable deposits in Australia, Chile, Argentina, and the Democratic Republic of Congo. Much of China's production is earmarked for domestic consumption, and a sizable chunk of the contracts for the output of other countries is already spoken for by a handful of corporations. In effect, there's a monopoly in place, keeping prices artificially high.

China's dominance in the lithium market has obvious geopolitical consequences, as it could be used to pressure other countries, especially with the world's growing dependency on lithium batteries.

Similar situations exist for many of the other key ingredients in lithium batteries, such as cobalt, copper, graphite, and others.

Finally, we have to mention lithium-based batteries' claim to popular infamy. They're prone to runaway thermal reactions that can cause them to catch fire. Your ears could literally be burning if that happens to your phone's battery.

At this point, it would be fair to ask if there is a way to make good, usable, rechargeable batteries without either killing the planet, going bankrupt, or starting World War III. It turns out that there might be.

Sodium: A Salt and Battery

The metal sodium sits on the next rung of the periodic table right above lithium. Given that position, it's reasonable to ask if it has chemical properties similar to lithium. The answer is that it does. It's highly reactive in the sense that it's willing to give up electrons, but also take them back - the fundamental idea of rechargeability. In fact, metallic sodium is so reactive that it will catch fire if exposed to air!

Sodium is abundant on our planet, and not only in cheap snack foods and hipster spas. Our oceans are full of sodium, and there are rock deposits all over the world. Thus, there are no geopolitical complications to overcome. Our blood and the cells of our bodies are jam-packed with sodium chloride, as are all other living cells, living proof that it's not toxic if enjoyed in moderation. And to top it off, it's relatively inexpensive to extract from the many sources that exist.

So the final question then becomes: Could we make sodium based batteries? We not only can, we already *are* making them. CATL, the world's largest battery producer has developed the technology, and by the time you're reading this they have probably reached the market. But they were not first. Several companies, for example British firm Faradion, are already shipping large-capacity sodium-based batteries to customers.

The Low-Sodium Alternative

There is even more good news on the horizon. Several companies are making progress developing "green" batteries from organic sources. Huh? Organic batteries?

One of the most promising organic battery technologies is based on peptides. Peptides are simply chains of amino acids, the stuff that proteins are made of. There are 20 naturally occurring amino acids, and each have slightly different chemical properties.

Depending on the order in which the specific amino acids are linked together, we end up with peptides and proteins with widely varying characteristics, some of which can be used to make rechargeable batteries. This is thanks to the electrical properties of various amino acids. Some of them - for example aspartate and glutamate - have a negative electric charge, whereas others - for example histidine, arginine, and lysine - have a positive electric charge.

What's so great about organic batteries? First of all, the chemicals inside them are fully biodegradable. There are no poisonous metals to worry about.

Second, since proteins are the building blocks of all living matter, there are plenty of cheap amino acids to go around if you know where to look for them. Batteries have successfully been created from farm- and forestry-waste that would otherwise be burned or left to rot! Nobody goes to war over farm waste.

One final, very interesting property of peptide-based batteries is that the charge time is much lower than what we get from lithium batteries. Imagine fully charging your Tesla in 30 minutes!

This technology is developing rapidly, and there are several pilot studies underway, primarily targeted at making batteries for electric vehicles.

All in all, there is hope for a future beyond lithium and lead. It's not a matter of technology anymore, it's a matter of economic and political initiative.

Shout outs to Joao, Saravanan, Rav, John, and Kirk.

Command Line Unminifier

by Gearbox

JavaScript and CSS files are usually posted online in minified format (minimum number of spaces and everything on a single line) in order to save transfer bandwidth. This makes it hard to analyze. Even though there are online tools to unminify such files, using a command line utility to do this work has the advantage of integration with already existing CLI tools (via pipes or command calls) and the potential to work in bulk.

Such a CLI tool can take the minified content of a JS or CSS file using the standard input and output the unminified content using the standard output. The default space indentation can be set to two spaces, but can be overridden via an input parameter ("indent"). For example, if we name the tool script webballoon.py to unminify the content of a file, we can call it on Linux or Mac like:

```
cat script.min.js | ./webballoon.py
```

or to use a custom indent of four spaces:

```
cat script.min.js | ./webballoon.py --indent 4
```

For implementation, Python 3 is a great choice, as it is installed by default on most Linux distros and has a huge number of packages for pretty much everything.

We start with the Python "shebang" line (`#!/usr/bin/python3`), which tells Bash to use the Python 3 interpreter if the file is called directly without passing it as a parameter to Python 3 (e.g. "./webballoon.py" instead of "python3 ./webballoon.py").

Next, we import the packages we need:

- *argparse* - to add support for input parameter parsing (for the "indent" optional parameter that we are going to use).
- *sys* - in order to use the standard input, output, and error streams and to specify script error code in case of unexpected input.

Although it might seem overkill to use a parameter parsing package for a single input parameter, the application might be further extended in the future, plus there's the advantage that you can call the script with a "-h" or "--help" parameter and it displays automatically generated help.

The `_get_indent_size` function is used to retrieve the value of the indent input parameter (defaults to 2 if the parameter is not specified). It uses the `_check_larger_than_zero` helper function to validate that the indent parameter has a specified value that's numeric and greater than zero.

We then use the `_get_indent_spaces` helper function to get a white space string of variable size that can be use to display the indent and the `_print_to_stream` helper function to print text to standard output stream without adding a new line at the end.

The core functionality resides in the main function. It is the module entry point and contains the input processing logic. It parses the input character-by-character and, based on the encountered characters, generates the output as follows:

1. In case the "{" character is encountered, it means that what will follow is in an inner scope, so we output "{", move to the next line, and output an increased indent.
2. In case the "}" character is encountered, it means that what will follow is in an outer scope, so we move to the next line, output a decreased indent, "}", move to the next line, and output the current indent.
3. In case the ";" character is encountered, it means that what will follow is on a separate line at the same indent, so we output ";", move to the next line, and output the indent.
4. In case the "," character is encountered, it means that multiple elements are separated, so we output a space followed by ",".
5. Any other character is outputted as is.

The full code listing below is available under Boost Software License 1.0 and is also available online at: `github.com/gearbx/webballoon`.

```
#!/usr/bin/python3

import argparse
import sys

_ BAD _ INPUT _ ERROR _ CODE = 1

def _ check _ larger _ than _ zero(value) -> int:
try:
v = int(value)
if v <= 0:
print(f"Invalid parameter value {value}", file=sys.stderr)
sys.exit( _ BAD _ INPUT _ ERROR _ CODE)
return v
except Exception:
print(f"Invalid parameter value {value}", file=sys.stderr)
sys.exit( _ BAD _ INPUT _ ERROR _ CODE)

def _ get _ indent _ size() -> int:
parser = argparse.ArgumentParser()
parser.add _ argument("--indent", type= _ check _ larger _ than _
➥zero, default=2, help="the indent size in spaces.(default 2)")
args = parser.parse _ args()
return args.indent

def _ get _ indent _ spaces(indent: int) -> str:
return " " * indent

def _ print _ to _ stream(text: str):
print(text, end="", file=sys.stdout)

def main():
indent _ increase = _ get _ indent _ size()
indent = 0
for line in sys.stdin:
for character in line:
if character == "{":
indent += indent _ increase
_ print _ to _ stream(" {\n" + _ get _ indent _ spaces(indent))
elif character == "}":
indent = max(0, indent - indent _ increase)
_ print _ to _ stream("\n" + _ get _ indent _ spaces(indent) + "}\n" +
➥_ get _ indent _ spaces(indent))
elif character == ";":
_ print _ to _ stream(";\n" + _ get _ indent _ spaces(indent))
elif character == ",":
_ print _ to _ stream(", ")
else:
_ print _ to _ stream(character)

if _ _ name _ _ == " _ _ main _ _ ":
Main()
```

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's summer here in the Pacific Northwest, and eagles are making my life miserable. The local eagle population has decided that our cell towers are a good spot to watch for rabbits, whose populations exploded over the spring. 5G equipment is particularly sensitive to line-of-sight interference, and eagles an automatic yellow card for interference. But they're a national symbol and a protected species and I can't do a single thing about them.

The eagles probably aren't responsible for unexpected roaming by our customers onto Canadian carriers, but they're as good a reason to blame as any around here, where radio signals scatter through trees and skip happily for miles across bodies of water. For a long while, this wasn't much of a problem, because U.S. carriers programmed their handsets not to easily roam onto Canadian networks. In fact, they did the opposite (and still do to some degree) and would lock onto the home network with a death grip.

These days, for whatever reason, our customers on the "borderlands" (as they are locally called) are landing on Canadian networks more often. Canadian carriers have gone on a building spree lately, investing heavily in growing network coverage as they build out their 5G networks while some have also added 700MHz 4G coverage. Frequencies are coordinated along the border, but Canadian carriers definitely aim for maximum advantage in covering the U.S. Our service is carefully tuned to stop working almost exactly when you cross the border. Depending upon where you are, theirs can be usable up to 20 miles inside the U.S. border.

Unexpected international roaming used to be something that carriers scrupulously avoided, and to some extent they still do. It created massive customer service problems whenever the bill showed up, given expensive international roaming charges. However, with the advent of cheap roaming agreements between North American carriers, U.S. carriers introduced service plans that include free roaming across North America. This means that a lot less effort is put into hunting down areas where Canadian carriers are effectively providing service to the U.S. side (not that much is likely to be done about these places anyway, because it'd involve investing in infrastructure, something U.S. carriers aren't especially inclined to do).

All of this is fine until someone calls 911, which creates a massive problem. People in panicked, stressed situations aren't always situationally aware of whether they are using a Canadian tower, and a lot of place names sound the same in Washington and British Columbia. So it can take awhile for the 911 operator to work out what's happening and where the caller is, and transfer them to the correct Public Safety Access Point (PSAP). That is, if they even know the correct PSAP. Often they don't. A 911 caller in western Washington will usually be in either San Juan or Whatcom counties, but not necessarily. This could mean a merry-go-round of transfers between PSAPs before a distressed caller (potentially in a life-or-death situation) is connected to the correct first responders.

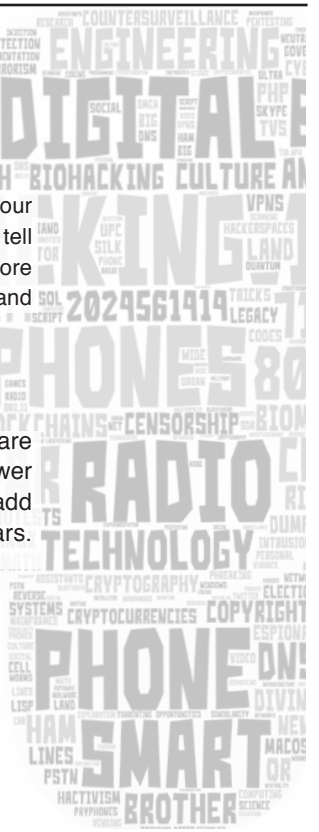
Enter Northern911, which is based in Sudbury, Ontario. This company has provided PSAP services to independent and VoIP

carriers for decades, and is essentially the "oddball PSAP." Owing to the geographically vast territory that they serve, their dispatchers are much more geographically aware than most and have an index of every PSAP in North America, along with the ability to transfer over primary e911 trunks into most of them. In fact, they operate a freemium "911 for 911" service, where 911 operators can call 1-866-869-9959 for assistance with properly routing the call. This is much faster than other commonly used methods such as NENA directory searches, and is likely to yield more accurate information (given that Northern911 dispatchers have considerable human expertise in which PSAPs serve what geographies). Up to five calls per month are free, after which Northern911 operates on a subscription model.

In emergencies, seconds can matter, and chat bots haven't been able to effectively replace 911 operators yet. And if you're having an emergency along the Canadian border and end up with a 911 dispatcher on the wrong side, there's a very good chance that some folks in Sudbury will be involved in figuring out where you are, and which first responders will be helping you. And with that, if you're one of the thousands of people swarming to the borderlands to enjoy the great outdoors this summer, please enjoy them safely. There are any number of emergencies that simply didn't need to happen or result in a 911 call, particularly those involving cliff diving, guns, and fireworks.

One thing that will be safe this summer? A New HOPE! Hopefully, I will have seen you there in New York when it happened in July. And with that, I'll be back to doing everything I legally can to encourage these eagles to fly north across the border and harass a Canadian carrier's towers.

WRITERS NEEDED!



There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at:

2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Problem of Effective and Usable Strong Passwords

by William Ben Bellamy Jr.

Note that in this article the word "password" is used for both singular words (strings) and phrases that are used as a password.

This article will focus on the following points:

- How are passwords attacked
- What makes a password strong
- Suggestions for building effectively strong passwords

Problem Statement

Typically, we each have dozens of passwords that we use regularly. Passwords help to protect the confidentiality, integrity, and availability of the systems and services we rely on.

For the past few decades we have been indoctrinated to think that each system requires a password that is:

- unique
- at least eight characters long
- composed from several character sets
- changed regularly

Compounding the problem is that each system/service that requires password authentication can enforce different requirements.

This is not sustainable. It forces the typical person to cut corners and look for "easy" passwords which leads to writing passwords onto paper near their systems, and using easily guessable words and phrases.

I propose that a practical and sustainable solution involves taking into account the techniques that password attacks (cracking) employ, and avoiding those techniques in order to produce passwords that are unlikely to be guessed.

How Passwords Work

When you type in your password, which is simply a string of characters, your system immediately calculates the hash value of that string. A hash value is produced by an algorithm that accepts any type or amount of material and outputs a fixed length value that uniquely represents the input material, but that cannot be reversed to find the original input material. It then sends the hash value to another system as proof that you are who you say you are - someone with permissions to access that system or service. That system - and network - only ever sees the hash value of your password, never the actual password.

The backend system compares the hash value you provided with its own stored copy of your password's hash value. If the two match, it can be assumed that you typed the correct password and have some degree of authorization on that system. If they do not match, then the correct password was not provided and no access is granted.

How Passwords Are Cracked

An attacker who has access to the password hash for an account/service will attempt to "crack" the hash value in order to learn the original password that was used to create that hash value and consequently have access to that protected resource or system.

There are two main approaches to cracking passwords: online and offline.

- Offline cracking generates the hash value of each password candidate and compares it to the hash value being cracked. Tools include John the Ripper, Hashcat, and rainbow tables.
- Online cracking submits generated hash values of password candidates to an online system in real-time until access is granted. Tools include Hydra.

Passwords usually are represented by their "hash value." A hash is a mathematical function that accepts any amount or type of material and produces a fixed length value that identifies the input material - both the content and the order - and which is computationally infeasible to reverse the process to determine a password given its hash value. If any portion of that material is changed, the fresh hash will be dramatically different from the previous. Also, it is mathematically infeasible to reverse a hash back to its original input. So a hash is like an absolutely precise fingerprint of the original material.

"Password cracking" is the process of working through a word list, and taking each word and hashing it in the same way that an unknown password was hashed. The two hashes are then compared and, if they match, you now know the original password. If they do not match, you try the next word in your list.

In addition, "rules" are applied to each word from your list. These rules describe how the initial word should be modified, manipulated, or in some way changed. These changes are intended to test variations on a word in ways that a person is likely to modify a common word in order to harden their password. The language used for rules is rather obscure and difficult to master. So most crackers will rely on existing rule sets rather than fine-tune them for a specific target. The actual word list, however, is often created with a specific target in mind.

These manipulations include, along with many, many more:

- changing letter case
- appending numerals or spaces
- prepending numerals
- inserting special characters

In this way, a single word from a word list can be morphed into hundreds of variations, most of which the attacker might never think of.

What Makes a Password "Strong"?

There are at least four factors that we can easily control that determine how strong a password is.

1. *The number of characters making up the password*. The more the better. Each additional character astronomically multiples the number of guesses required. Eventually the attacker will reach a point of diminishing returns and terminate the attack.

2. *The size of character sets*. A character set is a collection of related characters. For example, uppercase English letters, lowercase English letters, Arabic numerals, Roman numerals, special characters, and so on.

The more character sets we use in a password, the stronger it will be.

It takes ten symbols to represent the Arabic numerals 0-9. It takes 26 symbols to represent the lowercase English alphabet. So, in general, it is better to use larger character sets, and several of them.

- Alpha (upper and lower) =52 (a-z and A_Z)
- Numerals =10 (0-9)
- Roman Numerals =3 characters in 4 combinations and 1-4 symbols (I-X) (there is no zero)
- Typable special characters =~32
- Alt-characters (extended ASCII) (~129-255) 126 (`sites.psu.edu/➥symbolcodes/windows/➥codealt`, `www.alt-codes.net`)
- Unicode - astronomical count, but often impractical to type. (Unicode charts: `www.unicode.org/charts`) (Typing Unicode: `en.wikipedia.org/wiki/➥Unicode_input`)

So the size of a character space composed of upper and lower alpha, numerals, and special characters combined is ~94 potential characters.

3. *Length of the password*. It is that simple, yet extremely powerful. The longer the better. Every additional character dramatically increases the number of possible character combinations (complexity), making it increasingly computationally infeasible to successfully crack/guess.

4. *Frequency of Change*. A password is effective only for as long as it takes to crack/guess it. The previous steps will increase the time necessary to crack/guess your password to the point it is no longer feasible for an attacker to continue.

A Suggested Solution

The following suggestions will help create effectively strong passwords. You can use some or all of these to build a password. Remember that the key to an effectively strong password is the length of the string and the size of the character space.

Assuming your password is effectively attack-resistant to the point it is unlikely to be cracked, you can consider using a single password on many systems, and for a long time. And in any case, if it is cracked, the information about you on one system usually does point to the other systems you use.

General Suggestions

- Use all the character sets you can. This increases the overall character space size.
- Build a password that is at least 16 characters in length - preferably more than 24 (more on how to make that usable and practical towards the end).

The Detailed Steps

- *Decide on more than two core words/strings that will make up your password*. Select words/strings that together give you at least 16 to 24 or more characters. When choosing these words, try to have the first word begin with a lower case letter greater than "m". That way, if the word list is sorted, about the first half of the word list will be processed needlessly. Consider the following:

  - an obscure word you would like to learn to spell

- the name of a plant, insect, location, star, element...
- a favorite song title or phrase, a short portion from a poem, scripture...

- *Include a random string at some point*. Consider:
  - random keystrokes
  - a car license plate number or portion you happen to see (i.e., YEO-862)
  - keyboard geometry
  - product serial number
  - a MAC network address
  - the year of your favorite movie
- *Include spaces as delimiters between the words*. For extra strength, use two or more characters (space, underscore, hyphen...) as mixed delimiters.
- *Include an alt character*. This is very powerful since it is seldom in a password cracker's rules set, and it expands the character space astronomically. You will need to research how to enter ALT characters on your particular system. (One way to make entering ALT and Unicode characters easier is to, in some very secure way, save your full password and simply copy and paste it when needed.)
- *Even better, include an obscure Unicode character*. Again, you will need to research how to enter Unicode characters on your particular system.
- *Use geeking*. Geeking is the practice of exchanging regular characters for others of similar shape or sound. When using geeking, do not use the first opportunity, or all opportunities. For example, if you could geek five characters, then actually only geek two. Below are just a few examples:

```
0 - O
7 - T
@ - a
Vv - w
Nn - m
$ - S
/ - l
( - c
```

In addition, you can use the core portion of a password over and over and simply increment one character, the salt:

- Increment for each new password. For example, left to right across the shifted top row of numerals (~ to +). This is much more powerful than simply incriminating a numeral.
- Increment through the alphabet (a, b, c...) rather than numerically.

Things Not to Include in Building a Password

- unaltered dictionary words, even in combination
- regional terms ("go cats", "go cards")
- simple misspelled words (hackorz)
- nomenclature (leet, script kitty)

An Example

In this example, note that I am not using all of the possible suggestions. Use those that will help create a long and complex string that frustrates the techniques attackers use to crack/guess passwords.

- *Choose three core words*. Let's use "mood hack coffee". In this case, "mood hack" is a phrase with meaning, and coffee is (sort of) unrelated. This also starts with an "m" or beyond.
- *Add a random string (keyboard geometry):* "[poi". This give me "mood hack [poi coffee".
- *Mixed letter case:* "mood Hack [poi Coffee". Here I change only two letters to uppercase.
- *Geeking:* "nnood Ha(k [poi Coffee". Now I change "m" to "nn" giving me an extra character along with geeking, and is also later than "m" in the alphabet. I also change "c" to "(".
- *Include numerals:* "nnood Ha(k [poi C0ffee". Simply a "o" to an "0". Again geeking, but for the purpose of including at least one numeral.
- *Large string length (more than 16):* is now 22.
- *Use more than one character set:* Here I have uppercase, lowercase, special characters, numerals. That is a character space of ~94 characters.
- *Then for good measure, I append two spaces:* "nnood Ha(k [poi C0ffee ". This gives me 24 characters. That means that this password is one out of ~94 to the power of 24 (divided by two if you want to account for the average number of guesses) possible combinations. That is a really big number of guesses on average to discover this password.

How to Remember a Strong Password

So far, great. We have the information for developing a functionally strong password, one that is crack/guess-resistant. But, now we have to remember that long string of characters. Regardless of how effective a password is, if it is not easy to remember and use, it won't remain effective.

Fortunately, there is no real difference

between the words and phrases we have already learned as language and those that are contrived for use as passwords. So to "learn" these stronger passwords, simply use the techniques we used to memorize all of the words and phrases we already know.

1. *Keep the length relatively short: 24-32 characters*. Balance the number or words with their aggregate length. For example, two short words and one long word, or two long words and one short word. I find that less than 33 characters is comfortable as long as there is a meaning underneath that makes sense to me.

2. *Make the component words memorable*. The password needs to be thought of as a single idea rather than a bunch of keystrokes.

In the example "nnood Ha(k [poi C0ffee ", the core idea is "Mood hack with coffee". "Mood" uses "nn". "Hack" uses "(". "[poi" is just easy to type filler. "Coffee" simply uses a zero. Then end with two spaces. And spaces used as delimiters. Just a few tweaks on three words that constitute a meaningful phrase.

3. *Muscle memory*. Open an editor and type your new password over and over until your fingers are comfortable with the movements that are used. Start slow and deliberate, and increase the speed as you are comfortable. The key is that after a short while you will stop thinking about the individual characters you are typing and begin to understand them as a few words, and finally as one movement.

For example, type the following:

```
the dir path xcopy format
➥python list computer host
```

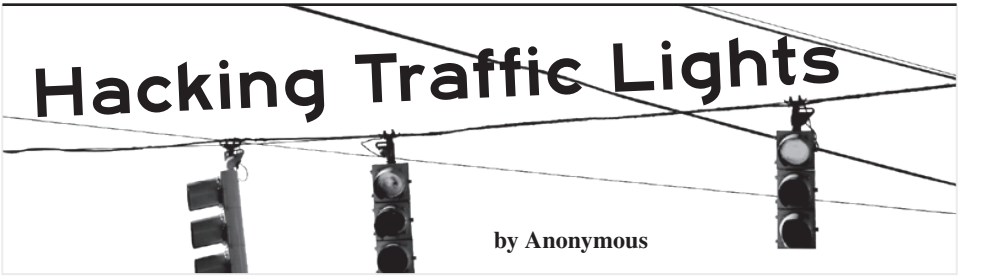
Notice how your mind and fingers know commonly typed material as a single movement (each word is a single movement). You do not think about each letter or the order of letters, you simply think about the word. It is the same as playing a musical instrument. Your hands know how to play an F chord rather than getting each finger to a particular place on your instrument. A G major scale is one long movement rather than a bunch of delicate movements.

So practice typing your new password until it is more automatic than deliberate.

Conclusion

This approach, or some variation on it, should allow you to consider using a single password on several systems, and for a longer time. That is because if your password hash is stolen, the attacker is unlikely to crack/guess such a long complex password.

This approach should also help make longer more complex passwords memorable and usable.



Hacking Traffic Lights

by Anonymous

Ah, the lowly traffic light. Faithfully rotating through a sequence of colored patterns, hour by hour, day by day. Being found at nearly every busy intersection, we think nothing special of them. Even less attention is paid to the nondescript metal cabinet resting just off the side of the road by every traffic light. This cabinet is generally the size of a refrigerator if standing alone, or a microwave if on a light pole. Most are unpainted plain metal boxes, designed to not attract attention. Do not be fooled, friend! Inside this cabinet, hidden in plain sight, is a wonderland of blinken lights, electronics, and computers!

But alas, the cabinet is locked. Do not be dismayed! It is but a simple tumbler, easily conquered. And if you are lazy, you can purchase a key for a few dollars online, as nearly all cabinets use one of a handful of keys. If you do obtain a key, you may find that it also opens other nearby cabinets. Even without a key, the thin sheet metal of the cabinet affords little real security from a determined individual.

Once inside the cabinet, you will find a hacker's dreamland of lights, wires, and switches. How does all this work? I am glad you asked! The heart of it all is the signal controller. This single machine controls all of the traffic lights. In the old days, these were mechanical, much like a clock. Later, microcontrollers were introduced and some still use these. However, today the trend is to

use controllers with embedded Linux.

Oh, did I mention these controllers are often networked together? Let that sink in a bit. Across the USA in particular, traffic lights are being controlled by networked Linux computers. Do you suppose these are installed by security professionals who change default passwords, disable SSH, HTTP admin portals, etc.? Or are they installed wide open as to be operated by city or town workers over a supposed "secure" network?

But wait, there's more! Consider that some traffic lights are remotely accessed via public IP address and connection from an Internet provider. One wonders if a security professional has configured and installed a firewall for these devices? Some, if not most, traffic controllers can be set with a password. This is often just a four-digit PIN. A look around the cabinet and you might even find it sketched on a scrape of paper.

The bottom of the cabinet contains rows of flashing metal "bricks." These are the load switches which translate the low voltage of the controller signal to 110 or 220 for the traffic light to operate. Be very careful! You will also find several switches on the inside of the cabinet door or just inside the cabinet. These may be used to reset the signal controller, manually cycle the signal, or place the traffic light in all red flash! Nearly every modern cabinet has a monitor that will not allow the traffic lights to go "all green" and in general will prevent any dangerous combination of lights to appear. If you try, the signal will enter "all red flash" as a protection. For your own safety, it is best to avoid this section of the cabinet.

Traffic lights are controlled by a combination of "detection" and "timing." The traffic light may have a timing cycle which runs from one to three minutes. Within this "cycle," a predetermined slice of the cycle is given to each light. However, if a vehicle is "detected," more time may be given to a particular light. Detection may be by buried wire loops which detect the metal of a vehicle. These wires are fed back to the cabinet into a "detector" (more blinken lights!) that tells the controller a vehicle has arrived. However, sophisticated camera systems are increasingly in use. You may find a video monitor in the cabinet which you may use to monitor the video from each camera. If not, every video system has a processor which can be accessed with a computer via serial or local Ethernet link. From this interface, you can view and edit the zones where the vehicles are detected. Microwave radar systems are also used to detect vehicles at traffic signals. These systems also have processors and, much like the video processors described above, can be accessed from the cabinet (or even remotely if networked). There are even Infrared and AI powered systems in some locations.

Most of the devices described above communicate over Ethernet. However, in many cabinets the primary communication protocol is Serial Data Link Control (SDLC) bus. SDLC is a fascinating protocol from the early years of computer networking. Unless you have been working with computers for a very long time, you probably have no idea what an SDLC bus is. As a quick introduction, SDLC is a 1970s-era frame-based data bus created by IBM to network machines over phone lines, satellite, and inter-building links (think Cold War, missile silos and PDP-11s). Hardly anything modern uses this protocol, save traffic lights. That said, SDLC is a very robust, well documented protocol and preserves a good deal of networking history. Along with SDLC, you will find RS-232 and RS-485 serial protocols commonly used to network within and between cabinets. As a rule, these protocols work with no authentication or encryption.

Traffic cabinets, in the USA at least, are a relic of a simpler time when high security meant a five pin brass tumbler lock. The serious truth is that traffic cabinets are ridiculously insecure, physically. Once physical access is gained, the cabinet is pwned. Even more disturbing is that if one cabinet in a series of network cabinets is breached, all of the cabinets are now pwned. If one of these cabinets has Internet access and this Internet connection is breached, the entire network of traffic signals will be compromised, without the need for physical access. I should not need to elaborate further the seriousness of such a situation for public safety.

Considering how vulnerable and valuable these systems are, why are we not seeing more attacks? Either these system have not caught the eye of would-be attackers, or they have already been compromised. Which do you think is more likely?

I'll Take Some Vigenère With My Caesar

by snooze

To brush up on my (extremely minimal) crypto skills, I recently began reading *Serious Cryptography*, which made me want to implement some of the concepts I was learning. For those of you who are unaware of what a Caesar cipher is, it is a pretty simple concept. You basically "encrypt" a message by rotating each letter of an input plaintext by three characters each time, and wrap around to the beginning of the alphabet if your "plus three" rotation ends after "Z."

For example, the letter A becomes D, and Z becomes C, so on and so forth. You would see the following in a Caesar encrypted message:

If you are familiar with this concept, you might also know it to be referred to as "ROT-3" encoding, where the ROT stands for Rotation and the number 3 refers to the amount of characters. Note that since there are 26 characters in the alphabet, you can expand on the Caesar cipher by changing that particular variable.

What I wanted to discuss next is what happens when we actually use a "key" to determine how much each letter gets rotated by since this is a bit more interesting. Pretend we had a key of "HAK" for the same "TESTZ" string above. "H," "A," and "K" give us ROT-7, ROT-0, and ROT-10, respectively. Since TESTZ has more characters than our key, we simply repeat the key the length of TESTZ, which would be "H A K H A." That results in the following output:

This is an example of the Vigenère cipher which, while more "secure" than the Caesar/ROT-3 cipher that came before it, is still comically insecure by today's standards and should not be used for anything remotely important. That said, I wanted to see if I could write an algorithm that accepts a key as input from a user, then encrypt a plaintext using said key, providing the corresponding ciphertext as output.

Grabbing user input and validating the key as alphabetical is easy enough:

```
import string
alpha = string.ascii _ lowercase

plainText = input("Enter your
➥plaintext to be encrypted: ")
userKey = input("Enter your
➥alphabetical key; exits on
➥invalid character: ")
cipherText = ''

# Check validity of key; for
➥demonstration purposes I only
➥accept alphabet characters

for char in userKey:
 if char.lower() not in alpha:
  print("Invalid key;
quitting.")
  quit()
 else:
  rot = alpha.index(char)
  print(rot)
```

If you run the above, you see that we get the "ROT" numbers as listed (7, 0, 10) previously. Now the first dilemma comes up; we need to repeat the key "HAK" once it runs out of characters due to our plaintext being longer than the key itself. After some sleuthing, it appears itertools.cycle is a great answer for this problem.

```
from itertools import cycle
cyc = cycle(userKey)

for char, rot in zip(plainText,
➥cyc):
 print(char, alpha.index(rot))
```

This gives us the following output and provides the logic we are looking for:

```
Enter your plaintext to be
➥encrypted: testz
Enter your alphabetical key;
➥exits on invalid character:
hak
t 7
e 0
s 10
t 7
z 0
```

Now it is time to utilize a ROT encoding algorithm which, as mentioned, I wrote previously. That said, I just added it to my code as a function called rotateChar and made some modifications to handle non-alphabetical characters and varying letter case. The full, somewhat commented code:

```
from itertools import cycle
import string
alpha = string.ascii _ lowercase

plainText = input("Enter your
➥plaintext to be encrypted: ")
userKey = input("Enter your
➥alphabetical key; exits on
➥invalid character: ").lower()
cipherText = ''
cycKey = cycle(userKey)

# Caesar/ROT Function

def rotateChar(s: str, rotate:
➥int):
 out = ''
 boolUpper = s.isupper()
 s = s.lower()
 if s not in alpha:
  out = s
 elif s in alpha and alpha.
➥index(s) + rotate > 25:
  if boolUpper:
   out = alpha[((alpha.index(s)
+ ➥rotate) - 25) - 1].upper()
  else:
   out = alpha[((alpha.index(s)
+ ➥rotate) - 25) - 1]
 else:
  if boolUpper:
   out = alpha[alpha.index(s) +
➥rotate].upper()
  else:
   out = alpha[alpha.index(s) +
➥rotate]
 return out

# Check validity of key; for
➥demonstration purposes I only
➥accept alphabet characters

for char in userKey:
 if char.lower() not in alpha:
  print("Invalid key;
quitting.")
  quit()

# Create nested list(s) with
➥the proper ROT number for
each ➥string in the plaintext

refList = []

for char, rot in zip([char for
➥char in plainText if char.
➥lower() in alpha], cycKey):
 if char.lower() in alpha:
  refList.append([char, alpha.
➥index(rot)])

# Iterate through original
➥plaintext and rotate when a
➥legal character is at index 0
➥of refList then pop index 0.

for char in plainText:
 if refList and char ==
➥refList[0][0]:
  cipherText +=
rotateChar(char, refList[0][1])
  refList.pop(0)
 else:
  cipherText += char

print("Ciphertext:", cipherText)
```

You can save the above code to a new file and run it with python3 /path/to/file.py - otherwise, my sample output below:

```
$ python3 vigcipher.py
Enter your plaintext to be
➥encrypted: Testing our CIPHER!
Enter your alphabetical key;
➥exits on invalid character:
➥secret
Ciphertext: Liukmgy swi GBHLGI!
```

Overall, this was a fun exercise and I look forward to implementing more cryptographic algorithms in the future!

Applications, Places, System: A Personal View of Linux

by Matt Johnson ech0plex88@protonmail.com

It's June 26, 2002. My freshman year of college is over and a summer of relaxation begins. One year of college, one year of independence, one year of downloading MP3s through Kazaa, LimeWire, Grokster, Audiogalaxy, and others at 1.544 MBPS. I fell in love with electronic music in high school, and college amplified that emotion. It wasn't just trance but breakbeat and ambient via Musicforhackers.com; tagline "Soundscapes for compromising a remote host." When you're trudging through calculus homework, you can benefit from Aphex Twin or Brian Eno.

In Ottawa, Canada, the GNOME (GNU Network Object Model Environment) Foundation released version 2.0 of their desktop. As foundation president Miguel de Icaza stated, "The GNOME 2.0 project is the culmination of a major effort which had the dual objectives of dramatically improving developer productivity and significantly enhancing the GNOME user experience."[1]

Unfortunately, the significance was lost on me because I was only vaguely aware of Linux's existence. Beginning with my first family PC in 1995, a Packard Bell 486, I explored Windows 3.1 and 95. The world of DOS became clear, and I was able to configure boot disks with autoexec.bat and config.sys with ease. Whatever it took to run *Star Wars: TIE Fighter*, *Silent Service II*, *F117 Stealth Fighter 2.0*, or any number of 90s simulators. By the time I graduated high school, my PC skills were based in Windows. Our school had Apple PCs with those hockey puck mice, but they were oddities, like a Fiji mermaid or pickled cyclops piglet in a circus sideshow.

Then I was a college freshman with a brand new Compaq desktop running Windows XP, sifting through our campus LAN looking for unprotected folders full of MP3s. My games of choice were *Half-Life*, *Return to Castle Wolfenstein*, *American McGee's Alice* and *Quake III Arena*. Everything Just Worked. In the spring of 2002, a teacher's assistant offered a recommendation. "You should try this," he suggested, like a street corner pusher in a rain-soaked city.

It was a Knoppix live CD, a weird fascinating experience. What is this desktop environment? What's with this penguin? At the time, I didn't know it was a Debian-based distribution using KDE. I only knew it wasn't Windows and, although interesting, wasn't my preferred OS. The live CD was returned the next day, and I didn't think about Linux for another nine years. Amusingly, the Knoppix site looks like it hasn't changed in the past two decades, and that is no criticism.[2]

These nine years passed in a flurry of ones and zeroes. My computer interests shifted from the physical PC as an object of amazement to exploring the ever-expanding Internet. I embraced social media with Facebook before Myspace, due to having a .edu email address. The personal MP3 collection grew, while movies were more easily accessible through LimeWire and that greatest of file hosting sites, the late great Megaupload.[3] Then, in the summer of 2011 I had my next Linux experience. During those in-between years spent running Windows Vista and Windows 7, I missed a significant amount of drama in the FOSS world.

On June 7, 2008, Andy Wingo blogged that "The problem, as I see it, is that GNOME is in a state of decadence - we largely achieved what we set out to achieve, insofar as it was possible. Now our hands are full with dealing with entropic decay."[4] Dissatisfaction grew and GNOME 3.0 began to take shape.[5] Two years passed and the GNOME 2.x desktop environment was the default in many distributions, including SUSE Linux Enterprise, Red Hat Enterprise Linux, Fedora, Debian, Ubuntu, and Linux Mint. The timeline progressed:

- *April 29, 2010:* Ubuntu 10.04 LTS is released with GNOME 2.[6]
- *September 29, 2010:* GNOME 2.32 is released as the last major software version.[7]
- *October 10, 2010:* Ubuntu 10.10 is the last version released with GNOME 2.[8]
- *November 17, 2010:* GNOME 2.32.1 is released as the last iteration of the desktop environment.[9]
- *April 6, 2011:* GNOME 3.0 is released.[10]
- *April 28, 2011:* Ubuntu 11.04 is released with the Unity desktop environment.[11]

Why the emphasis on GNOME 2.x? That comes later. Why the emphasis on Ubuntu? I'll cover that now. In the summer of 2011, I bought a Cr-48 Chrome Notebook through Craigslist. This was Google's pilot experiment Chromebook, distributed in limited numbers to participants in the Chrome OS Pilot Program. The light minimalist "black slab" design, resembling the monolith from *2001: A Space Odyssey*, was attractive. It also seemed like a fun device for experimentation once I learned that conventional full-featured operating systems could replace the stock OS. Carefully following instructions, I successfully installed Ubuntu 11.04 Natty Narwhal.[12]

This was my first experience with Linux since

trying Knoppix in college. I didn't know anything about the enormous variety of distributions other than Ubuntu, which happened to be the most popular search result. I was completely unaware of the GNOME 2.x/GNOME 3.0 controversy, and how new desktop environments sprang up in its wake. This was an entirely recreational and experimental project that lasted for roughly one month. MacOS never interested me, Windows was the "old reliable," Linux (Ubuntu) was something new. Unity didn't bother me, as I had nothing to compare it with inside the Linux DE ecosystem. It was fun while it lasted, but as before I soon returned to Windows 7.

As I was testing Ubuntu, a more significant project was underway. On June 18, Argentine programmer Germán "Perberos" Perugorría posted an announcement on the Arch Linux[13], Ubuntu[14], and Linux Mint[15] forums. Disappointed with the disestablishment of GNOME 2.x, he spent six months forking the project into a continuation called MATE. Named for the traditional South American drink, the project was described as "a non-intuitive and unattractive desktop for users, using a traditional computing desktop metaphor." Perberos described the project philosophy as a representation of mate drink preparation through its culture of sharing, simplicity, and efficiency.[16] It wasn't long before he was contacted by Clement "Clem" Lefebvre, of Linux Mint fame, who assisted with expanded development of the desktop environment. Clem posted the first blog entry on the project's home page on December 5, 2011.[17]

I returned to Linux in time for the release of Ubuntu 16.04 LTS and fell into a downward spiral of distro hopping. Ubuntu, Debian, CentOS, Fedora, Antergos, Mint, and even setting up Arch from scratch. Lots of flirting without commitment; I suffered from option paralysis. The only aspect I settled on was a preference for the MATE desktop. Since its inception, the DE had propagated to every distribution. I first experienced it through Ubuntu MATE. As Perberos described it years earlier, I was drawn to and appreciated the efficiency and simplicity. Windows 8.1 and 10 were tolerated, not enjoyed. When the Windows 11 beta was leaked, I took it for a test drive and decided 2021 would be my Year of the Linux Desktop.

Linux revitalized my perspective of the PC as an environment in itself, not simply a tool for accessing the Internet. It has been a wonderful journey, more fulfilling than the endurance tests of Win 8/10/11. It calls back to my mid-90s adventures with DOS and boot disks. The idea of community development, globally-shared hobbies, enthusiastic support and Free and Open Source Software is immensely appealing. In contrast to the cold monolithic *closed* world of Enterprise software, Linux is *open*, with all the vibrancy and chaos that includes.

I credit Ubuntu with bringing a popular marketing campaign to Linux, without which I may have never taken the plunge. I also credit Perberos with epitomizing the idea of a software passion project, by working hard to resurrect a dead desktop environment through skill and enjoyment. MATE, and GNOME 2.x by extension, symbolize the Linux experience for me. Function over form; "unattractive and unintuitive." That three-tier menu, Applications-Places-System, as iconic an element as NCC-1701. Spanning years of FOSS development; inspiring countless retired GTK2 themes across DeviantArt, and perhaps most perfectly realized with the Ambiance and Radiance themes of Ubuntu 10.04 LTS. GNU/Linux is how I want to experience the digital world - Free as in Freedom.

[1] foundation.gnome.org/2002/06/26/gnome-2-0-released-desktop-environment-boasts-simpler-user-interface-and-a-host-of-powerful-developer-tools/

[2] knoppix.net/

[3] arstechnica.com/tech-policy/2012/01/why-the-feds-smashed-megaupload/

[4] wingolog.org/archives/2008/06/07/gnome-in-the-age-of-decadence

[5] arstechnica.com/information-technology/2008/07/gnome-3-0-officially-announced-and-explained/

[6] arstechnica.com/information-technology/2010/05/lucid-dream-ars-reviews-ubuntu-1004/

[7] help.gnome.org/misc/release-notes/2.32/

[8] arstechnica.com/information-technology/2010/10/ars-reviews-ubuntu-1010-wip/

[9] mail.gnome.org/archives/gnome-announce-list/2010-November/msg00056.html

[10] foundation.gnome.org/2011/04/06/gnome-3-0-released-better-for-users-developers-3/

[11] arstechnica.com/information-technology/2011/05/riding-the-narwhal-ars-reviews-unity-in-ubuntu-1104/

[12] chromeos-cr48.blogspot.com/2011/04/ubuntu-1104-for-cr-48-is-ready.html

[13] bbs.archlinux.org/viewtopic.php?id=121162

[14] ubuntuforums.org/showthread.php?p=11333073

[15] forums.linuxmint.com/viewtopic.php?t=86481

[16] pclosmag.com/html/Issues/201703/page01.html

[17] mate-desktop.org/blog/2011-12-05-introducing-mate-desktop/

Dial-a-Word

by N1xis10t N1xis10t@protonmail.ch

This software is for finding words in phone numbers (like 888-EYES) that you see government agencies and others using. Now, I'm pretty sure that they just pay the telephone companies extra so that they get special phone numbers. The idea behind this software is to provide the user with the ability to acquire numbers like that without paying extra.

Functionality

When you are setting up a phone line with the telephone company, what they typically do is give you an option to choose a randomly selected phone number, or have them randomly select another one. When they present you with a number, feed it into this program with no dashes or special characters (like xxx5243373 where "xxx" is an area code) and it will search the number to see if it has any words in it. If it does, it will show you what the number is in the format "xxx5-CHEESE." If it doesn't find anything, or if you don't like what it did find, have them show you another number and then check it. Repeat this until you find one that you like, or until the technician gets fed up with you.

Dependencies

This software requires that the file "google-10000-english.txt" be in the same folder. This is a file that has the 10,000 most common English words in it, and can easily be found on the Internet. I have limited this program to such a small dictionary because the running time is simply too long to be practical when you try to use an exhaustive list of English words. Feel free to try to use a better dictionary.

Notes

This software cannot find words that are less than three characters long, as a side effect of having to filter out garbage words from the dictionary. This could be fixed by removing the filter and using a better dictionary.

This software is only 6.5 kilobytes in size (not including the dictionary), and would easily fit on a 5.25 inch floppy disk.

Copyright Notice


```
# Import the dictionary
dicti = open("./google-10000-english.txt")
Dictionary = dicti.read().replace("\n", " ").split()
DictLen = len(Dictionary)
dicti.close()

# Define what letters the numbers can be
letters = {"1":"1", "2":"A B C", "3":"D E F", "4":"G H I", "5":"J K L",
"6":"M N O", "7":"P Q R S", "8":"T U V", "9":"W X Y Z", "0":"0"}

number = ""

# Garbage word filter
i=1
while i <= len(Dictionary)-1:
if len(Dictionary[i]) < 3:
del Dictionary[i]
i-=1
i+=1

# Enter the main loop
print("Type 'exit' to quit.")
```

```
while True:
printnums = "\n"
number = input("Number: ")
if number == "exit":
break
modnumber = ""
printnumber = ""

# Start iterating through all the possible letter combinations for
the number
for i in range(0, len(letters[number[0]].split())):
modnumber += letters[number[0]].split()[i]
for i in range(0, len(letters[number[1]].split())):
modnumber += letters[number[1]].split()[i]
for i in range(0, len(letters[number[2]].split())):
modnumber += letters[number[2]].split()[i]
for i in range(0, len(letters[number[3]].split())):
modnumber += letters[number[3]].split()[i]
for i in range(0, len(letters[number[4]].split())):
modnumber += letters[number[4]].split()[i]
for i in range(0, len(letters[number[5]].split())):
modnumber += letters[number[5]].split()[i]
for i in range(0, len(letters[number[6]].split())):
modnumber += letters[number[6]].split()[i]
for i in range(0, len(letters[number[7]].split())):
modnumber += letters[number[7]].split()[i]
for i in range(0, len(letters[number[8]].split())):
modnumber += letters[number[8]].split()[i]
for i in range(0, len(letters[number[9]].split())):
modnumber += letters[number[9]].split()[i]

# Once the current iteration has been assembled, check to see if it
has any English words in it
for i in range(0, len(Dictionary)):
if Dictionary[i].upper() in modnumber:
# If it does, and it's unique, add it to the list of numbers to be
printed out
word = Dictionary[i].upper()
wordlocation = modnumber.find(word)
printnumber = ("^" + number[0:wordlocation] + "-" + word + "-" +
➥number[wordlocation + len(word):] + "^").replace("^-", "").
replace("-^", "").replace("^", "")
if not printnumber in printnums:
printnums += printnumber + "\n"

# Take away the last character so a new one can be tried
modnumber = modnumber[0:9]
modnumber = modnumber[0:8]
modnumber = modnumber[0:7]
modnumber = modnumber[0:6]
modnumber = modnumber[0:5]
modnumber = modnumber[0:4]
modnumber = modnumber[0:3]
modnumber = modnumber[0:2]
modnumber = modnumber[0:1]
modnumber = ""

# Print the results
if printnums == "\n":
print("\nNo words found\n")
else: print(printnums)
```

The Hacker Perspective

by ZauxZaux

We're probably all writing these submissions from quarantine. We've had time to reflect. Time to fear. Time to have hope. If we're fortunate, we've had an easy adjustment to forced "work from home" since it was probably already a perk of our jobs. "What it means to be hacker." The first time I became interested in the term was in the 90s. I watched one of the infamous movies that involved such folk and became instantly fascinated. Coincidentally, it was also the same summer I got my first laptop. What a monstrosity. The worst battery life ever. Heavy as brick. Whirring fans and horrendous boot times. Oh how I loved it dearly.

After watching that movie, I was convinced that I, a fool, had been overlooking this whirring brick and not seeing it for what it truly was: a bastion of power, a futuristic piece of machinery that could enable me to traverse cyberspace and travel into places unknown. Or so I thought. The only command I learned how to run that summer was "dir", and I got as far as downloading Python and running some sample calculator program. But fuck if I knew what was really happening. I was defeated: code and programs and hacker stuff were the things of super geniuses and people going to fancy schools, not of small town folk like me, whose only computer class up to that point was typing, and some CAD class that I had no interest in. At the time, the would-be hacker dreams were snuffed out, I was resolved to AIM, Yahoo chat, online games, and whatever else kids of my age were getting into, and some of what they weren't.

Fast forward to 2015. I had made a proper disaster out of my life from high school to 2014, got a degree I would never use, a fair bit of debt to go with that silly degree, and not a clue as to what might be next. Fortunately, by 2015 I had managed to pull myself out of the hole I had dug and began making some sort of an actual "life," albeit very humble at the time. One thing I learned through all of it was that I was more capable than I gave myself credit for. With enough time, effort, and will, one could not only rectify what had since seemed a hopeless life, but could also do all sorts of things. Things like ride a bike 27 miles to work in the middle of a scorching summer because it was a choice between food and bike ride or gas and an empty belly.

That summer I delved back into Python again. It was just as inaccessible to me, but the amount of learning information online had since become abundant and I had plenty of time on my hands, seeing as I had started fresh in a new place and had minimal social contacts. I resolved to doing at least an hour a day on a common learning site. I tracked my progress in a notebook. I took notes. I wrote for loops on paper like some masochist. I dove into Linux. Perhaps, just like most things in life, with enough time, effort, and will I could learn this stuff.

Technology was again at the forefront of my mind for a bit; it resumed the same place of intrigue and curiosity that it had when I was a child. My fascination was nostalgic; I was no more a 20-something-year-old when I was delving into all this. I was a kid again, indulging to my mind's content for hours at a time, lost in the endless complexity while barely scratching the surface. What a time.

Fast forward another year. I found someone I loved. We began trying to plan our lives a little bit. At that point, I hadn't any better ideas than becoming a therapist. The other half said that was fine, but that we would both be broke. We laughed. That same summer, entertainment made another lasting impression on me. This time the theme was computer security. And I couldn't get enough of vigilante hackers. Down the rabbit hole I went, overloading my brain with all sorts of security information. "Did you know you could hack your own Wi-Fi?" "We got you

this gift for your birthday, can you tell us what the heck even is a Raspberry Pi?" I was convinced that this was the way forward.

I ditched the therapist idea and was resolved to getting into the tech industry as fast as possible. It would be a two-pronged approach. First, everything runs on software, right? So software engineering seemed like a good approach, and in the spare time, I could continue to indulge my infosec obsession. I began going to meetups. I applied to internships left and right and was rejected. I began working at a cell phone/computer repair store. I met people in industry, some great, some not. I made a home of a local hackerspace, volunteering time to help others starting the same path I was on.

Before I knew it, I had landed a low-level analyst position at a service provider. My mom thought I literally guarded the computers - like mall security, but in front of a computer. Then onward to an internal security team for a bank. My first "real job" in industry. They told me seven times between interview to first day "you know we do a follicle test, right?" I don't know if it was my long hair that I had let grow for the past year for the first time in my life, or if that's how all banks were. Joke was on them though, I'd been clean for over two years. There I learned what a great team looks like and how it functions. What a good boss is. What a good CISO is. I also learned that even if you can't type well, you can still be a killer analyst. My favorite analyst can't type for crap, but damn is he smart and funny as hell too. I miss you, my Nigerian friend - you're right "we've got it too easy!"

To me, being a hacker has been about connecting with others. Whatever that may look like. It could be your BFF at a job, you know, the coworker you're just a little bit closer with than the rest. Or it could be someone from the meetup; you've never been to each other's houses, but damn if you don't greet each other with a hug and a smile and know a bunch of little oddities about the other's life. It might be a teen-aged hacker that joined your hackthebox crew that just laughs when you say "you're miles ahead of where I was at when I was your age." Maybe it's the super whiz you know, the one that used to do some grayhat shit back in the day, the one that's a staunch open source proponent, that drops little gems here and there about opsec, or wild ass stories from other places, that has a garage full of servers and doesn't have to work anymore because they're rich off of Bitcoin, but is working at some new place because a good friend is the boss, and they want to see that person succeed. Maybe it's the leader of the hackerspace, the loud rambunctious one, that will say what's on everyone's mind, and maybe be embarrassing at times, but that's also one of the most selfless people you know; the one that offered you money which you were always too proud to take when you were out of work; the one that always offered and paid for lunch because they knew times were tough, and they never expected anything in return. It's the person you only knew by their handle and not their real name, that is until a former client from a contract job called looking for help, and then you thought "I know who needs this work more than I do right now..." so you had to message them to get their name and info; and they trusted you enough and ended up making a bit of coin. It's the person that thinks *you're* the whiz, but they don't realize that the only reason you know what you do now is because you paid way too much for power over the summer running your own server, and learned a million ways to break an operating system, including but not limited to: recursively chowning a dir and not giving a fuck; being super 1337 and encrypting your disk, then forgetting the password; banning yourself from a VPS because you were hitting the wrong IP; running commands on files with * instead of using tab completion because you were too impatient to train your muscle memory; rsyncing without a dry run and copying dest to source instead of source to dest; breaking your LAN because you didn't understand default gateways and only learned enough networking to get by... the cup runneth over.

Being a hacker has become to me just as much about bits and bytes as it is about others. It's about staying curious and continuing to learn. The transition to being someone that RTFM, and grinning nostalgically at someone whose shoes you were once in getting frustrated and turning to you for an answer. More importantly, it's

about being willing to give that answer. To extend the hand that was extended to you. Sometimes we go overboard. I do. I have to remind myself it's okay to say no sometimes. When I'm volunteering, I have to remind myself that I'm a volunteer, and a human first. If I'm not keeping myself sane and happy, then I'm damn sure not going to be pleasant or of much use to others. Being a hacker is about being humble. Being able to say "I don't know." Because, more often than not, I *don't* know. That's become more true in my new position. The first week I grasped the gravity of the situation and the fires we were putting out... the amount of change we were in. I had a sleepless night full of stress when it all sank in. "What have I done!? I gave up cushy cozy bank life for stress and a bit more coin.... *What a fool!*" Then a five minute meditation the next day before work put things back into perspective. I was amongst friends. Real friends, the same kind of friends I mentioned above. One of them gave me some solace: "You have to remember that a lot of this is screwed up, but also, it's not your fault that it's that way. Remember that." So when all is said and done, we'll either emerge, having managed to pull off the seemingly impossible, or we'll go on to other things - saner places with saner paces.

Being a hacker is about finding a way. Finding a way to get in. Going back over the port list; what service were we missing? Scouring through the commands again; what flag were we missing? Googling harder; what article was I missing where this was done the *right* way? Implementing logging in your scripts; if only someone had built a sane way to track the progression of your programs! Being obsessed with reverse engineering for three week chunks; hey, I solved it and know all these r2 commands... that will surely be gone the moment something else catches my curiosity. It's about people saying "you're always on your computer!" and then having enough sense to step back and take a break, cook something delicious, or watch something interesting. It's about not letting praise go to your head, not because you can't take a compliment, but because you are in tune with your place and you know when you have become a big fish in a small pond. It's about sending DMs to that super nice Twitter person, who selflessly had an open ear for your concerns career-wise and offered you whatever advice they could, and then subsequently congratulating you once things worked out in your favor but you forgot to tell them so you did it six months later. It's about empathy for another Twitter friend doing security work in your home state; their pictures of the landscape make you long for home, and as they're going through tough times you wonder what if life had been different and you had somehow stayed there and been able to befriend this person IRL.

It's about information warfare and your cognitive dissonance as bots flooded Twitter during a big election; how you knew, not exactly, what was going on and you watched the effects play out; how you debated whether or not it would be worth the time to try and discuss such events with your parents on Christmas break. Sometimes it's about getting a foreign language intel report, then tediously copy/pasting it into Google Translate and blasting the result on Twitter because people were looking for an English copy - only to have the team drop their appropriately translated version a day later.

Being a hacker means being able to go into the unknown of the technological realm as far as your curiosity will take you. Engaging in debates with others. Helping others. Learning from others. Staying up late. Drinking too much caffeine. Becoming wiser. Discovering your true self. Doing what you love. Being there for those that love you. Identifying with vigilante hackers. Begrudgingly going to vendor events. Disagreeing with friends. Lasting relationships, fading relationships. Excessive bandwidth. Cheap laptops with modded ram. Responding to inquisitive text messages with "download team viewer first." Sending a "Let me Google that for you" link when you're feeling like a turd. Learning to love a language, learning to hate a language. Upgrading shells to fully interactive TTYs. Mapping SMB shares. Loving operating systems, hating operating systems. Being a hacker is every bit as dualistic as anything else in life. Blackhats, whitehats, grayhats. Wherever you are, happy hacking. We can do it. It's not over. It's only just begun.

End of the Dream

by Sean Haas

As I'm sitting here in my office, the Russian invasion of Ukraine is ongoing. I'm half a world away, tucked in the fold of some undisclosed state. Despite that seeming isolation, I still have a connection to the conflict. I have a friend, a journalist we'll call K, who just got into Odessa. He's based out of eastern Europe and has been trying to get into Ukraine since the war started. He finally made it after a month and some change. K has been keeping up daily reporting about the war, his travels, and where he gets his information from. Since the conflict started, I've been noticing a pattern, something gnawing away at me. I think it's something I should have noticed earlier. The dream of the Internet is ending.

The biggest triumph of the Internet has been its ability to connect the world. Some locales may only have limited bandwidth, but there are few places the Internet hasn't at least touched. The free and rapid flow of information has fundamentally changed the state of the world. This hasn't been a slow change, or some shift in irrelevant policy. I'm talking about change that has occurred in our lifetime, change that affects most of us personally.

I remember struggling with a dial-up modem back in the day. I'd check my email every few days, maybe download a file or two overnight when no one was hogging the phone. Now I'm constantly connected to some networked something. Information flows right into my fingertips. Many of my friends I've never met face to face, but I can keep in touch with them as if they were sitting right here in my office.

The roots of the Internet are fundamentally militant and aggressive (look up Paul Baran's report on distributed networks if you want to feel some spook energy), but as the ARPANET matured it transmuted into something fundamentally different. The modern Internet is, by and large, a productive force that's made the world a smaller place. However, that may be approaching an end. What if the Internet no longer touched everywhere the sun shines? What if the free flow of information ran into a roadblock?

I don't think that you necessarily need to look at all sides equally when covering a conflict. People often lie, governments always have agendas, even something as mundane as the media that carries a message can color its content. Combat footage played over a radio show loses something in translation. However, I think it's always worth a few brain cells to look at what both sides are arguing. Sun Tzu said something to the effect of: "know your enemy and know yourself." Well, we mostly know ourselves, so information gathering is often an exercise in knowing the enemy. That includes knowing how the enemy presents itself to its citizens.

K and I are on the same page when it comes to this. The media lies, some media lies more than others, but it's still important to take a look. Know your enemy, know their lies, and know how they want to be seen. To that end, K often reports on Russian state media. It's all part of the blend that makes for good journalism. At the beginning of March, the European Commission announced moves to block content from Russia Today and Sputnik. Maybe that's a good move, maybe it's not - I'm not here to argue either way. But it makes it a little harder to know your enemy.

The EU is using interesting tools to restrict this flow of information. The Commission is working with large tech companies to stop the spread of selected Russian news sources within the EU. They are using a legal framework to pressure private entities. In most cases, these entities, mainly social networks, are based outside of Europe. These are American companies that happen to do business within the EU's borders. To keep operating in that locale, you have to play by the rules.

The Kremlin has started enforcing similar policies. In the same timeframe, sites such as Facebook and Twitter have been blocked within Russia. The tools used here are different than in the west. Reporting makes it sound like these sites are blocked lower down on the network stack. In Russia this was done via, once again, legal actions. The intent of the EU and the Kremlin here is in unison: they both seek to control the free flow of information.

This is only the surface level of the story. Russia is also being disconnected on the infrastructure level. At least Lumen and Cogent have severed connections to the country. Lumen specifically is a possibly dangerous case. They are a Tier 1 ISP; that's one of the components that people reference when they talk about the "backbone" of the Internet. A single Tier 1 pulling out of Russia will probably just mean worse bandwidth, annoying but not an immediate disaster. What happens if more providers follow suit? What if there is political pressure at home to cease dealings with Russia? What if new laws within that country make it either dangerous or no longer profitable to operate there?

We can complicate the picture. There are 15 Tier 1 providers. These providers are based out of the United States, the U.K., Sweden, Spain, Japan, Italy, India, Hong Kong, Germany, and France (note that most of these are NATO countries). The reason these providers matter is that their networks can access any IP address in the world, at least in theory. If you have a hook into one,

then you are tied right into the information superhighway. Theoretically, if a regime were to alienate all those countries, then they could be totally isolated from the 'net.

We have yet to see a situation where a country is totally cut off from the Internet for an indefinite period of time. It seems that once the Internet arrives, it's there to stay. I'd guess the network is just too handy for governments to totally pull the plug, or it's proven too profitable to those who back regimes. That said, there are some nations that approach digital isolation.

The canonical example is always China and the so-called Great Firewall. It's well known that the Chinese government has gone to great lengths to restrict the flow of information in and out of the country. This ranges from censorship on government-regulated platforms to fully blocking certain services. All backed up by laws and regulations, of course. But even this firewall is surprisingly porous.

PCCW Global, a Tier 1 provider headquartered in Hong Kong, retains connections with mainland China. There's one backbone right there. Foreign operators can drop servers in China - it's just a bit of a process. About ten years ago, one of my coworkers spent a few months trying to get some servers colocated in China. They eventually gave up on the idea. At the time, it was just too expensive to justify, but it is possible. So while the Internet in China may look different, there is still a flow of information. There are broad swathes of the network that will still look the same.

Even a pariah state like North Korea is hooked into the World Wide Web, at least in theory. Access is severely restricted in-country, but they do have service providers that connect up to larger networks in China and Russia. Those, in turn, eventually find their way up to Tier 1 providers.

Practice is a different matter. North Korea actually offers a taste of where we might be headed. Internet access isn't just censored, it's hard to come by. Certain government agencies, schools, and research centers have a link to the outside world. For everyone else, there's Kwangmyong: North Korea's own intranet. This is a network isolated from the rest of the world. The technical details aren't entirely forthcoming, as one can imagine. It sounds like Kwangmyong is air gapped, or otherwise physically isolated from the good fiber of the wider world. It also appears to use the same protocols as the normal Internet. Everything is just in miniature, fully controlled by the North Korean government.

A network like this offers some distinct advantages to a regime. The reduction in scale makes censorship much easier. While systems like email and chat rooms supposedly exist inside this network, they operate on a smaller scale. Fewer users means fewer eyes are needed to track their movement. Total isolation ensures that your nice network can't be used as a vector for the wrong kind of ideas. No bad news comes in, no bad news goes out, and no international actors can compromise your network. Imagine the savings in security alone!

Someone connected to the Kwangmyong isn't just looking at some limited set of the overall Internet. They aren't connected to the Internet at all. Their networked world isn't made smaller, it just is small. So what happens if North Korea decides to invade South Korea? Let's say a journalist is trying to report on the conflict. How do you know your enemy if you can't even read their domestic news? How do you get sources on the ground if no one on the ground can shoot you an email? It's not that there's no information, there's just no flow.

We may be heading towards a wider adoption of the Kwangmyong approach. A nation wouldn't even have to be a pariah state to pull the plug on the Internet. North Korea has allocated IP addresses - they can route to the rest of the world. They've just chosen to isolate the vast majority of their network. This is, no doubt, partly due to internal political pressures and partly due to external pressures.

I think it's at least possible for a similar system to be implemented in any nation in the world. Cuba has a similar system in place; a connection to the Internet for a select few users, and government-controlled intranet for the balance. Myanmar has, at some points, maintained their own national intranet. In 2011, Iran announced their intention to develop a similar intranet.

We can also add Russia to this "maybe" list. In 2019, a slate of laws, sometimes called the Sovereign Internet laws, were passed. According to the State Duma these laws mandate the creation of a "national Internet traffic routing system" (`duma.gov.ru/news/44551/`). This system can serve as a centralized means of censorship and tracking. It can just as easily serve as a choke point to switch Russia from the Internet to its very own intranet.

At what point does the balance of financial and political pressure cause that switch to be flipped? I think we might find out soon.

Where does that leave the Internet? Maybe it sees a downgrade, maybe it drops the big I. The death of the Internet may be even closer than we think. PRISM and similar projects administered by the U.S. government are already able to track Internet traffic. That takes some serious hardware and some serious access. It takes arrangements similar to those set up in Russia. I'd argue that the feds already have the technical ability to cut America's network off from the wider world. Can we truly consider the Internet free if that ability exists? Can the dream of the Internet come true while political actors can control its fate? I, for one, am savoring each packet I receive.

Why Exploiters Should Optimize Their Code

by greg

As far as Internet "bad actors," or "exploit bots," or simply "assholes" running code that tries to exploit websites for "shits 'n giggles" (or whatever reason) - by which I mean those who are simply looking to disrupt and to "hack" sites that have WordPress installed to take over admin accounts or to delete content - I have some things to say.

First, and foremost, I am not discussing those who would want to remotely (or otherwise) install malware or ransomware, but those actors who regularly use Hypertext Transfer Protocol (RFC2616 et.al.) directly to try to exploit websites.

Like this:

```
GET    /wp-includes/wlwmanifest.
➥xml HTTP/1.1
```

You should all know what I mean. (If not, keep reading *2600 Magazine*...)

If one *has* WordPress installed, that may be a legitimate request, but if one does *not* have a WordPress website (like my pathetic little static site), such a request *should not happen*.

Thing is, they do. They occur, literally, about one thousand times per month. That ain't the problem, per se, as my site don't care. To it, it's just a 404 - which I make the response just a few bytes directly by Apache's .htaccess file.

The thing is, multiply that by one billion websites and the entire Internets slow down.

Get it?

Obviously, WordPress is not the only code being exploited every second of every day over the entire Internets. I am using that as just one example. I am not mentioning the 2,000 or so other "CMS" software with exploits....

A few thousand, few byte, 404s per month? Yes, no big deal. But it's more than that.

1. Exploit code does not just try for that one file, they try for dozens of path variations.

2. Exploit code does not use a single IP address or User-Agent string.

3. Exploit code does not give up. Ever.

All this means is that one cannot block them easily. Deny by IP? Losing battle. Deny by request strings? Losing battle.

Again, I am thinking of just WordPress shit. (If you have WordPress, more on that later.)

The simplest blocking mechanism is this Apache configuration:

```
ErrorDocument 404 "FU"
RedirectMatch 404 "(?i:wp|wordpr
➥ess|admin|xmlrpc)"
```

That won't cover all, but it is the basic example to stop 90 percent of WordPress exploits upon first request before loading one's own massive 50MB+ CMS! (One can see how just a few more strings in the match list can help.)

Now, to the point of this article, an appeal to *exploit code authors*. Yes, that is exactly what I am doing.

This appeal is based on one simple little obvious fact: `GET / HTTP/1.1` and then look at the results and *see if any WordPress signature is there!* And there will be! For WordPress *informs everyone that it is a WordPress site!*

Therefore, to all Wordpress exploit coders, just check the root page and if WordPress is not indicated, *stop further requests and move on to your next target!*

Let me add here a log excerpt of an example of some WordPress exploit code. Instead of wasting *2600 Magazine's* valuable space, I will not excerpt the entire log blurb but the files requested - each request just one or less seconds apart:

```
/
/
/wp-includes/wlwmanifest.xml
/xmlrpc.php?rsd
/
/blog/wp-includes/wlwmanifest.xml
/web/wp-includes/wlwmanifest.xml
/wordpress/wp-includes/
➥wlwmanifest.xml
/website/wp-includes/wlwmanifest.
➥xml
/wp/wp-includes/wlwmanifest.xml
/news/wp-includes/wlwmanifest.xml
/2020/wp-includes/wlwmanifest.xml
/2019/wp-includes/wlwmanifest.xml
/shop/wp-includes/wlwmanifest.xml
/wp1/wp-includes/wlwmanifest.xml
/test/wp-includes/wlwmanifest.xml
/wp2/wp-includes/wlwmanifest.xml
/site/wp-includes/wlwmanifest.xml
/cms/wp-includes/wlwmanifest.xml
/sito/wp-includes/wlwmanifest.xml
```

Let me remind you that this happens thousands

of times *per month* on just my no good, static website. But who cares, right?

You need some math: *billions of websites every second of every day*.

Ignoring *all other exploitable web code*....

Here is the crux of the title to this article:

I appeal to all WordPress exploit coders to please check the root page and, if WordPress is not indicated, move on to your next target!

My criticism is, are you coders or are you assholes?

Fine with your exploit coding! Just, please, for the sake of the world, *do it right!* Blind requests like the above example, is... *simply pissant amateur coding*.

None of you are hackers. None of you are doing anything but declaring, "I am an Idiot Script Kiddie." Grow up.

Hacking into the Past

by Curtis Vaughan

In my youth, I would take apart various electronic games, un-soldering and re-soldering them, and taking pride in the fact that that the successful operation on the device worked. However, with respect to my first computer - a TRS-80 - it would have been beyond all reason to vivisect such an investment. An old TV, a radio? Who cared? But my computer? No way.

Back then, computer magazines would advertise computers that you could assemble yourself. Although interesting, I did not have the confidence to build a computer, nor the resources.

Time jump to the late 20th century: then an adult without any technical training, I often fixed tower computers and even built a few. Jump again to today and the advancements in technology - most computers are single-board devices. Alas, there's nothing to assemble and little that can be repaired. Not that that has stopped me.

A few years ago while browsing the web, I discovered PDP kit replicas. Intrigued by the possibility of not only building, but operating, my own PDP-8, I took the bait. Thus began my new hobby into vintage computers.

Big time jump to the dawn of microcomputing, albeit through the lens of retro kits. Starting with the PiDP-8/1, I then went on to build a PiDP-112, an Altair 88003, an IMSAI 80804, and finally a KIM-15 - all computers that I had only read about were now at my fingertips.

Building them was only the beginning of the adventure. Although sometimes challenging, the real work was figuring out just how to operate the various systems. What could one do with them? What programs could be run? This is where things get really interesting or, depending on one's disposition, quite dull. You will have to dive into reams of documentation, which is often somewhat esoteric. In additional to technical documentation, the magazines of the era (most of which are available at archive.org) will also further one's submersion into the past.

With my curiosity piqued, I began to collect vintage computers: Kaypro 4, HP 54B, Poqet Pocket Computer, Heathkit M4100, and various TRS computers, including the TRS-80 Model 1 - back to my very first computer.

Perhaps because I'm a Linux user, I'm also something of a Luddite. As I often use terminal-based programs instead of perfectly reasonable GUI applications, it was natural to use various text-based programs and games on these computers. Of course, I've played my fair share of text adventure games, but there were terminal-based versions of *Lunar Lander*, *Pacman*, and *Donkey Kong*. Although I had used computers during the BBS

age, I never had a modem, so it was an adventure for me to visit still existing BBSes from these systems.

To further challenge myself, I discovered Wordstar for the Kaypro. I vaguely recall knowing about Wordstar, but I had never used it. But now, there it was waiting to be "newly" exploited. As with vintage hardware, one will find another adventure into the past figuring out how to use vintage software. In this case, I decided to fully immerse myself and write part of this article on Wordstar. Due to the modern-day demands of the *2600* editorial staff, however, I could not submit this article in Wordstar format and had to deal with conversion issues. Again, learning! I was quite impressed by how capable Wordstar is and wondered whether we really need such complex word processing programs today?

Part of this article was also written in AlphaWorks on the extremely portable Poqet Computer. The major hurdle in this case was getting files off the proprietary PCMCIA memory cards used by the Poqet. Prior to using the Poqet to compose anything, I had to figure out how to access the PCMCIA cards from another computer. After days of trial and error, I finally found an old PC tower, onto which I was able to install Windows 95 and get a PCMCIA adapter to work with said cards. There were so many times when I was ready to give up, but success meant a much greater appreciation of this first-generation pocket computer.

I would encourage readers to invest in at least one of these vintage projects. Whether you have ever soldered before or not, you'll get the hang of it pretty quickly. I hadn't done any soldering in 40-odd years! As you solder away, imagine those early computer designers planning out the boards, circuits, etc. I have no idea how one does that.

I know there are many out there who cannot understand why one needs the vintage hardware when one can simply run an emulator. Undoubtedly, I could never afford every bit of vintage hardware and have on many occasions run emulators. But if you are not sitting in front of a device that sounds like a prop airplane, ensconced in the smell of overly heated electronics, bathed in the strobing warmth of a CRT, then you will never puncture through the firmament holding you in the present. The past will remain an illusion.

Once you start down this journey, you will want to join in relevant user groups, as they provide a plethora of information and assistance. I was also amazed to discover that there are many enthusiasts who have gone through the trouble of developing accessories to these, dare I say, outmoded computers, making them very competent devices.

Needless to say, I do live in the present, but now I have the option to hop behind one of my time machines and venture back to the vintage computer days.

References

obsolescence.wixsite.com/➥obsolescence/pidp-8
obsolescence.wixsite.com/➥obsolescence/pidp-11
adwaterandstir.com/altair/
thehighnibble.com/imsai8080
www.tindie.com/products/tkoak/➥pal-1-a-mos-6502-powered-➥computer-kit/

EFFecting Digital Freedom

by Jason Kelley

Supreme Court Decision Overturning Abortion Rights Is a Privacy Wakeup Call

Fair and meaningful protections for data privacy are essential to independence and autonomy in the modern era. Everyone deserves to have strong controls over the collection and use of information they necessarily leave behind as they go about their normal activities, like using apps, search engine queries, posting on social media, texting friends, and so on. But after June's Supreme Court ruling in *Dobbs v. Jackson Women's Health Organization*, people are becoming more aware than ever before that those controls are sorely lacking.

Today, the concern is over abortion access - and for good reason: changing laws across the country now mean that those seeking, offering, or facilitating abortion access must assume that any data they provide online or offline could be sought by law enforcement. But tomorrow, the concern could be over something else. It is essential to remember that what is currently legal may not always be legal, and that who is in power can always shift, along with what laws are enforced, and how.

This isn't idle speculation - digital trails have already been ransacked in the service of questionable prosecution. After the "J20" protest over U.S. election results in 2017, Department of Justice prosecutors served a search warrant on the hosting provider of a site that was dedicated to organizing and planning the protest. The request would have required DreamHost to turn over the IP logs of all visitors to the site - anyone who visited, whether journalist, activist, or just interested reader - but it was later narrowed after pushback (though that later request was not without its flaws). By early July 2018, federal prosecutors dropped many of the charges against many of the defendants in the case, but even this sort of overbroad demand for digital data has a chilling effect on future protest organizers.

To ensure that digital data isn't misused by companies, courts, law enforcement, or the government, EFF supports data privacy for all. There are three main fronts in the fight to protect digital privacy and, whoever you are, you can help.

First, there are basic steps everyone can take to minimize data collection. EFF recommends a variety of methods in our Surveillance Self-Defense guides, available at `ssd.eff.org`, as well as other guides on `EFF.org`. We've got tips for protesters (for example: removing fingerprint unlock and FaceID on your phone, enabling full-disk encryption on your devices and using encrypted chat). We've got recommendations for those in the abortion access movement (keeping more sensitive activities separate from your day-to-day ones, carefully reviewing the privacy settings on each app and account you use). And we've got basic guides for anyone who wants to take their privacy into their own hands, while recognizing that there is no one-size-fits-all digital security solution.

But it should not be entirely up to individual people to take these elaborate steps to protect their own privacy. Because privacy is a fundamental human right, it should be protected in law and statutes. Digital privacy protections in the U.S. are generally weak, and we all must push our local, state, and federal representatives to do better. Perhaps the most important thing we can do to minimize data harms is to ban online behavioral advertising, which creates staggering profits for tech companies by targeting ads to us based on our online behavior. This incentivizes all online actors to collect as much of our behavioral information as possible, and then sell it to ad tech companies and the data brokers that service them. This pervasive online behavioral surveillance apparatus is what turns our online lives into open books. But there are also smaller bills that help fill the gaps: for example, Rep. Sara Jacobs' "My Body, My Data" Act will protect the privacy and safety of people seeking reproductive health care. Specifically, this bill would restrict businesses and non-governmental organizations from collecting, using, retaining, or disclosing reproductive health information that isn't essential to providing the service someone asks them for. Regardless of where you live in the U.S., or in other parts of the globe, you can visit EFF's Action Center at `act.eff.org` to find out how to speak up for better laws.

Lastly, we must demand that companies do better. There is a lot that companies - from ISPs to app developers to platforms and beyond - can do to protect privacy, and those steps will benefit all users. We must push companies to minimize the harm that can be done. In some cases, that means demanding better privacy options by default. In other cases, it means minimizing the use of "dark patterns" that push users to make choices harmful to their privacy. And generally, it means ensuring companies allow pseudonymous access, rethink data retention policies, encrypt what they can, don't share or sell their data, and make their tools interoperable with others, so we can have choices about how we use their products.

This is a tall order - we don't always have much say in what companies do, especially when it hits their bottom line - but you can start by making the switch to more privacy-protective apps where possible, and speaking up when a company whose service you use is negligent with their data protections. And if you're building your own tool or app, of course, you can make privacy a priority.

The Supreme Court decision to overturn abortion rights makes what was benign data now potentially criminal evidence. But it might not stop there. What we know from the past 30 years of work protecting digital rights is that if technology can be used to aid criminalization, it will be - and it might not matter whether the law appears just or not. As always, EFF will be fighting back in the courts, in the legislature, and online - and you can fight back too. It will take all of us, working together, to protect each other.

The Dark Side of DarkMatter: The Evil Hackers behind Project Raven

by Johnny Fusion =11811=

Scrolling through my social media feeds in the third week of September 2021, I came across a story about Project Raven. Three people - Marc Baier, Ryan Adams, and Daniel Gericke - who are either former intelligence operators or military from the United States were levied heavy fines by the Department of Justice and are forbidden to ever seek out a security clearance for life. This was a deal to avoid prosecution for their crimes. What were their crimes? They participated in the most unethical hacking I have ever heard about. Working for a company in the United Arab Emirates known as DarkMatter Group, they were an elite red team working on behalf of the Emirati government to spy on its own citizens, Emerati enemies, and even networks of the United States. But why is this the most unethical hacking in my opinion? Because of their hacking, human rights activists were tortured and imprisoned. Hacking does not exist in a vacuum. It is not just a challenge to test one's limits of their technical acumen. It has real effects on real people, and Project Raven led to real human suffering.

Set the Wayback Machine for the first years of the second decade of the 21st century. Cyber warfare was becoming the new battlefield for the 21st century, and countries all over the world were getting started in an arms race for not only defensive capabilities but offensive as well. Governments were using corporate contractors, often filled with former feds, Edward Snowden perhaps being the most well-known of these types of contractors. Before his whistleblowing, he worked for one such contractor, Booz Allen, that gave him access to all the secrets he was about to spill. Remember that name - it will come up again.

These contractors did not just work for the American government, but provided malware and attack vectors to other governments, equipping countries with cyberweapons sold to anyone who had the coin by those who could obtain a license to export technology and train foreign governments in cyber defense and policy. In September of 2012, one such company, CyberPoint, obtained a license to train the government of the United Arab Emirates in cyber defense - blue team sort of stuff. However, the UAE had other designs.

CyberPoint did not stick to blue team type defense such as firewalls, intrusion detection systems, or other defensive strategies. What is known, thanks to whistleblower Lori Stroud (who actually recruited Edward Snowden into Booz Allen's team contracted to the NSA, giving Snowden access to even more classified material - the perceived disgrace from this turn of events was the reason she left the NSA and went to work for Project Raven) is that this was the "unclassified cover story" for Project Raven to hide their red team style offensive exploits and penetration for the Emirati government. It was perhaps the UAE's desire to have more control and do things in-house that led to the Emirati company DarkMatter taking over the contracting for Project Raven in 2016, and the Cyberpoint contractors who wanted to keep their lucrative jobs in tax-free Dubai moving to DarkMatter. At the time, it was felt that DarkMatter had poached the United States talent working for Cyberpoint.

DarkMatter for all intents and purposes appeared to be an Emirati company, but in fact, they were part of the Emirati government, specifically The National Electronic Security Authority (NESA), the Emirati equivalent of the United States' NSA. These were state actors pretending to be a cybersecurity firm, and they were recruiting. They went to cybersecurity conferences such as RSA in San Francisco and Blackhat in Las Vegas looking for elite hackers to fill their roster by promising six-figure salaries, housing, and a tax-free lifestyle in Dubai. Maybe if you were at Blackhat, you came home with some DarkMatter swag. Many hackers took up DarkMatter on their offer, getting a major payday, but what was the cost?

To put it bluntly, the UAE wanted hackers to build and implement a surveillance state that could be described as "1984 on steroids." Blanketing the country with probes that could hijack cellular signals, do man-in-the-middle attacks, and inject malware, they would be able to intercept all cell phone communication in Abu Dhabi and Dubai, and with the press of a button pwn all the phones in a specific area like a shopping mall on the mere suspicion of a single suspected terrorist or dissident who might be there.

One may argue that every government

participates in some form of a surveillance state, including the United States. The difference is that even though DarkMatter told its hackers that they were fighting the very real threat of terrorism, they also were spying on what the UAE considers dissidents. It should be pointed out here that the UAE does not have freedom of speech. There are no First Amendment protections in the UAE and no exceptions for Americans working in their spy program. The watchers are definitely being watched. Criticism of the government is a punishable offense. Speaking for human rights protections could very well get you disappeared, tortured, secretly tried, and imprisoned. The hacking taking place under the aegis of Project Raven in fact did lead to these outcomes.

The tool that got the most press in early 2019 when Reuters broke the story is called Karma. It used an exploit in iMessage for iPhones that compromised a target phone just by sending a text message that didn't even have to be read or otherwise interacted with. This cyberweapon gave Project Raven hackers access to the device. It sounds a lot like the tool known as Pegasus that has also been in the news lately - and Apple recently pushed patches to fix it. However, in my research, I have not been able to determine if Karma and Pegasus are indeed the same tools, but the similarity of the exploit is uncanny. iMessage is such a desirable vector for exploits, as it is guaranteed to be on every Apple device out there. And because of Apple's closed system, Apple users cannot opt out of this application.

Hackers love freedom, often expressing this in free speech and free software. Many hackers believe in the sovereignty of their own lives and their choices. However, if we are going to exercise this freedom, we must temper it with the responsibility for the consequences of our actions. No matter how isolated or sandboxed you think your hacking is, none of us is an island. Our choices ripple out and affect those who we may not even realize or have the vision to see. People exist within our sphere of influence and beyond the horizon of what we can see. We must not remain ignorant of the impact of our hacking. What does our own freedom mean if we are taking away the freedom of others? Can we really say we are advocates of liberty if we do not work to ensure liberty for all instead of selfishly looking inward and thinking we got ours, and screw everyone else?

Hackers exist in a community of like-minded individuals with a diversity of opinions, skills, and goals. We form collectives to work together to achieve our goals, be it an open-source project, presenting at a conference, or writing for this magazine. We may see hackers as an in-group and those outside our community as "other," but in truth, we are all connected, every single one of us. Human beings create technology in order to be connected and interconnected with other human beings, especially in the realm of communication. From things like smoke signals, drumming across distances, running between cities with messages, postal systems, the telegraph, the telephone, radio, and television, and finally the Internet, humanity has increased our connection with one another to facilitate the sharing of information and understanding of one another.

But there is also a dark side. Human beings have used technology more and more to divide. To foment terrorism, spread misinformation, and facilitate fascism. The hackers of Project Raven were some of those individuals, under the aegis of the Emirati government, to squelch free speech, which is the lowest form of fascism - and facilitate torture of human rights activists, which is well into the realm of authoritarianism. Technology can facilitate freedom and technology can also enable tyranny. Even though some technology is utilized for good or ill, technology is not ethics neutral. There are some applications that are always unethical, immoral, and - I will say it - evil.

Some of the dark side hackers for DarkMatter were ex-feds. While giving lip service to the founding principles of the United States, they were more than willing to set these aside both in their work for the United States and Emirati governments in exchange for a big payday. We know Lori Stroud, the Project Raven whistleblower, was just fine with the NSA spying on everyone as Edward Snowden revealed while participating in it, but only drew the line when the Emirati equivalent, NESA spied on fellow Americans using Project Raven. She was already accustomed to facilitating the compromising of devices of journalists, human rights activists, and foreign governments around the world, and the torture of Emirati dissidents in exchange for six tax-free figures. Stroud knew she was a spy but thought she was a "good" intelligence officer. It was fine to do this to brown folks in the Middle East, to people who were "other," but when it came to Americans, her perceived in-group she suddenly found scruples for what she was doing. Her hacking had a real human cost.

But at least she eventually contacted the FBI about Project Raven, and Reuters did the initial investigative journalism that brought it all to light. Marc Baier, Ryan Adams, and Daniel Gericke cut a deal to pay a fine for breaking U.S. hacking laws and prohibitions for selling military technology to avoid prosecution. This does not undo the damage they have done. They used their technical acumen, access to high technology, and their ability as hackers to cause real harm - real human suffering because of their hacking.

It is a common story. Though I am merely a competent hacker and not a superstar, puttering around more as a hobbyist and technological idealist than an InfoSec worker (the closest being sysadmin jobs in Amsterdam, and California back in the nineties), I have often been approached to do something unethical when people find out I am a hacker, and I am sure many readers of this magazine have as well. What we decide to do matters. It would behoove us not to just hack code, but to have a moral code of what we are willing to do and not do. If we are going to cause harm, who are we causing harm to? Sometimes justice demands direct action, but if we are not careful, some company can wave a fat wad of cash under our noses and we compromise our values and, through our skills, become an agent of injustice. Or maybe we do something "just to see if it can be done."

We have all been there. Hackers are curious creatures. But we must not allow our curiosity to bring actual harm or suffering to other human beings unjustly. We must build an awareness of the influence hacking can have on individuals and organizations. We can use hacking for righteous causes or, like the hackers of Project Raven, for great evil. The choice is yours. Choose wisely.

I Don't Think I Was Supposed to See That

by lg0p89

Data security at times is underrated. Unauthorized persons viewing material is bad enough, however, when you add in the material being from senior management, you have a recipe for issues and people feeling badly. One area for this leakage has been with documents. At least two businesses I consulted with have been Microsoft shops. This gives the curious ample areas to peruse for fun.

One of these apps is Delve. If you happen to have a bit of spare time, for example a Friday after lunch when everyone is in a food coma, take a quick look around. Finding this, if you haven't already had the pleasure, is easy (open the Office app and you'll see Access, Calendar, Delve, Excel, etc.). Just check on that happy Delve icon. Here you'll see Home, Me, Favorites, and People. To get to the juicy bits, click on People. Here you'll see your command/management structure. Now the fun begins.

First, take a look at your documents. You'll see the documents you have emailed and worked on recently. Now, if you are brave enough, you can look at other people by clicking on the other people you work with to see what they have emailed, authored, or modified recently. (Warning: they may become irritated if/when they find out with the system.) That is an awfully large range of documents to let others simply have access to.

The first place I noticed this was at a manufacturing company. I was a little bored and began tooling around, seeing what I could see. In my adventure, I saw the CISO's name and thought it might be interesting to check out what was new. Yes, indeed there were a number of documents I probably should not have seen. These included budgets and other documents well above my pay grade.

Naturally being curious, this clicking activity was done at the next place. If it worked once, twice certainly should be the charm. Well, it worked again. This time, I was a bit more adventurous. I was able to see the documents for the CEO and COO, as well as human resources and other management members. Just by clicking a few items and not doing anything exciting or using mental gymnastics, I was seeing purchase orders, resumes for applicants and staff, research papers, bids, policies, incident responses, and many other items that should have been confidential, yet anyone could look at them. Fortunately for me, I was also able to see co-workers' documents.

The Delve disclaimer on the screen says that you, the user, can only see files/documents you have access to. This sounds very official and makes it seem as if there have been rules put into place to limit access based on the user's role, position, or work group. Not really. You tend to have access to most documents as the target doesn't know about limiting who has access to these or toggling this function to confidential. This may be the case in IT, but not with operations. It is likely their staff outside of IT are relatively clueless regarding the issue. To mitigate this involves more than clicking one button.

In my case, this was reported to IT as a potential problem. As a responsible researcher, this was appropriate. Was this fixed or at least mitigated in some fashion? No.

About Conversation, Thought, and Language

by Diana K

Some may wonder what conservation, thought, and language have to do with hacking in terms of expanding your knowledge of things and knowledge of your own perceptions. Let me answer this with a true account.

My alma mater was UW Parkside. I graduated in pre-med and computer science with a breadth of knowledge in art and history (actually, an academic minor at other universities) at a difficult time in the U.S. UW Parkside was established in 1968 at the most intense time of the Vietnam War as university protests were high at UW Madison and other universities.

However, UW Parkside was established with a different conversation. Many of the early professors were from UW Madison and did not wish to export the loss of conversation that had occurred at Madison. So, an idea was set up that although a topic may be loaded or charged, UW Parkside was supposed to be a thoughtful and academic space built to coincide with nature (actually, the campus still coincides with nature as it is part of a forest coexisting with the urban space outside of the university).

The first practice of this principle occurred in computer science and business programming classes. At that time in 1968, the university batched programs written in FORTRAN and COBOL to Madison to run and send results back. The first practice was that students, guests, and faculty were not allowed to mock the computer language that one used to solve a problem on a computer, sort of like a Constitutional amendment of language and thought freedom.

A second part of the practice stated that UW Parkside's library would obtain books from many sources and authors - and that professorial pull was not allowed to decide what books, magazines, and newspapers the library could obtain. The library was given complete independence from the administration and academic departments starting in 1968 and still continuing today. The advantage of this was that the library was able to obtain newspapers and magazines like *Le Monde*, *Der Spiegel*, *Paris Match*, European newspapers, as well as science journals like *Bioscience*, *Nature*, and *Biology* from the U.K. Outlier publications were also able to be obtained. The ability to gain access to various thoughts reflected the policy of UW Parkside, which was to trust the reader that they could make up their own mind and evaluate without blinders or without muffling (a concern I have had since the end of 2020 with regard to the shutting down of social media sites on the Internet and the muffling of voices not in chorus with the majority party).

As a result, my language comprehension included French, German, Spanish, Italian, and Russian. The comprehension included the ability to read, write, and speak - although my speaking fluency is reduced due to health issues. The important thing is that I saw that it was not about one language being better than another, but rather that language provides a perspective to evaluate or express an idea from a different perspective.

As my language comprehension increased, I began to see that FORTRAN, COBOL, and PL/1 (the language I programmed in as a programmer) were different ways to perceive or express an idea. So, I went from FORTRAN to BASIC to machine code (TI 58/59, SR-56, Z80, and PDP-11/20 assembly) to PASCAL and others.

One summer, as I was transitioning from ninth grade in junior high school to tenth grade in senior high school, I decided I wanted to learn PASCAL. My dad told me that Parkside had a liberal policy of allowing non-students to have a practice computer account. I went to the university computer center and asked for a non-student programming account to learn PASCAL. I filled out a form on green bar paper, about half a page, with information like name, address, phone number, and parent's name (for applicants under 18). I was then asked to read a simple typed double-spaced page with rules of use. After signing that, I was given a username, password, and assigned 128 blocks of storage.

"Blocks of storage" is an old term that is no longer used. It is similar to how much disk space you have to run or store programs on your hard drive. A block at that time was 512 bytes. So 128 blocks translated to 64 kilobytes of information. This amount may seem low, but you have to remember that in the mid 1970s, many hard drives used on minicomputers for business were only ten megabytes, which is one millionth of a ten-terabyte disk drive in common

use today. Yet, that amount was sufficient to run many applications and programs back then.

The most important part of the open policy of non-student accounts then was that, compared to the security and rigor of today, it was a different time. People trusted each other and opening an account for the local community was not something to worry about - we all knew each other. With the environment that existed at UW Parkside, we did not have to worry about misuse of the account. There were safeguards installed to prevent misuse.

Some in other parts of the world - or even other parts of the U.S. - will say "you guys were very naïve and immature to put that much trust into non-students." Not really. One has to remember Wisconsin as it existed in the time of the mid to late 70s. Where UW Parkside was located, the area was a refuge for those escaping the race politics of the state of Milwaukee and those escaping the one-party political state of Chicago.

My family moved back to Kenosha from Wauwatosa in 1974. The race politics of Milwaukee had encroached upon Wauwatosa, and so we returned to my dad's home town. Then, it was an auto town that valued education and arts, and was also away from everyone in various political groups yelling at each other as they were doing in Milwaukee and Chicago at the time. Peaceful, quiet, and you could leave your violin in a music locker unlocked without fear of it being stolen.

Although the setting was safer than Milwaukee and Chicago at that time, we did have our discussions. Like many kids who were raised in the late 60s through early 70s, we would play war and have Mattel M-16 toy guns to simulate with.

When we moved to Kenosha, there were many veterans who had come back from Vietnam. One of them discussed an important issue that many of us in the neighborhood were not aware of. The toy M-16 guns we were playing with were the same size and made exactly the same sound as a real M-16. The veterans who talked with us didn't mention PTSD, but they did mention that the sound and sight of them caused flashbacks. So, as a neighborhood, we stopped playing war and instead focused on baseball.

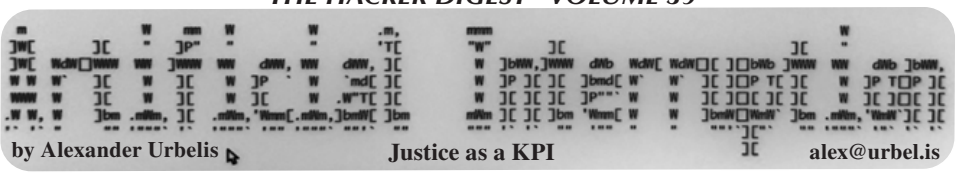
During the 1970s in Kenosha, we were having the same discussions about national politics and what to do about those who were coming back from Vietnam. A thing to remember about Kenosha is that there were many military families. My grandfather's name is inscribed on the wall of the library of World War One veterans from Kenosha. Also, Kenosha was an auto town that greatly supported education and there were many who had questions and concerns. However, in that time of Vietnam, Watergate, and the Nixon resignation, we argued but never came to blows.

Also, everyone was encouraged to speak their own languages. Secondary languages included Polish, Italian, and German. No one was shut down unless someone was deliberately trying to start a riot. So, to me, when I learned various programming languages (up to 100 now from the early beginnings of the 70s) with FORTRAN, BASIC, machine code/assembly, and PASCAL, I think that even in a turbulent time like the 1970s, I did not feel like I do today. I felt freer to express my thoughts openly than I do today.

Part of the reason why I have concerns about expressing my thoughts today is that area of Kenosha/Racine which used to be a haven from the race politics of the state of Milwaukee and the one-party system state of Chicago is now absorbed into both.

What does this mean? I am a contrarian and I believe in reading and listening to multiple points of view. When we would visit my cousins in Madison, I would read different papers, such as the *Capital Times* (the liberal paper) and the *Wisconsin State Journal* (the conservative paper). At home, I'd read the *Chicago Tribune* (the conservative paper and I have been told I was reading "the Colonel's paper") and *Milwaukee Journal* (the liberal paper). Yet, today, when I try to share views and concerns about what I see happening worldwide, nationally, and locally, there is only a small circle of friends I can talk to. When I do try to reach out locally, as soon as I deviate from the majority party talking points, the listening stops and I am shut down in trying to share something important.

Today, I went to have tacos with a friend and I wore my *2600* t-shirt with the blue box schematic in front. Part of the reason I wore it is that I wanted to express being proud of the hacker culture that seeks to expand knowledge and insight. Also, I wanted to see what others would think at the bar I go to. I'm glad that I was surprised. Many were happy to see me wear it. Over a pitcher of beer, I discussed the components on the front of the shirt. Also, others who were retired looked and smiled at the fact that the spirit still exists.



by Alexander Urbelis

Justice as a KPI

alex@urbel.is

Sitting in my office in midtown Manhattan at the end of May, the sun was shining and, while in the midst of writing something on a short deadline and deep in thought, I was distracted, as always, by an Exchange notification of a new email. Though these new email notifications can often be disproportionate in their ability to be disruptive relative their temporality, this one was particularly so. In the two lines of text that popped into the lower right hand corner of the monitor, I saw something unusual: a notification that the Department of Justice had revised its prosecutorial guidelines for bringing charges under the Computer Fraud and Abuse Act (CFAA).

The notification was effective. My interest was piqued. I clicked the banner, opened the email, and was amazed to find the entirety of the email just as fascinating. I learned these new prosecutorial guidelines mandated that "good faith security research" would no longer be treated as a crime under the CFAA. This seemed like a victory for white hats, security researchers, pen testers, bounty hunters, etc., depending on how these new guidelines defined the contours of good faith security research. Too narrow and the change would have no effect; too broad and the statute itself would lose its meaning and force.

The CFAA is a famous and infamous statute: on the books since 1986, proposed by Congress in 1984, and drafted in direct response to the cult classic hacker flick *WarGames*. The new guidelines for prosecution under the CFAA coincidentally take their definition of "good faith security research" from another infamous statute in the hacker community, the Digital Millennium Copyright Act (DMCA), under which the Motion Picture of Association of America sued *2600 Magazine* just about 23 years ago. Because the DMCA deals in some respects with reverse engineering and security testing, it had a fairly broad definition of "good faith security research," i.e., "accessing a computer solely for purposes of good faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services."

On the surface, this looks like rather expansive classes of activities that should not fall afoul of the CFAA. That said, there are many ways this definition can be interpreted and, for this reason, security researchers and prosecutors are likely to disagree on boundaries. As such, the CFAA will continue to exist as a nuanced law subject to multiple interpretations. These boundaries, by the time of publication of this article, will no doubt have already been addressed in a robust, respectful, and meaningful way at the HOPE panel I will have moderated.

But even now, on a gut level, the mere idea that good faith security research, that ethical hacking, is not outside the law but within it, should finally feel like the hacker community is seeing the policy changes it clamored for over the last three decades - that finally things are looking more just. Even though the law is not changed, the new guidelines are a public statement of what the DOJ believes is right and wrong, and of what is just and unjust to pursue as a prosecution.

Because of this shift towards justness, I began to ruminate, to re-think justice, the very elusive nature of that concept itself, with a particular focus on how to measure justice. Since this policy change would result in DOJ prosecuting fewer actions as crimes, would a lower number of CFAA prosecutions signal a greater amount of justice? How would the efficacy of this policy change be measured? What, if anything, can we make of differences in interpretation of these new guidelines between U.S. Attorneys' Offices? If there are fewer cases in New York brought under the CFAA but an increasing amount in, say, Kentucky, then what does that say about the result of the new guidelines? In short, can we measure justice like it's some kind of key performance indicator (KPI)?

It's certainly not how Aristotle thought of it. As an undergraduate, I was very fortunate to have the opportunity to attend Oxford University as a visiting student. While there, I studied Aristotle's *Nicomachean Ethics* with a truly great man, the Rev. Dr. Cyril Barrett. Cyril was an Irish Jesuit priest in the most irreverent, progressive, and controversial ways possible. I recall many fervent discussions during tutorials with Cyril about whether

Aristotle had it right or totally wrong, and a good deal of those discussions centered around the concept of justice.

Justice was a virtue to Aristotle; it was a standard of conduct to which humans should strive. Virtue, as Aristotle famously defined it, existed in the middle ground (i.e., the mean) between excess and defect. This concept makes sense for characteristics like temperance or moderation, because an excess of temperance would make one fussy and overly prudent, while on the other hand, a defect of moderation could lead to extreme or disproportionate behavior, like binge drinking. In the context of drinking, Aristotle would have neither approved of persons who were straight-edge nor persons who regularly drank too much - moderation was the key to virtue. Going too far in either direction from the mean, according to Aristotle, would lead to vice.

For Aristotle, justice was also a virtue - a rational mean between two extremes. While we can certainly envision there being a defect of justice or, in other words, too little justice, it does not necessarily make sense that there could be too much justice. Moving in the direction of ensuring a just result, viz. achieving justice, seems exactly like what a governmental agency that calls itself the Department of Justice should be doing.

On the defect of justice side in the specific context of the CFAA, we have an example from our community that will always make our hearts heavy: Aaron Swartz. Over a decade ago, based on what appears to be a now-rejected view of what the CFAA covers, the DOJ charged Aaron with eleven CFAA violations for systematically downloading academic journals from JSTOR. The U.S. Attorney's Office in Massachusetts intended to use Aaron's case to send a message. The State of Massachusetts, on the other hand, declined to bring any charges against Aaron for the same conduct. Nearly two years later, after DOJ rejected a plea arrangement, Aaron hanged himself in his Brooklyn apartment.

If ever there was a defect of justice, this case was it. To the contrary, did the decision of the State of Massachusetts to not view this conduct as criminal create an excess of justice? I say no: Aaron surely suffered and learned his lesson by the mere fact that both the State of Massachusetts and the U.S. Department of Justice were investigating his conduct. Viewed in the light of the new guidelines, even contemplating pursuing charges against Aaron's conduct could be seen as a defect of justice.

That raises the issue of whether the guidelines changes are too little too late. Overzealous pursuit of CFAA charges took a precious life from our community. The government moves slowly, arguably too slowly, but at least this is movement, and movement in the right direction.

I submit that, in Aristotelian terms, there may now be a way to measure the impact of the CFAA policy changes on whether the Department of Justice is pursuing just cases. The first metric would be to take the total number of cases where CFAA charges are contemplated, which we can call N. Subtract from N the total number of cases across the United States for which U.S. Attorneys' Offices have declined prosecution on account of new guidelines' carve-out for good faith security research. We can call that total D. Thus, the equation of (N-D) = the total number of cases actually pursued under the CFAA, which we can call C. Let P = the total number of CFAA cases pursued across the United States in previous years.

P should be greater than C. If C is greater than P, then it is likely that the new guidelines are not being implemented or there is a problem of inconsistent interpretation. C, therefore, could be further analyzed by jurisdiction. Unless there are a greater number of CFAA cases countrywide that fall outside of the new guidelines, C should decrease. The percentage of C's decrease can thus act as an Aristotelian marker as the spot that indicates the mean, or the middle ground, for justice.

Measurements such as these, though not actuarial in nature and certainly subject to some variance based on the facts and circumstances of individual cases, should also allow easier recognition of cases that would fall outside the mean of justice - cases like Aaron Swartz's. Those cases tend to be the ones that the government pursues to send a message, and which would deter future conduct. Those cases, therefore, are more likely to be inherently defective of justice, or more colloquially, those cases are simply less just. It is for this reason that I submit that U.S. Attorneys should be measured, not by their convictions, but by the use of sound discretion in declining to pursue certain cases.

Those declinations indicate an understanding of the need and place for good faith security research, a recognition of the policy errors of the past, and a commitment to prevent injustice going forward. This is an area where less can certainly be more as we, as a community and a country, continue to struggle with and strive for justice.

Brute-Forcing a Museum's Math Puzzle With Python

by Brenden Hyde

TL;DR: A seemingly simple math puzzle stumped me, so I brute-forced it with a Python program.

Background

During a visit to a museum called OMSI,[1] I noticed a puzzle that had a 3x3 grid and some wooden blocks labeled 1 through 9.

The grid looked like this:

```
[] - [] = []
           x
[] ÷ [] = []
           =
[] + [] = []
```

The puzzle was called "Four Equations," and the goal of it was to arrange the blocks to meet these constraints:

The top row was a difference (A - B = C).

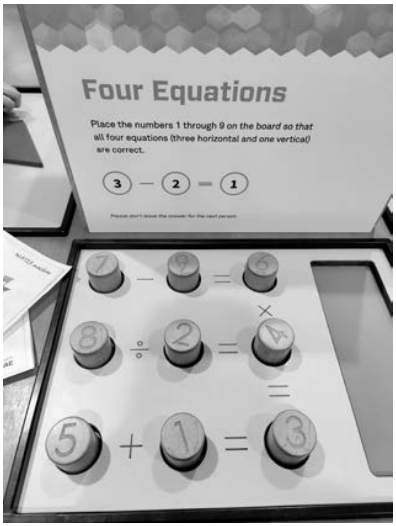
The middle row was a quotient (D ÷ E = F).

The bottom row was a sum (G + H = I).

The right column was a product (C × F = I).

All four equations had to be solved at the same time, and you could use each number only once.

Here's a picture of the puzzle with its blocks jumbled:



Motivation

As you might infer from the picture of the wooden blocks and simple, gigantic print on the sign, this was a puzzle for all ages including children, and yet I couldn't solve it in the five to ten minutes I tried.

Slightly annoyed, I gave up, sanitized my hands, and vowed I'd solve it later with a computer.

Number of Possible Solutions

The way to calculate the total number of possible block arrangements in this puzzle is with factorials.

There are nine starting blocks to choose from.

After you choose one, there are eight remaining blocks.

After you choose another, there are seven remaining, and so on until you run out.

That means that the number of possible arrangements is 9! or "nine factorial."

This can be written as:

```
9 x 8 x 7 x 6 x 5 x 4 x 3 x 2 x 1
```

The number 9! is equal to 362,880.

That's the number of naive guesses it would take to guarantee that you either get the answer or prove there isn't one. I say "naive" because not every permutation in our huge list is a potential solution.

The possibilities shrink when you consider the mathematical relationships among the numbers. For example, the second row is a division problem.

Because 2, 3, 5, and 7 are prime numbers, none of them can be the first number (dividend).

The ninth box is the product of two numbers, so none of the primes can go there either, as we don't have any duplicates, and a prime number only has two factors: one and the prime itself.

You could solve the Four Equations problem like a Sudoku, given that it has so many logical constraints to eliminate most solutions.

But, I have a computer, and I don't have the patience for that!

Solving It With Python

I chose the Python programming language to build my puzzle solver, since it's powerful and easy to use. If you don't care about the code, you can safely skip to the section entitled "Solving the Puzzle."

There are two main pieces to my Python program:

1. Get a list of all possible permutations of the numbers 1 through 9.
2. See if any of them solves the puzzle, and print it if so.

Getting All Possible Permutations

I want to find every way that the numbers 1 through 9 can be scrambled.

Rather than reinvent the wheel, I used the permutations function from Python's itertools module. This function returns all possible permutations of a list of numbers.

Here's some example code that achieves this:

```
from itertools import
```

```
➥permutations
one _ thru _ nine = list(range(1,
➥10))
all _ perms =
➥list(permutations(one _ thru _
➥nine))
```

In the above code, I first generate a list of all numbers 1 through 9 with Python's range function.

range takes two arguments here: the lower bound (starting number) and upper bound (ending number).

Confusingly, range is inclusive on the lower bound and exclusive on the upper bound. That means that if I run range(1, 5), it'll give me the numbers 1, 2, 3, and 4, but not 5. Therefore, I use range(1, 10) in the example to get 1 through 9.

After I get the list of numbers, I use permutations plus a built-in function called list to create the possible solutions.

Constraint Checking

Equipped with a list of possible solutions (and many erroneous ones), it's time to solve the puzzle.

To check if a permutation solves the puzzle, the code uses Python assertions. An assertion is just a statement that is either true or false. If the statement is true, Python does nothing and moves on to the next line of code. However, if the statement is false, Python raises an error to tell us this isn't a solution. This error is called an AssertionError.

Here's a snippet that uses an assertion to check if the difference between the first two elements equals the third element:

```
def check _ solution(p):
    try:
        assert p[0] - p[1] == p[2]
    except AssertionError:
        return False
    else:
        return True
```

In the above code, we make a function called check_solution that takes a list called p as an argument.

To grab an item out of a Python list, you refer to it by its index. An index is the numerical label that represents the item's place in the list. The first element has an index of 0, so if my list were [1,2,3], the number 1 would be at index 0, the number 2 would be at index 1, and 3 would be at index 2.

Our list is called p, so the first element in the list is called p[0], and the second one is p[1], etc.

In the code, we assert that p[0] - p[1] == p[2].

If this is true, as in the example case assert 6 - 4 == 2 then the function returns a value of True.

If that assertion is false, for example assert 4 - 2 == 7 then an AssertionError is raised by our function, and we handle it by returning False.

The above example only solves one of the four constraints, but we can test addition, division, and multiplication just like we did for subtraction.

Those assertions are included in the code, but I've omitted them here to stop the reader from falling asleep.

Solving the Puzzle

With all the math riff-raff out of the way, we can solve this puzzle.

Assuming you have Python 3.6 or greater installed, you can run my accompanying script from the CLI like so:

```
python3 grid _ puzzle.py
```

The answer will be rendered to the screen:

```
Solution found!
---------
9 - 5 = 4
        x
6 ÷ 3 = 2
        =
1 + 7 = 8
---------
Solution found!
---------
9 - 5 = 4
        x
6 ÷ 3 = 2
        =
7 + 1 = 8
---------
The total number of solutions is
2
```

Conclusion

To my surprise, there were two solutions to the problem.

My program started guessing with the number 1 in the first box, and the real solutions both started with a 9 in the first box, so it took a lot of attempts to get it right.

Specifically, it took 345,295 guesses to get the first solution and two more for the second!

It took about 45 minutes of coding and 50-70 lines of code to solve this problem. The actual execution of the program takes less than a second!

While I could have made paper cutouts and solved this by hand, I enjoyed doing it more with code, as it let me be sure there were only two answers.

The source code for grid_puzzle.py is in the penultimate section of this article after the conclusion and before the footnotes.

The code is licensed under the GNU General Public License, Version 3.[1]

If this article makes it to publication in *2600*, I will also make the Python source code to solve the "Four Equations" puzzle at the link in the footnotes.[2]

With my code now complete, I am finally armed with the computational power to brute-force a children's puzzle. The next time someone asks me if I'm smarter than a fifth grader, I can respond more confidently than ever with a resounding, "probably!"

Source Code

```
from itertools import permutations

def render(l):
    """Render a 3x3 grid of a list `l`."""
    try:
        assert len(l) == 9
    except AssertionError:
        print(f"Expected list of length 9. Got length {len(l)}")

    first_row = f"{l[0]} - {l[1]} = {l[2]}"
    second_row = f"{l[3]} ÷ {l[4]} = {l[5]}"
    third_row = f"{l[6]} + {l[7]} = {l[8]}"
    leading_1 = " " * 8 + "x"
    leading_2 = " " * 8 + "="
    padding = '-' * len(first_row)

    rows = [padding, first_row, leading_1, second_row,
➥leading_2, third_row, padding]
    for row in rows:
        print(row)

def generate_lists():
    """Generate all permutations of range(1, 10)."""
    all_perms = list(permutations(range(1, 10)))

    return all_perms

def check_solution(p):
    """Given a permutation of range(1, 10), return True if p
➥solves the puzzle."""
    try:
        assert p[0] - p[1] == p[2]
    except AssertionError:
        return False

    try:
        assert p[3] / p[4] == p[5]
    except AssertionError:
        return False

    try:
        assert p[6] + p[7] == p[8]
    except AssertionError:
        return False

    try:
        assert p[2] * p[5] == p[8]
    except AssertionError:
        return False
```

```
    return True

def main():
    all_permutations = generate_lists()
    all_solutions = []
    for index, p in enumerate(all_permutations):
        solved = check_solution(p)
        # print(f'Trying permutation #{index + 1}...')
        if solved:
            print('Solution found! ')
            render(p)
            # print(f'Took {index + 1} guesses to solve.')
            all_solutions.append(p)

    print(f'The total number of solutions is {len(all_
➥solutions)}')

if __name__ == '__main__':
    main()
```

Footnotes

[1] www.gnu.org/licenses/gpl-3.0.en.html
[2] github.com/bxbrenden/four-equations-puzzle

Hacking and Politics: Why Talking About Both Matters

by Screaming Yellow Fish **sharky.yellowfish@gmail.com**

I've noticed a trend of late in what seems to be a louder chorus of voices who run the gamut from annoyed to royally pissed off at what is perceived to be the political tone of the magazine. It seems to me that this has always been the focus as part of the "voice" of *2600*, and as it has become louder, as well as the current political climate writ large, it has moved me to investigate and see for myself if I myself am biased and there is meat on this bone, or if the current climate is driving a deeper divide between us.

My original intent was to look at the editorial of the first magazine printed for each year. Since I have just completed a cross country move and could not locate my 8.5 x 11 copies of *2600* from 1984 to 1986, I chose to start from 1987 Volume 4, Number 1 and continue on through 2021, Volume 38, Number 1. Not unlike perusing YouTube or anything on the web, I became distracted by an article by none other than Cheshire Catalyst in the January 1987 issue ("TAP: The Legend is Dead.") Funny how I landed on that, as that article touches on many of the very points I have been pondering.

For those who don't have access to that article, allow me to synopsize. *YIPL* (Youth International Party Line) was created by a group of anarchists (Cheshire's term by the way, no letters please for "why did you use that term" blah blah). The "Party Line" part of the name was a reference to the term used when the phone company would connect parties in a networked call. You can Google "party line" and "selective ringing," or just purchase the back issues for the article - it's well worth it.

I should point out that I find it fascinating that my 27-year-old son who possesses half a dozen cell phones; has dozens of aliases online; and communicates via Facebook, Twitter, and TikTok would never imagine that before 1969 it was illegal to attach your own devices to a phone line, that calls were metered, that there was a concept of

"long distance" vs. local, that calls were sometimes operator assisted, etc. He looks at a cell phone and asks "wait... you actually use that to make... phone calls?"

Back then, that was the impetus for exploring the phone network, as well as the seeds of the disdain for both the phone company and corporate America. This is not a new concept by any stretch.

In 1971, Abbie Hoffman and Al Bell got the idea to create the *YIPL* newsletter to share information with the members of this technical underground in the same way that the Bell System published information to its own members. It contained pretty random content, and contained anarcho-techno stuff (again, Cheshire's description) including lock picking, making pipe bombs, and other radical stuff.

Here's the kicker. In 1974, Al Bell said to himself (and I am quoting from the article) "What's all this political shit doing in what should have been a technical newsletter?" He left the Yippies, changed the name of the newsletter to *TAP*, and set up shop.

At this point, I read the rest of the article (the last time I read this was in 1987), and it started the wheels turning. My original intent when I started out was to demonstrate that *2600* has always been, and largely still is, a mix of both technical and political content. Imagine my surprise to find an article from 35 years ago from someone who I respect and admire greatly that actually offered up evidence that nope, this is not a new concept.

This got me thinking... what would I have said back then? What would be my advice now? I think it's often human nature when facing a problem to try and minimize options and to pare down the problem into nice neat packages. Thing is people are messy. We are not made of nice neat stuff. We talk at each other instead of to each other. We assume there is only option A or B instead of looking beyond to options C, D, etc.

Here's the thing. I am a tech head, nothing makes me happier than delving into the gritty details of cross site scripting, ARP table poisoning or NVM external memory access cycle times. Thing is, there is no such thing as a free ride.

Do you think the price of the magazine you are holding in your hand is the cost of a subscription, or picking up a copy of the magazine at your local Barnes and Noble? Try this scenario on for size. Texas lawmakers successfully managed to ban abortion in the state of Texas by end running the Constitution. Here's how they did it: The new law allows any private citizen to sue Texas abortion providers who violate the law, as well as anyone who "aids or abets" a woman getting the procedure.

Now let's suppose they decide to go after anyone who prints or publishes any "objectionable" content such as, say, *The Hacker Quarterly*. First Amendment: "Congress shall make no law... abridging the freedom of speech, or of the press." Texas lawmakers can't outright ban *2600*. They can enact a law that allows any private citizen to sue Texas bookstores, service providers, or anyone who violates the law, as well as anyone who "aids or abets" a "person" obtaining "*The Hacker Quarterly*."

Still think that politics doesn't apply to *everyone* who reads this magazine or surfs the site?

Ever since *2600* started publishing, I've read all kinds of attempts to define hackers or hacking or the hacker's ethic. Most more or less seem to hit it on the mark, some more than others. There have been some impressive articles published, including the continuing "Hacker Perspective" column. I would like to offer this:

Above all else, the hacker spirit, or ethos is more than just the exploration and sharing of knowledge... it is about being the voice for those who otherwise don't, can't, or wouldn't have a voice.

We all need to stay engaged, lest we lose the place to talk about and share in the things we love to do.

An Atavistic Freak Out, Episode Five

by Leon Manna

This story is a work of fiction.

Por eso soy andariego
Pa' olvidarme de pesares
Soy barco de cualquier puerto
No me le arrodillo a nadie
Me juego en cualquier gallera
Aquí o en otros lugares

- El Charrito Negro

I'm a coward and a fool! It seemed so simple in the moment, like such a sincere thought. Inner doubt, self loathing. It'll be my turn soon, here or in other places! God! We swam back to shore and started heading towards my apartment. Lenny coughed up seawater and looked at me. "Let me get a ride," he said.

"So you're living here now?"

He nodded. "Yeah dude. I got shot with a .22 like, four times in Miami. Four separate times! Can you believe that? Besides, you pay me to be your lawyer. You're the only person within a hundred mile radius who I can somewhat tolerate, and even then... You piss me off." He seemed to be in a good mood, I guess, despite the backhanded compliment.

"Just take my moped." He hopped on it and rode off. I watched him crank the brakes too hard and crash onto the sand. Then he got up like nothing happened, turned around, gave me the stink-eye, and rode off. About 15 feet later he did that whole thing again, and then disappeared on a bend in the road.

Lenny Cruz (right) and Leon (left)

I heard the dial tone. Then Ary picked up. "What do you want?"

"Uhh... Your stuff isn't at the apartment. I haven't seen you in a couple days. Are you okay?"

"No, I'm not okay. My *ex* boyfriend is a sociopath and I followed him across the country for no reason. I'm going home. I already bought a ticket."

"Wait, wait, wait I -"

"I don't want to hear it. I hate you."

I couldn't even say anything. Can I even be mad? No. Then she hung up, and that's where the Ary plotline ended, as well as any future I had with her. Once again, I felt guilty. It's my fault.

Across the U.S., a federal agent named Segev Bezalel, who we will refer to as Moe, gets a call about a strange guy. A strange guy who smokes crack in Best Buy. The strange guy has been doing unspeakable, despicable acts of cybercrime. Thousands upon thousands of dollars, missing, totally gone with no idea where it went. It's me. I'm the strange guy.

So the detective thinks to himself, "Piece of cake."

But the detective gets frustrated quickly because Leon Manna, who lived in Arizona, died pretty recently. What confuses him is that there's another Leon Manna in Utah. When he checks on that, it shows that he *also* died, but in 2013. Then he checks again, and sees a Leon Manna in California. And then he sees one in Nevada, and South Carolina, and then New York, until he's filled in all but 15 of the states in the U.S. Some are dead, some are alive. Each one has a vaguely similar description. I am everywhere and nowhere at the same time. I am more powerful than god.

This boggles his mind. How did he impersonate someone who's been dead since the last decade? How could it have happened? Moe has no clue what to do. He calls his boss, but it's three in the morning, so he doesn't pick up. He calls about ten other buffoons, none of which pick up either. He finally reaches his boss's boss, who "has no clue who the fuck he is and why the hell would he fucking call me at 3 AM, I mean who has the nerve. Your boss will be hearing about this."

But something didn't sit right with him. He listens to the tone on his phone while he waits for Leon to pick up. He's about to terminate the call when he hears a voice on the other end.

"Hello?"

Moe paused. "Is this Leon Manna?"

There was silence. Then, "Long time, no see. I miss you Moe."

"Segev, dumbass. Let's talk, please. You don't need to run."

"No, Moe. I do need to run."

"You don't. We gathered everything, Leon. I even see an armed robbery here. We're going to catch you eventually."

"No the fuck you will not. Also, that robbery wasn't me. It was a man named Nash Nashville. You'll find him in Memphis. I wouldn't bother looking in Nashville, though. If he's not there, I'd check your mother's house."

"Well, that's just disrespectful." But the call was terminated and there was nobody listening to hear him say that. When he called back, the number was disconnected. In the morning, he calls his boss. His boss decides to send him on a maniacal wild goose chase, investigating every single Leon Manna in the U.S.

So what now? Well, I have 15 states that need Leon Manna in them. A federal semi-turncoat is always won over with blackmail. They do nasty stuff, they really do, you just have to catch them. This is how we operated for a while. And then, we met this guy somewhere in a stack of papers. We knew he was from New Mexico, but we didn't know his name. I'll let you fill the rest in.

Moe sees this. Just like my shapeshifter act at Sawtooth, this actually did the opposite of what I thought it would. I was just trying to cause as much confusion and chaos as possible, there was basically no strategy past that. Moe isn't an idiot, and he realizes very quickly that I'm making all these fake identities in different states to confuse him. Why? Because if he would do it, I would. That's sorta how he caught us. They assigned my case to him after they did a profile on me. There was a reason it was him, but I simply can't tell you why just yet. There's more to say before. He calls his boss and after like, seven layers of bureaucracy or something, someone finally orders the Social Security Administration to check in on all of these Leon Manna clones. The SSA says they can't do that within the timeframe they needed because there were multiple real Leon Manna identities in some of those states. So after swearing profusely at the person from the SSA, the moron demands that they investigate every case of Leon Manna in any state ever, regardless of how long it takes. This was a huge waste of time because they can't seem to figure out which ones were real and which weren't. They couldn't go and check every single Leon in real life, they simply didn't have the resources, and I wasn't important enough for that.

So the Federal Pig calls the SSA back and says that they need to check to see which Leon Manna identities match up with each other in other states, for unknown reasons. I'm not sure what their tactic was there. But every single picture was a different person. I'm really good at photoshop.

...

What to do, what to do... I didn't know yet. I was thinking about it, waiting for 1.5 grams of phenibut hydrochloride to kick in when I heard a knock on my door. Déjà vu.

Again, Lenny, except normal this time. "I'm going to Cuba. We both have warrants."

"I know," I said. "I called the county office claiming to be an employer looking to hire us. I said I just needed to know if there was anything that should disqualify us. The list was pretty long, this isn't good."

"Well, let's go then."

I thought about it for a second. "What about a contingency plan?"

And so here's what happened: I sat back and did nothing. But one night, at 3 AM again, there was nobody in the office except for the security guard. The first thing that happened was somebody made it into the server that stored digital evidence of people Moe was investigating via the EternalBlue exploit. The intruder dropped a small executable file into a temporary folder, executed it, and then disconnected. This executable, which had been encrypted and then packed into another executable, remained unflagged by antivirus and looped through the entire filesystem until it had collected the paths of every SQL database file on the system. Then, the executable proceeded to overwrite that database with null bytes. Then it did that to the entire HDD. Then it destroyed the backups. Then wiped the MBR of the server.

The Master Boot Record (MBR) is the first 512 bytes in the first sector of your HDD that tells the computer where the OS is and then how to load it. If you overwrite the MBR with null bytes, the computer will not boot. If you overwrite it with your own code, the computer will run whatever you placed every single time it starts.

Long story short, the server says "fuck you" on boot, every single time. So did every computer in his office. Then, somehow, the intruder got control of the thermostat in the evidence room and then turned it up to a dangerously high temperature, making most or all of the physical evidence useless. At least the shit they had on me. Eventually the evidence room caught on fire due to the amount of paper documents inside. Needless to say, panic ensued.

But this wasn't me. The IP address they associated with the intrusion originated overseas. The executable had basically nothing in it of value, even though they spent a lot of time reverse engineering it. The IP they had came from a country where they had no jurisdiction, far far away. Somewhere in Europe I think... But I wouldn't know, I just sat on my couch and watched a movie.

What evidence? What are you talking about?

Oh God when will it stop on: An Atavistic Freakout*?*

Foreign Payphones

Ukraine. Seen in Dnipro less than a month before the invasion, we can only hope this phone and the adjoining postal box still exist. The building was damaged by a Russian missile on 12 March.

Photo by Svyatoslav Pidgorny

Foreign Payphones

Honduras. From Copán Ruinas, this one has definitely seen better days. The phone itself looks well maintained apart from the obvious issue.

Photo by Nicolas Stavros Niarchos

Foreign Payphones

Malaysia. Discovered on Langkawi Island, this phone exudes a defiant tone. A real fixer-upper.

Photo by Zak Cunningham

Foreign Payphones

Turkey. Found next to an elementary school in the Fatih district of Istanbul, this model looks both heavily used and well maintained.

Photo by Ammar Husami

Payphone Booths

United States. Seen outside of the local independent Pymatuning Telephone Company in Transfer, Pennsylvania, this booth wins awards for its association with the cool sounding names - and for simply existing and providing shelter. The phone itself is a functioning second generation GTE 120B.

Photo by Maya King

Payphone Booths

England. While this Oxford booth looks just like the real thing - and no doubt was at some point - it's actually an ATM, at least on one side. Someone had the bright idea of attaching an actual payphone to the outside, which is one of the strangest things we've ever seen. And yes, it works.

Photo by Jeff Alyanak

Payphone Booths

Cuba. These booths are just plain weird. Found in Havana in a place that advertises the country people are already in, these look like museum exhibits somehow. They are certainly the clearest booths we've seen in a while.

Photo by c

Payphone Booths

United States. This Seattle phone booth, seen in the Maple Leaf neighborhood, is torn between being a phone booth and a library. The phone doesn't work and the shelves are empty. Stay tuned.

Photo by Jesse Arnold

Working Payphones

Romania. This cheerful looking phone was found inside a university hospital in Bucharest. We're told it's in pretty good condition and that there are not very many left.

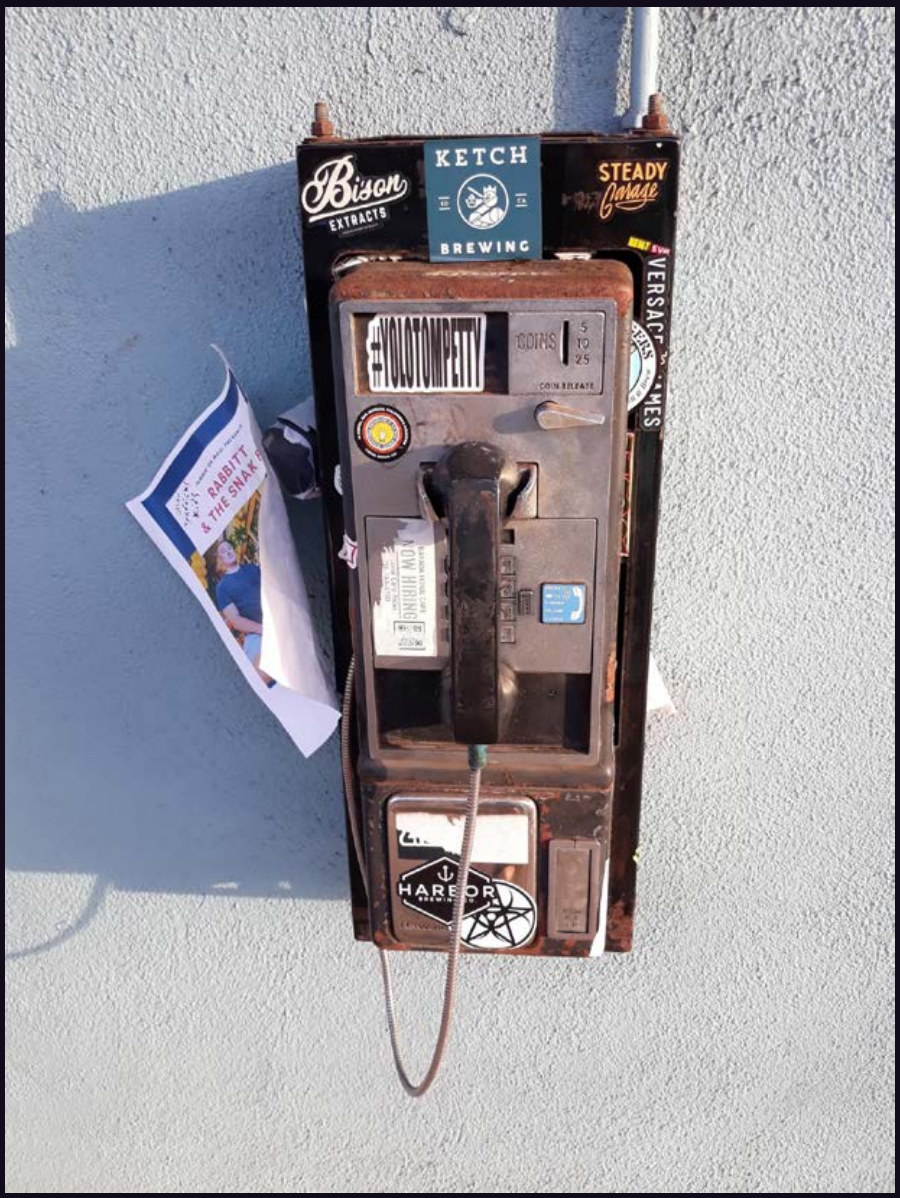
Photo by Daniel Cioaca

Working Payphones

Switzerland. Spotted at the Thunplatz train and bus area in Bern, this efficient looking model looks like it's prepared for just about anything.

Photo by Tom Dalton

Working Payphones



United States. Seen on the Hawaiian island of Maui in the town of Paia, you would never think this phone was actually in working order. But it is! And it moonlights as a bulletin board.

Photo by Jim

Working Payphones

Canada. These win the prize as they're all working. You'll have to go to the B gates at Vancouver International Airport to see them, but it's well worth the trip.

Photo by Babu Mengelepouti

Uncertain Payphones

Ireland. We've seen phone booths converted to libraries but this is a first. Seen in Westport, this former phone box now sells eggs on the honor system. (And it's also a library.)

Photo by Daniel Cussen

Uncertain Payphones

France. We honestly don't know what's going on here as most of this phone's features seem to be obscured by dust or sun or just fading into nothingness. Supposedly all payphones in the country were disappearing by 2018. Here's one they missed.

Photo by Nicolas RUFF

Uncertain Payphones

United States. Found at a Buca Di Beppo in Washington DC, this phone appears to defy the odds by even existing. The coin vault and instruction card were once updated, but nobody ever got around to replacing the handset sticker for Bell Atlantic, a company that hasn't existed for more than 22 years.

Photo by Byte Stealer

Uncertain Payphones

United States. Where else but inside the New York Public Library on Fifth Avenue in New York City would you expect to find a payphone in an old-fashioned wooden booth with chair, fan, and light? It's actually one of several. But you'll be disappointed if you expect any of them to work.

Photo byAnne Jackson

Defiant Payphones

England. As long as these boxes exist, we'll always believe there's hope for payphones. You can find them dotted all throughout the country. This one was in Whinfell Forest, Brougham, Cumbria.

Photo by XCM

Defiant Payphones

United States. You may have heard stories a few months back about the last payphone in New York City being disconnected. But there are still plenty around and here's the proof. You can visit this one in the subway station at Rockefeller Center.

Photo by Zachary Edminster

Defiant Payphones

Austria. You may think it's the plant that's being defiant here in Vienna. But it's the payphone that's really struggling to remain relevant. And this one works fine - if you can get to it. (And note the size of that phone booth!)

Photo by Richard Hanisch

Defiant Payphones

England. This phone seems a bit defensive with its threatening tone and use of the word "loser." But it's clearly been through a lot and is likely still under constant attack. Even the nasty ad warning against vandalism has been defaced.

Photo by Matt Thrailkill

Colorful Payphones

Spain. This pleasant looking model was found in Pontedeume, Galicia and is owned by Telefónica, the oldest communications company in Spain. Their old "T" logo can still be seen above the receiver. Unfortunately, the phone is not in service.

Photo by Francisco J. Tsao Santín

Colorful Payphones

Gabon. This grimy but intact model lives in the train station in Booué. But when picking up the receiver, nothing was heard.

Photo by Vernon A. Thorax

Colorful Payphones

Vatican City. Discovered by the Sistine Chapel, this bright yellow phone only works with cards that you can buy at the local post office.

Photo by Matt Anderson

Colorful Payphones

Israel. Spotted inside the old city of Jerusalem inside the Greek Patriarchate, this payphone still has a dial tone, but can be used to make free calls only.

Photo by Babu Mengelepouti

Foreign Payphones

Brunei. Half of a pair found in an empty parking lot next to the Royal Regalia Museum in Bandar Seri Begawan, this phone is only set up for calling cards. You can see the old JTB logo on the sign above. The newer TelBru logo can be seen on the sides of the kiosk. There's no sign of the current name, which is Imagine.

Photo by Sam Pursglove

Foreign Payphones

South Korea. Seen in the countryside town of Suncheon, also half of a pair, both of which were fully operational. This close-up view shows how both coins and cards are accepted. Operated by KT, formerly Korea Telecom.

Photo by Nara

Foreign Payphones

Australia. This phone is located at the Waurn Ponds Shopping Centre in Geelong, Victoria. Unlike most payphone companies, Telstra has made their phones completely free for calls within the country. (You can see how someone has scratched off the "pay" part of "payphone.")

Photo by DarkLight

Foreign Payphones

Canada. Spotted at the Northern Store in the remote community of Churchill, Manitoba. Pressing the button gets you a free call to the local taxi company. (We don't know what happened on October 1st.)

Photo by TProphet

Artistic Payphones

Germany. Seen in a museum in Düsseldorf, this is an actual work of art by the artists Christo and Jeanne-Claude. The notes next to the exhibit say the payphone "was an important object" during their time in New York City when "they had to communicate with numerous people." We concur.

Photo by Kai Kramhoeft

Artistic Payphones

United States. This working phone is directly outside the Buncombe County Courthouse in downtown Asheville, North Carolina and is used by people without cell phones who are going through court proceedings. The positive and comforting messages here have likely helped many through difficult times.

Photo by Will Hazlitt

Artistic Payphones

Poland. This relic was found at the Klubokawiarnia KEN54 pub in Warsaw. The phone itself would qualify as a work of art, but the surrounding decorations certainly add to the atmosphere.

Photo by Sam Pursglove

Artistic Payphones

United States. Maybe it's the landscape or the way the colors really seem to go well with each other, but we found this non-working, lonely phone to be a thing of beauty. Seen in Julesburg, Colorado along the South Platte River Trail Scenic Byway.

Photo by Screaming Yellow Fish

The Rule of Law

We've complained about a lot of things in these pages over the years. And we don't see that coming to an end anytime soon.

In the hacker world alone, there have been so many cases of injustice that many books can and have been written concerning only some of them. This has been the case from the beginning, mostly based upon fear and misperceptions. Intelligent people are punished, castigated, thrown out of school, fired from their jobs, even sent away to prison all because of fear, anger, and a general lack of understanding.

It's that last element that feeds the other two and it parallels so much else that goes on in the world and that has filled our history. Not understanding people who are different in some way is what causes some to want to hurt them - or at least to keep them far away.

We speak out about these things because we feel we must. Especially those instances where more people seem to disagree with our conclusions... those are the ones where our voice may be the only opportunity to hear a different perspective.

But, of course, injustice is everywhere, and the hacker community is rather tiny when put into perspective. In the larger world of technology, we frequently witness issues of privacy intrusions, corporate abuse of technology, governmental overreach, or just plain old shoddy security that helps make it all possible - this is all injustice of a different kind that affects everyone in some manner. Technology enthusiasts like us have a unique view into these issues and often can explain things in ways that others can't or won't. Again, we feel compelled to use our voices to draw awareness when it all just doesn't seem right.

And, of course, we also touch upon the bigger picture on occasion, where events are just too consequential to ignore. Movements towards fascism, oppression, mass disinformation, or all manner of ugliness that can turn the tides of history - these cannot go unremarked, even when our voice is but one microscopic element of a chorus standing up against the darkness. We must never silence our true feelings, not when we feel alone nor when we feel like we're amongst millions.

But throughout all of these instances, each and every time we've spoken out on some issue, raised awareness of an injustice, or questioned assumptions, we've never given up on the system itself, even when that system was proving to be corrupt or broken. We always believed that there was a pathway for justice to prevail, however difficult.

We've seen federal agencies like the FBI and the Secret Service lie and abuse their power many times over the years. We've witnessed all kinds of abuse by law enforcement in many jurisdictions. And we've experienced our share of ignorant judges, caught up in their own feelings of power and control, unwilling to learn or question their own preconceived notions.

But we've also seen good. We've been there when justice *has* prevailed. We know that the system can change if we get involved and start changing it from within. We believe in people power, a difficult but invaluable nut to crack, but which is capable of forever altering everything once awoken.

While some of this might seem naive and hopelessly optimistic, what matters is that we all speak our minds honestly and do our best to build the world we want, all the while dealing with the inevitable setbacks and disappointment. The progress is there if we're willing to see it.

In recent years, we've been disturbed by increasing signs that these beliefs aren't actually held by everyone, particularly those who had previously claimed to value them more than anyone else. And apparently, all it took to unveil this well hidden truth were some simple setbacks of their own.

Recent events in our nation have uncovered some truly shocking truths. The sense of entitlement that a particular faction clung to turned into something much uglier once it was questioned and defeated. Many of us saw

something like this coming. But the majority didn't realize what we were facing until January 6, 2021. That was when we almost lost our democratic system of government. On that day, not only was the United States Capitol stormed by violent protesters at the behest of a defeated president, but it was attacked from within by lawmakers who tried to carry out this president's orders and overturn a legitimate election. There is nothing in that statement to debate; this is very well documented from all sides.

To see police violently attacked by the very people who claimed to be their biggest supporters really put things into perspective. Apparently this "support" was contingent on their not being on opposite sides of an issue. Once that happened, law enforcement became the enemy and were even called traitors by those who had assumed police would help them overturn the election.

Fast forward to this summer when the now former president was accused of having stolen a bunch of top secret documents that could threaten the country's security, as well as put a number of individuals in harm's way. Once more, the entitlement kicked in with him and his cronies believing they somehow couldn't be touched by the law. But that's not how the system is supposed to work.

When the FBI did their job and conducted a search of the location where these documents were believed to be, *they* now became the enemy. Members of Congress were quoted saying things like "Defund the FBI" and even "We must destroy the FBI," referring to them as part of the "deep state," jackbooted thugs, Democratic operatives, you name it. Names and addresses of agents were made public. They were now targets.

We believe all of this illustrates a very basic fact. For all of the times we've found our community to be the victims of injustice at the hands of federal, state, or local authorities, we fought back through our words and whatever legal representation we could muster. We condemned actions that we found to be unfair and we called people out who were acting in a particularly dishonorable way. But we never advocated attacking, targeting, or causing any sort of harm to them as individuals, nor did we attempt to tear down the institutions they represented. We certainly called for change and for people to be held accountable for their actions. That's how the system *should* work.

The people who have been in the headlines recently don't have the same confidence in that system. When things don't go their way, they become violent in short order. It doesn't matter if what they are fighting against is the will of the people or a representative of law and order. It doesn't matter if it's a person they were friends with a few days ago. Once you cross whatever line they draw, *you* become the enemy. We've seen this happen repeatedly and it's both fascinating and frightening. But it's also empowering because it makes it so much clearer that all of us who have been standing up to injustice over the years - whether through the courts or in the streets - have been on the right side of history. We don't even have to agree with each other; it's the act of standing up for your beliefs and fighting back against the wrongs you perceive that qualifies as honorable. We all need to recognize that.

There are some tough times ahead. When this issue hits the stands, we will have just come through an election that will push us in one direction or another. We're either feeling inspired or dejected, or perhaps a combination of each. What we can't let go of is that feeling of healthy rebellion, constant questioning, and a willingness to take action. Only the truly desperate feel the need to tear everything down and collect enemies when they don't immediately get what they want. Their tantrums show their immaturity, along with their lack of belief in democratic systems that often require an abundance of patience and a lot of time.

We have a great deal to fight for and about. And we're not at all thrilled with how the system is designed and abused by those with power. But our dissatisfaction doesn't push us into despair. Instead, it serves as motivation for us to try harder and continue the battle for another day. It's easy to forget how these challenges are putting us in a better place. Sometimes it takes the actions of those who are on the wrong side to really make this clear.

A New HOPE: Release Notes

by Members of the Organizing Committee for A New HOPE

We would like to share some of the decisions we made when planning and implementing A New HOPE, and describe some of the outcomes and lessons learned. We offer this as a reflection on what worked well and what could have been better. We aspire for this article to be helpful to people organizing other conferences, and also as a guide to planning future HOPE events.

HOPE Conference Background and History

HOPE is Hackers On Planet Earth, a conference series sponsored by *2600 Magazine*. The first HOPE conference was in 1994, and they have happened more or less every two years since then.

Most HOPE conferences have been three-day events, featuring a very wide range of talks as well as lots of other content. Workshops, performances, villages, tutorials, and lots of unplanned hallway interaction all contributed to fun-filled and very informative conference programs.

Until 2022, all HOPE conferences but the second had taken place at the Hotel Pennsylvania, a large but dated hotel in the heart of midtown Manhattan. Unfortunately, Hotel Pennsylvania is now being demolished to make way for a new office skyscraper building.

HOPE in 2020 was an entirely virtual event, with a full range of talks and workshops, but with everything online. Most past events since around 2002 had three simultaneous talk tracks, but in 2020 there was only one talk at a time, along with one workshop and some late night performances. This conference lasted a full nine days. You can find out more about HOPE 2020 at `xiii.hope.net`.

After The Circle of HOPE in 2018, the Hotel Pennsylvania dramatically increased its prices. Because HOPE strives to be a relatively inexpensive event to attend, we started looking for other possible venues.

We put out a call to HOPE fans, looking for potential venues. We heard about quite a few, all around the U.S. and even in a few other countries. We followed up on many of these suggestions, and we also heard a strong preference for staying in New York City - it's a great destination, for many purposes.

Choosing a New Venue

In Spring 2019, we issued a Request for Proposals (RFP) to look for other venues around the New York metropolitan area. We got some great free support from the New York Convention and Visitors Bureau to identify candidate venues and distribute the RFP to potential respondents. We made sure to reach out to all the places that had been recommended that were within 50 miles or so of New York City.

The RFP generated some strong responses, and we ended up working with a couple of major Manhattan conference hotels to get an estimate of costs. We also heard from St. John's University, based in Queens, New York.

St. John's seemed like a good fit for us. It is an idyllic campus in a city neighborhood that is busy, but not nearly as built up as midtown. On-campus housing was available, and they had relationships with some nearby hotels that could offer discounted blocks of rooms. They had some pretty good spaces, including some large auditorium or theater-style rooms.

Working With Volunteers

One of the key benefits of St. John's was that there were no impediments to volunteer labor. All of the conference organizers are volunteers, and HOPE runs on volunteer power. Volunteers operate the info desk, the audio/visual production, setup and cleanup, and everything else.

We had learned at Hotel Pennsylvania that many hotels have labor unions for their staff, and there are requirements for using contractors that are part of labor unions. We are in favor of labor unions, and would love for the people working for pay at our events to be part of unions. However, the union restrictions at hotels make it difficult and expensive to use volunteers.

Hotel Pennsylvania was less restrictive, as only part of the hotel was unionized. We found out that the big Manhattan conference hotels are entirely unionized.

As a brief example, if we wanted to bring and set up our own audio/video equipment, we would need to pay union employees to set it up, plug it in, and operate it throughout the conference. If we wanted to have our own volunteers do that - or other activities like setting up tables and chairs, running a video camera, setting up our own lighting and sound, or even unloading a truck full of gear we had rented - we could only do this if our volunteers were augmented by "shadow" labor by union personnel, at their regular hourly rates.

These union policies followed by the big conference hotels were all fascinating to learn about, and ultimately meant that we could not have a conference in a major Manhattan

conference hotel without significantly increasing our costs, and also limiting our use of volunteer labor and donated equipment.

Pivoting in 2020

The lack of restrictions on using volunteer labor at St. John's was another benefit. We visited the campus and liked what we saw: This could work! In addition to being a suitable venue, St. John's has a strong cybersecurity program, and they seemed to see their interaction with HOPE as synergistic with what students learn in the program.

By late 2019, we had a contract with St. John's University for the 2020 event to begin in July. We did some planning and opened the Call for Participation by the end of 2019. We were on track for another great HOPE event!

And then, COVID-19 struck. By March 2020, it was looking increasingly unlikely we would be able to have HOPE in person. Lockdowns and other restrictions on gathering were happening everywhere, including New York City. Universities were sending staff home and shifting to all-virtual instruction. A vaccine against COVID-19 was, at the time, still just a theory.

We pivoted, and HOPE 2020 was instead held as an entirely online event.

Teleconference Choices in 2020

For 2020, we followed a similar process of program planning as for our past events: a Call for Participation soliciting proposals for talks, workshops, performances, and other content, and then an evaluation and selection process.

Delivery was entirely different, though. We had four main groups of challenges:

1. How would presenters give their presentations?
2. How would attendees view the presentations?
3. How would attendees interact with each other and with presenters?
4. What parts of HOPE would be free to anyone, and what parts would be restricted to those who purchased tickets?

For the first challenge, we tried all the mainstream technologies. We selected Zoom (`zoom.us`) for speakers, and Big Blue Button (`bigbluebutton.org`) for workshops.

The choice of Zoom was based on the capabilities of the client. We test-drove many of the available technologies, hoping to find free software that would perform well. Unfortunately, we found that the free software clients were sometimes challenging to install, and the teleconference experience was often glitchy (audio/video dropouts, poor performance with low bandwidth, or unreliable network connections).

Zoom "just worked," and in early 2020 "Zoom" was often being used synonymously with "teleconference." We decided we would have a live moderator who could interact with the speaker, and a live (remote) production crew using Open Broadcaster Software (`obsproject.com`) to mix the Zoom teleconference with a background, and also we used `otter.ai` to provide live automated transcripts.

Because we were nervous about teleconferencing problems, including situations where speakers had network outages or other issues that prevented them joining the live conference, we encouraged speakers to pre-record a talk of approximately 30-40 minutes and upload it in advance. Most speakers did pre-record, and that resulted in some really fascinating and well-produced talks.

The HOPE conference emcee introduced the live speaker, then we played back the pre-recorded talk, and the speaker took questions afterwards from the emcee via Matrix (`matrix.org`).

Attendees didn't use Zoom. Instead, they watched the livestream. The livestreams for talks and performances were broadcast by our partners at The Internet Society (ISOC) to `livestream.com` (Vimeo) on the ISOC channels, as well as to YouTube and Twitch. Archiving to The Internet Archive happened right after each talk.

You can find all of these talks online on YouTube at `www.youtube.com/user/➥channel2600`.

For workshops, we decided to use Big Blue Button. This is great free software. Even though the client isn't as reliable as Zoom, it has tremendous features for instruction. With BBB, it's easy to have breakout sessions, to have attendee-to-attendee interaction, and to have moderation as needed.

The workshop presenters in BBB were supported by a live volunteer who assisted with setting up the BBB environment and provided additional support throughout the workshop.

Most workshops were recorded, but they did not get the same level of live production via OBS that talks did. You can find 22 workshop recordings on YouTube in Channel2600.

For attendee interaction, we chose Matrix. Matrix is an open standard and communication protocol for chat and other real-time communication. We ran our own Matrix home servers and, since it's a federated system, people could join if they already had an account on another home server.

We collaborated with the folks at `element.➥io` on solving a couple of issues. Talented HOPE volunteers set up our servers and created a bot that would let people into the Matrix chat

forums for HOPE 2020 when they provided their ticket code.

All of our challenges were met! People with tickets could get into the Matrix chat forums and interact with presenters and each other. The general public could watch the livestreams in a few different ways. We had volunteers doing live production, and ended up with very few technical glitches or quality issues with the speakers, workshops, and performances.

All of this experience served us well when we started planning for HOPE in 2022.

Planning for A New HOPE

By late 2021, it was beginning to look like a live event in 2022 was going to be viable. A vaccine had been developed and, since the start of the pandemic in early 2020, a variety of approaches to having relatively safe public events had been proven.

We set up a new contract with St. John's, launched a new Call for Participation, and started getting ready for the summer. We decided to call this event A New HOPE. This name was chosen to recognize and celebrate how science had brought us understanding and protection from the virus, and that so many of us had learned how to better care for each other by following the best current health guidance, like physical distancing and wearing masks.

The name A New HOPE also recognized the tremendous losses of life, health, and opportunity that had happened during the pandemic. In case you are wondering: We never heard from Disney with complaints about how our name is similar to a certain well-known science fiction movie franchise. The name A New HOPE is not "confusingly similar" to their trademark.

By the spring, we decided that A New HOPE would require all attendees to be fully vaccinated. We also decided that (unless the situation changed) we would require people to wear masks in all indoor spaces, except while on stage or eating and drinking. If you are a regular reader of *2600 Magazine*, or a listener to the *Off The Hook* radio show, you already know that *2600* values following the best current scientific and health guidance on how to protect ourselves and each other from COVID-19.

A vaccination and mask policy for A New HOPE made a lot of sense, and we got a lot of positive feedback from attendees about this. We also got some negative response, and almost none of the people who responded negatively ended up buying a ticket.

Building Community

During our virtual event in 2020, we found there was a lot of pent up desire among hackers to be able to interact with each other again, and to have a conference that touched on all the hacker themes that HOPE is known for.

Leading up to 2022, it became clear there was a lot of enthusiasm and anticipation for actually getting together again. So many of us had felt isolated during the pandemic, and teleconferencing and other online contact are not enough.

During the opening and closing ceremony sessions at St. John's, speakers emphasized that we were all there because we wanted to be part of the HOPE hacker community. Attendees had made the decision to show up in person because this was going to be a richer experience than watching a video and interacting by chat.

More importantly, the opening ceremony put out the expectation that we were going to be conscientious and caring for one another. Conference organizers knew that many attendees were nervous about being at a large in person event, due to the lingering presence of COVID-19 and also due to being somewhat out of practice at live face to face interaction. St. John's was a new venue and not as centrally located as Hotel Pennsylvania. We'd all need to allow each other, and ourselves, a little slack in our interaction.

Being Excellent to One Another

Another part of what was expected of attendees was increased awareness of the goal of "being excellent to one another." This is the core tenet of the HOPE Code of Conduct. There were some real failures in how some CoC and security-related issues were handled by HOPE in 2018, and we worked hard to design a more effective multi-layered approach for 2022.

One great benefit to A New HOPE was our partnership with Operation Hammond. This is a group of volunteers who provide support to attendees with issues related to Code of Conduct, mental health, first aid, or other concerns. Hammond dovetailed with the HOPE security team, whose volunteers were mostly responsible for physical security and the conference perimeter. St. John's also had campus safety personnel on-site, to facilitate emergency response as well as to interact with other campus personnel.

Internally to the organizers, security team, and Operation Hammond, we had developed an escalation pathway for different types of issues we might encounter. We communicated this to volunteers during a pre-HOPE volunteer teleconference and gave a summary during the opening ceremony. We did end up encountering a few issues during A New HOPE, and our plans worked out well. We can only credit planning partially, though; we also credit that the vast majority of attendees were polite, patient, supportive, conscientious, and self-aware.

The sense of community, which developed

before and strengthened during A New HOPE, was wonderful to be a part of. In post-conference feedback messages, many attendees expressed gratitude for being part of it. We are optimistic that the same sort of community feelings and mutual respect will be able to continue at future events.

Technology Choices

Building on our experiences in 2020, we decided to use Zoom for our handful of remote speakers. Most speakers, all performances, and almost all workshops were in person at St. John's.

In the month leading up to A New HOPE, we ran into issues with our technology planning and rentals. Lots had changed since our previous in person event in 2018 and, among other things, the prices for our audio/video rentals had skyrocketed. To make a long story short, we made a last-minute change to work with an organization called Sonus (via an introduction from another hacker conference) that would run the livestream. They did a great job.

The livestream was important for virtual ticket holders, as well as attendees who could not attend in person due to COVID-19 and other challenges. It was also a great way of watching talks and other content from hotels or from simulcast rooms we set up at St. John's.

Perhaps more importantly, at least for posterity, the livestream was also recorded and archived to Channel2600 on YouTube. Videos are also available for free download elsewhere, and you can buy a copy of all recordings online at the *2600* Store (`store.2600.com`).

Because of the last-minute changes, we only ended up sending the livestream to YouTube (plus we sent part of the first day to Facebook, but almost nobody was using this and we didn't get it running again).

The overall on-site experience at A New HOPE was comparable to recent HOPE events at Hotel Pennsylvania. Volunteers built out wonderful spaces for talks and performances, with theatrical lighting and sound for two main speaker tracks. A third track in a smaller room had a less sophisticated A/V buildout, but still had a high quality livestream.

Workshops happened in classrooms in our main St. John's building, using in-room projectors. We had some rooms set up for classroom-style workshops, and others with tables suitable for things like soldering or other hands-on activity. Workshops were not recorded or livestreamed, but one of the workshop presenters got COVID-19 just before A New HOPE and made remote presentations.

We used the same Matrix chat as in 2020, and the same bot and ticket system to allow ticketed attendees access to the conference-specific chat forums. Live on-site emcees would monitor the Matrix chat, as well as the speaker room, for audience questions. There was a Mozilla Hubs virtual environment, too, where people could watch the talks and interact with each other.

The infodesk volunteers also monitored Matrix chat, so they could give great help to any attendee, whether they were on-site or not.

Copyright Strike

In 2020, we made detailed plans to avoid all types of outages and problems. We had multiple livestream providers. We had backup volunteers. We added DDoS protection to our conference website and other systems. In 2022, the intense planning for the conference, with a primary focus on being in person, led us to forget some of that caution.

Due to the last-minute change in our plans for the livestream and recording, we had set up streams to YouTube only.

During our 8 pm Saturday slot, a fantastic presentation was happening, called "Hacker Representation Through the Years: A Guided Tour of Hacker Appearances in TV and Cinema." As you might expect, this talk included brief clips from media.

In the midst of this talk, our YouTube stream was taken down by Google, in what they call a copyright "strike." This is when an algorithm decides that your content is violating someone else's copyright or another of the YouTube terms of service.

Figure 1 shows what people watching the livesteam saw.

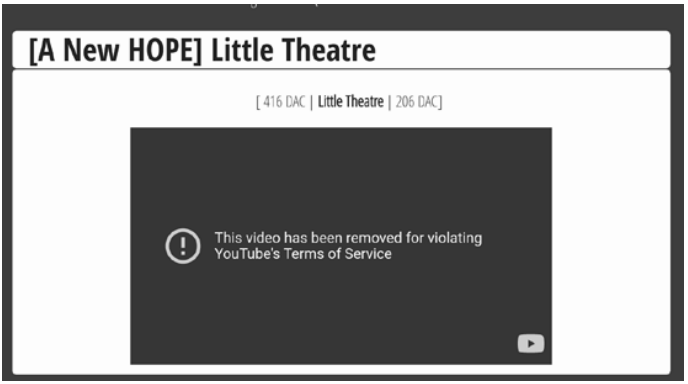


Figure 1: YouTube's notice of video removal

Ironically, we discovered the strike was

specifically due to a short clip from the *Mr. Robot* series. This is a fictional series about hacking, which many people think is quite accurate about hacker activity and culture.

Panic ensued. A second copyright strike would mean that all the Channel2600 livestreams would be removed for a week. There was essentially no pathway to a mitigation or review, and Google's algorithm has no notion of fair use.

The "fair use doctrine" is a crucial part of U.S. copyright. It means that copyrighted content may be utilized, without requiring permission, for certain purposes. Some of these purposes include brief extracts, scholarly use, and satire. At 8 pm on a Saturday in July, there was no opportunity to make a case for fair use, and nobody at Google who we could find to listen.

Luckily, the Channel2600 maintainers were eventually able to identify procedures to get the livestreams restored. People watching the livestream missed much of the talk, but we were making an on-site recording.

The next part of the YouTube saga was a couple of weeks later. *2600* staff had worked tirelessly to convert the on-site recordings into 85 separate videos for distribution by YouTube, through *2600* store sales of USB drives, and other means.

When the "Hacker Representation" talk was uploaded, though, it was immediately and automatically blocked by YouTube. The other videos were available, but not this one, and the playlist with all videos was broken. As with the livestream, this happened algorithmically - there was no pathway to discuss fair use with anyone at Google.

2600 puzzled over this for awhile. We discovered that the video was online, but not findable in the U.S. YouTube. It was findable in the U.K. and Germany, because evidently the automated copyright complaint by the owners of *Mr. Robot* was only directed at the U.S. instance of YouTube.

Eventually, it turned out that there was an automated appeal process where Channel2600 could contest the automated takedown. This finally got the video available again on the YouTube playlist for A New HOPE when NBC Universal (the owners of the copyright) granted permission.

You can watch the video here: `www.youtube.com/watch?v=M_JA9m7vprg`

You can hear more discussion about this series of algorithm-driven events in recordings of the *Off The Hook* radio show from August 2022, online at `www.2600.com/offthehook`.

Some of the Lessons Learned

A New HOPE was a wonderful experience for the conference organizers, and many volunteers and attendees expressed their appreciation for a smooth event.

Post-conference feedback yielded a list of items of concern for the new venue at St. John's. While most attendees liked the campus setting, some found it to be too isolated - hotels were not close enough (and the discounted hotel rooms were sold out), we didn't provide enough information about nearby food options, and there wasn't as much nightlife in the area as would be found in midtown Manhattan. And because St. John's is a dry campus, attendees wishing to party needed to do it elsewhere (like the bar at the conference hotel). But this also had its advantages as we had zero late night drunken incidents at the event while continuing to operate around the clock.

The space at St. John's was quite nice. The classrooms worked really well for workshops and other things, like our live simulcast of the Dutch hacker camp happening the same weekend, May Contain Hackers. But it was tough going from one air conditioned building to another, through the heat wave that hit the area that weekend. Those with mobility issues found the campus had not made provisions with HOPE for parking close to the buildings, or shuttles between the buildings.

The dorms, which were used by around a quarter of attendees, meant another walk through the heat. St. John's dorm rooms were a great convenience - nearby and reasonably well appointed (though not as fancy as a hotel). But they charged by the person, which made it expensive compared to a hotel that could house two plus people. Also, St. John's offered no accommodations for family housing or for having multiple genders in a suite of rooms. St. John's only recognizes two genders, male and female, and required a lot of personal information to register to stay in the dorms.

All that said, we found St. John's to be a wonderful host. We had outstanding support from the campus information technology group, which operates the network and all the classroom technology. All the groups took great care of HOPE and its attendees, including conference services, facilities, performing arts, housing, custodial, and food service.

Attendees reported a very positive overall experience in talks and workshops, as well as for performances, villages, an unscheduled "fourth track" (open microphone), and other content. There was good variety, including the usual mix of highly technical talks, and those with a more social or humanistic nature - not

that different than prior HOPE events, and also not that different from the mixture of articles in *2600 Magazine*.

The experience for virtual attendees could be improved. It's tough to run a hybrid event (online and in person) when many key volunteers are already stretched thinly, and a successful virtual experience really needs a dedicated crew. For A New HOPE, the Mozilla Hubs environment was really cool, but could have been better utilized. The Matrix chat worked well, but there was not really an area for virtual and in person attendees to socialize with each other and feel more like part of the community.

There were around a dozen vendors who attended, to present their wares and have interesting discussions with attendees. There was a very nice lounge space for vendors, as well as a coffee house with Starbucks and a snack concession in the afternoons. This was also a good space to socialize.

Registration and badge pickup went very smoothly, with almost no wait. Everyone needed to present their proof of vaccination at the door, then get a wristband to pick up their badge using their ticket code. This was the same code that gave access to the online Matrix chat. There were almost no issues with proof of vaccination or with masking. Everyone needed to buy their ticket in advance - there were no sales at the door - and we sent out some advance emails so attendees knew what to expect.

We learned a whole lot about technological planning and resiliency. Firstly, we need to work harder to avoid last minute changes.

In the future, we will try to take a more professional-style project management approach to conference planning. For example, if we had used a tracking system for who-does-what, with target due dates and regular reviews of items, we would have greater visibility on things that were falling behind or creating risk.

An "agile" approach (in the sense of software development project management) would ensure that we're not going to be rigid. After all, we're a bunch of hackers, and also a bunch of volunteers; creativity and flexibility is our thing! But that doesn't prevent us from upping our game for planning, and having a mutual understanding of accountability with each other to come through on our commitments.

We definitely will revisit our use of Zoom for future teleconferencing needs. Free software packages like Jitsi and Big Blue Button have a lot of strengths and are improving over time. We can also expect that presenters of the future will be more experienced, sophisticated, and self-sufficient in the use of teleconferencing than they were in 2020.

Resiliency for streaming and our overall online presence will be a big focus for any future event. Luckily, this is not hard to do - it was an oversight in 2022 that we didn't have multiple streaming destinations. We would love to work with our friends at ISOC again.

We used Pretalx software for our online schedule. This is free software used by our friends at Chaos Computer Congress. In the future, we are considering adding an online web-based submissions and review process to supplement our existing email-based process. The expert reviewers and organizers for talks, performances, and workshops do a great job, but might benefit from a more modern online system.

Perhaps the best lesson learned, or re-learned, is how wonderful HOPE attendees are. The event in 2022 was friendly, filled with engaged and caring people. Presenters gave generously of their time and knowledge. The info desk, registration desk, network team, A/V team, Sonus, Operation Hammond, security team, *2600* store, emcees, media team, website team, and many many other volunteers made everything work, and helped to foster the sense of community that was so refreshing.

HOPE always welcomes input, as well as new volunteers. Keep an eye on `www.hope.net` as we work towards the next event in 2024. Feedback is welcome, by email to `feedback@hope.net` or in the letters department of *2600 Magazine*.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Internet of Problems

by RG

Recently I received a new LTE router in hopes of boosting Internet speed at home. If you aren't familiar with LTE routers, they are effectively a combination between a traditional home router and a cellular hotspot device. The Internet is provided via cellular towers and then served to end users as an ethernet or Wi-Fi connection. These devices have become more common for users in industries such as construction and for rural Americans who don't have access to many Internet service options.

Curious as always, I wondered if the device had any obvious security flaws. Many home routers are not secure by default and require additional configuration to minimize vulnerabilities. To work, the device utilizes a SIM card and is given a public IP on the carrier network. This is standard for cellular devices. However, the device also served up a configuration interface over port 80 on its public IP address by default. To make matters worse, the default username and password combination for the device was "admin:admin".

According to a survey by Broadband Genie, only 14 percent of the 2,205 survey respondents have updated their router's firmware and only 18 percent have changed the device's default admin account password. This survey was taken in 2018 and has since been widely referenced. While the education provided to many users working from home during the COVID-19 pandemic may have lowered these numbers, it is likely that many routers are still vulnerable. For instance, the previously mentioned survey also cited many users being confused by their router settings. Anecdotally, I've known plenty of people who are unable to distinguish the difference between their wireless password and the administrative console password.

Knowing that this device was by default unsecured, open to the web, and came with no documentation, I wanted to see how many similar devices were out on the open Internet. To do this, I first went to `shodan.io` and logged into my account. There are several options for web scanning, but Shodan is my preferred tool. I then performed the following steps:

1. Since I already knew my IP, I simply searched for it. This returned useful information about my device. Specifically, it grabbed the http banner and then hashed it. Additional information on pivoting with property hashes can be found here: `help.shodan.io/mastery/property-hashes`.

2. I took the banner hash for my device and searched for it. This search returned all devices similar to mine. In total there were 31 devices. Based on our numbers from before, we can assume potentially 25 of these devices are accessible with default credentials.

3. 31 seemed low for the number of LTE routers on the open Internet, so I tried a few different scans. One particular scan for "Server: GoAhead-Webs port:80 country:"US"" returned roughly 30,000 results. GoAhead-Webs is a simple web server used for devices without much memory and appears to be heavily used by lightweight LTE routers.

What can be done with this type of access? Look no further than Duran's article in Volume 38, Issue Number 4 of *2600* where they describe methods for finding and manipulating routers. It would be easy to lock users out of their devices, potentially upload tainted firmware, or even in some cases gain direct access to their network. This is not an invitation or encouragement to break the law, of course, rather the intent is to show the severity of the situation.

As previously discussed, many users do not understand how to properly configure their devices and manufacturers often do not provide sufficient security documentation. This combination of unsecured by default devices and no documentation puts the onus of security on the end user. In this case, manufacturers are passing off the cost of security. Currently, it's difficult to know which manufacturers are providing a better product when it comes to secure devices. Due to this lack of visibility, companies often are not incentivized to take this cost on as they see no competitive advantage in doing so. This is a major problem plaguing IoT devices. I've asked questions about this issue in a few webinars with security professionals and additionally have done research on the policy angle. The consensus seems to be something along the lines of an energy star rating equivalent for IoT devices. *Executive Order 14028*, "Improving the Nation's Cybersecurity," has required NIST to create a pilot program to do just this. NIST is currently in the process of defining the criteria of this program. While this may or may not be the best long-term solution, it's important that this topic is discussed and that the problem is continuously worked.

- *Survey Source:* `www.bleepingcomputer.com/news/security/survey-reveals-users-have-no-clue-about-router-security/`
- NIST IoT Labeling: `www.nist.gov/itl/executive-order-improving-nations-cybersecurity/cybersecurity-labeling-consumers-internet-things`

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It was a surprisingly calm summer here in the Great Northwest. We had cool temperatures and rain later into the summer than usual (I was beginning to call it "Juneuary") and this seems to have moderated the fires that engulf our region every year. Now that the summer is over, I'm glad I am not writing this year about fires engulfing our outside plant and *literally* burning up your phone line (although this is a continued high risk). Instead, let's rewind to the 1990s, and services that used to *metaphorically* burn up the phone lines of the Central Office: pay-per-call services.

"Now wait a minute," you might ask. "Weren't *all* calls in the 1990s pay-per-call?" Well, yes, you had to pay for a lot of calls in the 1990s (even local calls in some areas), but "pay-per-call" service was a special billing category. With a pay-per-call service, an information provider (such as a celebrity horoscope, dating service, lucky lottery number of the day, or whatever anyone could dream up to create) could *share in the revenue* from your call. This, at one point, led to a $3 billion industry that younger people today have never interacted with and probably don't even know existed.

Pay-per-call services were either regional or national. Here in the Pacific Northwest, US West first offered local pay-per-call numbers in the 976 exchange (NYNEX, the provider serving *2600*, offered similar services in the 540 exchange). This exchange was programmed to be an intra-LATA long distance call from everywhere, with special rates. This meant that if you wanted to call a 976 number, you'd have to dial 1 first. When you called one of these numbers (such as 1-976-6969, known as the "moan line," an interactive adult "service"), you'd be charged a higher rate than a regular long distance call. The rate was set by the provider and, naturally, it wasn't announced, and you didn't have to agree to the charges before you were billed (after all, you had dialed 1 first, so you knew there would be charges, right?). Unfortunately these services cost much more than a regular long distance call: up to $9.99 per minute!

The ~~ill-gotten gains~~ revenue would be split between US West and the service provider (in most cases via an intermediary called a "service bureau" who provided a voice platform and technology services at a fee, and who managed interconnection and billing with US West). Everyone was happy except for the parents of teenage boys, who would call the "moan line" and giggle until an eye-popping phone bill showed up in the mail (US West would be happy to negotiate a 50 percent discount with the bill-shocked parents, but they'd never write off the bill entirely). Back then, it wasn't unusual for teenagers to be grounded from the family phone, and groundings resulting from 976 calls were a very common occurrence at my high school!

In 1987, AT&T began testing a nationwide pay-per-call service in the 900 NPA. This was essentially the same idea as 976 numbers in the US West service territory, except that the service would work all over the country. Of course, long distance and service charges would go to AT&T as well, rather than to the "baby Bell" local exchange carriers it now competed with. The concept quickly took off, with everything from dial-a-psychic to sports talk services. (The "moan line" was conspicuously missing; AT&T and MCI, who later began offering "900" services, both banned adult content - initially in both theory and practice.) Keep in mind, this was before the days of the Internet, so most people only had access to information that was in the newspaper. Pay-per-call services allowed service providers to create both

broadcast-style and interactive services catering to niche interests. These valuable services were popular and millions of satisfied customers were happy to pay the charges. At least, this is the argument that service providers and the phone companies used when arguing with the FCC and Congress that they should be allowed to continue in the business.

Satisfied phreaks were certainly happy for someone else to pay their 900 number charges, and pay-per-call services were a favorite termination point from compromised DISA ports and beige boxes. Some of these services allowed setting up conference calls, allowing ten or more phreaks - all standing at different payphones - to talk for hours on someone else's $9.99 per minute dime. For extra phun, making a three-way fraudulent call to the "moan line" was always a good laugh for everyone on the purloined conference call.

By 1991, the pay-per-call industry was raking in close to $3 billion per year, and it peaked at *over* $3 billion in 1992. You could barely turn on a television without seeing an ad for a 900 number. However, billing complaints were truly getting out of hand, and pay-per-call services had become the Number One source of consumer complaints to the FCC. In response, Senator Daniel Inouye of Hawaii introduced Senate Bill 1579, which eventually passed in 1992 and introduced significant constraints on the pay-per-call industry. While there was a lot in the bill (which is linked below), it provided the following key consumer rights:

- No more deceptive advertising of rates and terms was allowed (so no mumbling the prices at chipmunk speed under blaring music).
- Rates were required to be clearly announced when the call was answered, and the caller would have an opportunity to hang up before being charged.
- New restrictions on advertising to children were introduced.
- Carriers were required to block pay-per-call numbers upon request of the subscriber, only a nominal one-time fee could be charged, and no fee was allowed when blocking was requested within the first 60 days of establishing service.
- Dispute resolution procedures were required.

There were also some unrelated provisions in the bill, including an infamous provision that made it illegal to listen to analog cellular calls, or to sell radio scanners capable of monitoring these frequencies. Privacy concerns had become an increasing issue with cellular customers, so pretending that certain radio frequencies didn't exist was the solution prescribed by Congress. To this, OKI 900 said "Good Timing."

In the bill, Congress directed the FCC to do most of the heavy lifting in creating and enforcing the rules. The FCC addressed this with gusto, given that, as mentioned, pay-per-call billing disputes were their Number One complaint. While it's true that the rules they issued could perhaps be described as a telecommunications embodiment of Thor's hammer, they were probably not responsible for the rapid decline of pay-per-call services. 1993 was right around the time that dial-up Internet service started to gain early popularity, and much of the information previously only available on pay-per-call services was *freely* available online, on services such as AOL. By 1995, dial-up Internet capability was included in Windows 95, and Internet usage exploded. Pay-per-call service revenue dropped precipitously in line with the rise of Internet popularity overall and, by 2013, Verizon (the last remaining "900" service provider) finally ended service.

And with that, I'll see you again in the winter. Drive safely this fall, and if you are looking for Halloween costume ideas, consider dressing up as an AT&T bill for 900-number calls!

References

www.csmonitor.com/1991/1030/30091.➥html - "Pay-Per-Call Services Ringing Up Lots of Flak"

www.congress.gov/bill/102nd-➥congress/senate-bill/1579 - Senate bill constraining pay-per-call billing practices

www.deseret.com/1991/7/17/18931201/➥complaints-about-900-service-➥skyrocketing-senate-panel-told - "Complaints About '900' Service Skyrocketing, Senate Panel Told

Keeping America Informed: An Introduction to Government Documents

by Infra Read

The motto of the U.S. Government Publishing Office (GPO) is "America Informed," and for us to be informed, it helps to know what our elected officials and other people with power are saying and doing. Much of this is made purposely obscure, but a massive amount of government documents is out there, and they can be a way to find out in more detail what our government is up to.

The GPO makes reports and publications of all kinds available to the public, including transcripts of hearings from the House, Senate, and government committees on every subject. The Federal Depository Library Program (FDLP) sends free copies of physically published documents to participating libraries, who are legally required to give the general public access to the documents.

That means that a local university may restrict most of their services to their tuition-paying students, but if they are part of the FDLP, they need to provide general access to their government documents. This should include physical ones on their shelves, and electronic documents that are accessed through their online card catalogs. If they don't allow physical check-out, they have to let people access them on-site, and if computer access is generally restricted, they have to provide some way, like temporary passwords, for anyone off the street to access the documents from a terminal in the building. A map of libraries in the FDLP is at: `ask.gpo.➥gov/s/FDLD`. The libraries listed as "Regional" receive and keep basically all documents that are published through the program; the "Selective" ones only receive selected documents, and they are allowed to remove older ones from their collections.

Fortunately, the majority of new government documents are available in electronic form, and anyone with Internet access can view them for free. The main Catalog of U.S. Government Publications (CGP) is found at: catalog.gpo.gov/. This is a pretty straightforward search engine, although keywords with too many hits can sometimes cause an error.

To find the most recent documents, you can search using the "Electronic Titles" link under the "Catalogs to Search" banner at the CGP home page. This brings up a search field for electronic documents only, and a link for "New Electronic Titles," monthly lists of the recently released titles. This will include older records that have been digitized and added to the listings. The backlog of documents, from before digitization was the norm, is continually being worked on. For example, the July 2022 list contains a series of technical reports from the 1940s' National Advisory Committee for Aeronautics, a report on welding techniques from 1963, and space shuttle structural analyses from 1989.

Between transcribing, digitizing, and releasing the documents in a finished form, there can be time lags, so sometimes even a document with a publication date of 2022 can be for a meeting from 2017. A lot of it is fairly current, though, and hearings on big, newsworthy subjects, such as the impeachment hearings for Donald Trump or the January 6th riots, will usually get printed and distributed fairly quickly.

All these searches should bring up electronic resources with purls (permanent URLs), and unlike many library systems, the search logic is fuzzy enough to bring up related subjects. For example, a search for the term "cyberpunk" doesn't have any hits, but it does bring up similar terms; for example, "cyberprotests" (which were considered a "threat to the U.S. information infrastructure" in a 2001 report from the National Infrastructure Protection Center (`purl.fdlp.➥gov/GPO/LPS15585`).

In the results list for "cybersecurity," there's also more recent information, like the hearing on the "Cybersecurity State Coordinator Act of 2020 report... to establish a Cybersecurity State Coordinator in each state, and for other purposes," from June 2020.

Some of these documents are very dense and legalistic, clearly not designed to be read by the general public, but others, like the Congressional hearings, are often more readable, even interesting, since they include direct transcripts of everything spoken, and even note when there's laughter during a hearing.

A related resource of interest is the Congressional Research Service at `crsreports.congress.➥gov/`. They have some interesting things like the "Overview of Governmental Action Under the Stored Communications Act (SCA)," which "governs access to stored wire and electronic communications such as emails and other online messages held by service provider," currently being looked at for its relationship to private messages via social media.

One particularly interesting government entity was the Cyberspace Solarium Commission, a cybersecurity taskforce whose documents are available at `www.solarium.gov/`. This was a working group that produced white papers, a cybersecurity briefing for President Biden, and

a 182-page final report of proposals from 2020, including "Reshape the Cyber Ecosystem" and "Preserve and Employ the Military Instrument of National Power."

Much of the specific work on cybersecurity is done under the umbrella of the Cybersecurity and Infrastructure Security Agency (www.cisa.gov/), an agency under DHS oversight that contains multiple specialized divisions, including the National Security Telecommunications Advisory Committee. Many of their hearings and documents are available through a CGP search. The Department of Defense maintains a separate U.S. Cyber Command, but much of their documentation is available only through Freedom of Information Act requests, not through the GPO.

All the material produced by the GPO technically belongs to the American people at large and is legally required to be made available to them. This is a little-known resource, but while some of it takes work to weed through, it's full of information.

- Main GPO page: www.gpo.gov/
- Main FDLP page: www.fdlp.gov/
- List of government entities and their types of publication available through the FDLP: www.fdlp.gov/sites/default/➥files/listofclasses.pdf

Windows Installers

by street

Windows files with the MSI extension are used to install software packages. They do this by extracting themselves to the file system and modifying the Windows registry. They are special files used by the Windows operating system. Normally we take these files for granted, and trust the source that they come from.

MSI installation packages can be built with several tools. WiX and Visual Studio Community Edition are both available free and can build MSI packages.

The gold standard for building MSI packages has always been InstallShield. While InstallShield offers a free demo, the price of the commercial license was more than I could afford. But that didn't stop me!

Revenera is the company that owns InstallShield, and they also provide training courses for their product. It wasn't necessary for me to take the courses, because they already have free documentation online (docs.revenera.➥com/?product=InstallShield).

Using InstallShield to create an MSI file is very simple. You can add files and folders from your computer into the project, and then tell InstallShield where you want it to install them on the target machine. It can even add shortcuts to the start menu and desktop, or modify the registry. It's not hard to make your own forms, or change the default ones. The dialogs are customizable, and you can add your own graphics.

If you open the dialogs from the InstallShield menu, you can click on the dialogs text and graphics and quickly change them. You can also change a dialog's button and modify its destination to another dialog that you want the button to lead to.

As a hacker, I'm interested in what MSI packages aren't intended to do. I can use an MSI file to bundle legitimate software along with malicious code. I can even take a legitimate MSI file and reverse its installation by preserving the file structure and registry entries of the original installation. Add a simple reverse shell or whatever additional software you want. Then add a registry entry to Windows, telling it to run the new program at startup.

Microsoft provides a free tool called Process Monitor (docs.microsoft.com/en-us/➥sysinternals/downloads/procmon). This tool lists all the changes to the Windows file system and registry. It becomes a simple matter after that to build the delivery system for a trojan horse program.

Any kind of malware could work as a payload, and there is no need to change the flow of the original program or understand low level code. The only change is in how the software is installed.

Most companies will sign their programs with digital signatures to prevent the code from being modified. To do this they will buy a code signing certificate, which uses public/private keys to verify the program's integrity. However, creating a new Windows Installer does not actually modify the program.

The option to stop uncertified programs from running completely is something Microsoft has been playing with. They have been moving forward with new security changes in Windows 11 to only run apps verified in the Microsoft Store. This can prevent you from running perfectly safe software, or software that is even more secure than what is being offered in the Windows Store.

Microsoft has built a new installer format called MSIX. The MSIX format requires you to register the installer with Microsoft. They have not however stopped us from using the old MSI format.

Hack Your Brain

by Pavel Aubuchon-Mendoza

In the 1995 film *Johnny Mnemonic*, we see Keanu Reeves dive into a simulated representation of his brain and remove malware that had been slowly killing him. What a gift to have direct access to your brain with the ability to make changes for the good. Well, it turns out you can - no cybernetic dolphin required.

Your thoughts and emotions are not an abstract construct that emerges from your brain. Every thought has direct physical representation in your brain in the form of electrical and chemical interactions. If we had the technology, we could watch the electrical interplay of neurons that represent the words you are reading right now. Your thoughts literally are the physical interactions of your brain, and by changing our thoughts we can change the physical structure of our brain via the miracle of neuroplasticity.

In this article, we will draw an analogy between your brain and a computer system, and then absolutely beat that analogy to death. Please keep in mind that I am not a mental health professional (more of a hobbyist) and nothing I say should be considered medical advice. Talk to your doctor.

End Bad Processes

Over time, your brain inevitably has some bad inputs. You've got some recursive processes that just keep cycling back around and eating up resources. This can leave little remaining for the productive programs that you want to use. You can end the bad processes and assign a higher priority to the ones you want to enjoy. Learn to identify the negative thoughts before they spiral out of control, and stop them in their tracks. Know the things you want to enjoy, and revel in them. Let the enjoyment of small everyday things sink in. Your baseline emotional state can be generally positive, but sometimes it requires work. Reference *Rewire Your Anxious Brain: How to Use the Neuroscience of Fear to End Anxiety, Panic, and Worry* (Pittman/Karle) and *Hardwiring Happiness: The New Brain Science of Contentment, Calm, and Confidence* (Hanson) for specific instructions on how to do this.

Defragment Your Hard Drive

Okay kids, listen up. Back in the day, we had to defragment our hard drives to keep them running efficiently. Computers, much like our brains, don't always do a good job of storing information in real time. Events (particularly trauma) need time to get processed and filed away correctly. You know how sometimes you go to bed and you start thinking about everything you did that day? That's your brain starting this work. However, most of this happens while you sleep. If you're not getting seven to eight hours of sleep a night, your brain is not getting enough time to put everything away where it needs to go. The effects of not doing this are cumulative. Prioritize your sleep. If meditation is your thing, that achieves some of the same goals, but cannot replace sleep.

Invest in a Good Antivirus

Malware inevitably ends up on an unprotected system. It is simply the result of existing in the world. Sometimes they are insidious and indistinguishable from normal processes. In the worst case, they can give outside actors access to your core system. Fixing this is not something you can do on your own. Therapy is the antivirus for the brain. These are trained professionals who can identify and root out the malware that is disturbing your system. Therapy does not mean you are not strong and capable. Asking for help is an act of courage and should be commended. Check out the "find a therapist" option on `psychologytoday.com` to get started. It can be overwhelming to begin this process if you are already suffering, so enlist a friend to help if needed.

Install More Memory

Many people, myself included, take Selective Serotonin Reuptake Inhibitors (SSRIs) or similar medications that increase the amount of the "happy" chemicals circulating in your brain. These are often the

first line drugs used by physicians to treat depression and anxiety. In my experience, these give you extra resources to deal with the challenges life brings. They may not necessarily fix the problem, but they do make the machine run better - which is sometimes all that you need to start the repair work. If you do not have a primary care doctor, these services are available online. Cerebral is a popular choice.

Reboot In Safe Mode

This is an advanced topic, and should only be undertaken with medical supervision. You can obtain direct access to your core OS by use of psychedelics. There is so much exciting research coming out about the use of psychedelics to treat and, in some cases, completely cure treatment-resistant anxiety, depression, PTSD, and others. As of this writing, psilocybin is a Schedule 1 drug in the U.S. - the same category as heroin. However, starting in 2023 therapeutic psilocybin will be legal in the state of Oregon. The cost and availability to the average consumer remains to be seen. Ketamine is another popular agent, and can be obtained for mental health purposes with a doctor's prescription in some states. Mindbloom and WithPeak are popular online options. Savvy readers are probably thinking that they could obtain these substances on their own. I can guarantee that catching a felony drug charge will not be beneficial to your well being. These are potent substances and should not be taken without supervision.

Conclusion

This is truly the tip of the iceberg. There are many other options and strategies, and I encourage you to seek out professional help if you need it. We need every single hacker, weirdo, and deviant we can get right now to help make this world a better place. Take care, and be excellent to each other.

HACKER DILEMMAS

by aestetix

To remain a hacker in today's polarized world is increasingly difficult and leads to serious philosophical dilemmas. We are not talking about politics, but attitudes towards technology. To illustrate this, we will review a few of these dilemmas: old versus new, sharing of modified code, and ownership of networked systems.

In the "old versus new" debate, we see novelty battling nostalgia. Every new gadget that comes out offers - at least in theory - cool features with which techies want to play. But once the glow of newness dies away, we are left with a blunt question: what makes this device better than the old one? At a certain point, there is a law of diminishing returns. For example, while 4K video resolution is clearly an enhanced experience over 720p, does 8K offer the same improvement over 4K? And, conversely, how many times has a website (like reddit) put out a "new" design that destroyed usability?

But sometimes new *is* demonstrably better. Take newer software versions: while there are routine updates like security fixes, major updates - such as moving from single- to multi-core architecture - can offer exponential improvements. Just compare screenshots of Windows 1.0 to Windows 10: the difference between older and newer versions is simply staggering. Of course, we also get software like Node.js, which over time seems to have gotten worse and more bloated. In fact, a common complaint about modern software is the bloat that makes it run slowly on faster hardware, in contrast to retro software that often had to be tweaked in very creative ways to meet hardware limitations. So is new or old better? The answer is not so clear cut.

For our next dilemma, we turn to code sharing. With the advent of version control systems, like git, and websites to share projects (such as github) comes two developments: the ability and encouragement to share software that is "in progress," and the push to likewise share any changes we've made via pull request or repo forking.

When we talk with artists, we learn that sharing "works in progress" is very controversial, especially when we are used to only seeing a final product, like a book or a painting. Similarly, some open source developers will quash their git commit history when they put out a new version.

There's also the question of whether the art created is inspired by the artist, or inspired by external pressures that the artist feels once the "in progress" art is shared. Conversely, many argue that there is no such thing as a "finished" project, and when a code repository is transparent down to the level of individual code commits, it can create an inviting atmosphere, welcoming contributions from anyone in the world. One could even argue that such radical transparency helps sidestep potential biases of the original maintainer of the codebase.

In the case of changes to code, there's an additional issue of ownership. When we take some code and modify it, licensing notwithstanding, or if we make some big improvement to it or manage to port it to an otherwise unavailable computer system, do we have an obligation to share this contribution with others? This boils down to whether code sharing is a zero-sum game: that is, when we add something new into code that is local on our computer, does not sharing it somehow take something away from others who are using unmodified code on their own computers? One could argue that it does, because someone else wrote the initial code base that we modified. However, if we follow this reasoning to its logical conclusion, then if we fix a security hole in the code and do not share it, and someone else using the unmodified codebase gets hacked, we would be at fault. Although without the original code base, neither the security hole nor our fix would even exist.

This begs another question: if we choose not to share our code, what impact does this have on the community in general? Or, put another way, which has primacy of importance, our personal agency and privacy, or the good of the community? There is also a deep can of worms there regarding private property that is beyond our current scope, but it's important to acknowledge that it's there. So in the end, who really should "own" the code? There is no obvious answer.

And finally, we visit the age old debate of systems ownership, and the benefits therefrom. Let us take the idea of a networked system of computers, and look at it from different viewpoints. If we take the "my computer is my castle" approach, then there should be no ownership change for a computer, on or off the network - it belongs to us. The moment a packet has left the network cable and entered the memory or disk of the computer, it is owned by the destination IP, rather than the source IP. The software on our system is ours: we own it, and any interaction it has or makes with other computers on the network is determined by us. Likewise, if we have a hardware problem, we should be able to fix it on our own. This sentiment is the hallmark of the "right to repair" movement, and views the corporate nature of things like software activation and "take it to the Apple Store" with suspicion.

On the other hand, we could also view our computer as one member of a networked community of systems, with mutual responsibilities to each other. If our computer gets hacked by a virus, who is to say that that virus won't spread to other computers as well? In this approach, we have an obligation to keep our computers updated with the latest security patches, not just for our own safety, but for the good of the others as well. We can take this a step further and, assuming we sometimes have idle time on our systems, donate resources like CPU cycles to a good cause like SETI@home, protein folding, COVID-19 vaccine research, etc.

But with all of this there is a large downside. By allowing a third party to automatically access and send updates to our computers, we are also at risk from their mandates. Let's say Microsoft decides they do not want Windows users to be able to use Google Chrome - what's to stop them from using their automated updates permission to also uninstall Chrome and set a registry key preventing us from running it? Or worse, why not simply outsource the functionalities found in applications to some "as a service" website, where our computer becomes nothing but a dumb terminal without network access and approval to access the centralized system? A third time, we discover why this "choice" is a dilemma.

The nature of a dilemma is such that a given situation has multiple views on the "correct approach," none of which are "correct," and each, if taken to the logical extreme, become tyranny. When there is no good answer, we must revisit our own conception of first principles, and decide what for each of us is the best balance. A parting rule of thumb: when something is controversial, it means that there are no easy answers, and so when trying to pick a path, it is important to consider all viewpoints.

An Introduction Algorithm to Decoding an Enigma

by Diana K

Over the weekend, I watched the movie *The Imitation Game* about Alan Turing and the computer built to decode the Enigma. In the 80s, while studying AI at UW-Parkside I was able to meet a friend of Alan Turing's who oversaw the Turing Institute. In addition to studying AI, I was interested in encryption as well and started understanding a Bazeries Cylinder like one used in *The Da Vinci Code*.

The Enigma is like a Bazeries Cylinder except that it has a plug board which provides an additional transition. So, instead of a three-state transition as in a Bazeries Cylinder, there is a four-state transition provided by the plug board. To give an Enigma example, consider the following morning message (assume it is written in German like in WW II):

```
The Weather for May 21st, 2022 is
8 degrees C and Sunny.
```

In reading the message, it seems pretty simple, and one might have the ability to use a brute force algorithm to break about 51 million combinations on a computer that ran at a processor speed of about 1 kHZ. Actual, the solution could not be found within the timeline of 18 hours from the 6 am broadcast.

What was a faster way? The faster way was found by talking with others who intercepted the encrypted messages and could tell that a specific person on the other side was typing the message. By realizing the same person was typing a daily weather report at 6 am on the other side, one could have a set to compare. For example, the person would ably follow the same message format:

```
The Weather for May 23rd, 2022 is
14 degrees C and Sunny.
```

Then, taking the next step of comparing the actual message with the encrypted message, part of the state transition could be obtained. The weather report messages were deciphered by those who were able to use alternative methods to deliver the messages, but not the Enigma encoding and plug board.

At a listening center, a group would have the decoded message:

```
The Weather for May 21st, 2022 is
8 degrees C and Sunny.
```

And the encrypted message:

```
"Yop%Raebtep@Ayv!9v{WOSD%hf@
➥g$sfuadq&q@qkg*znght,"
```

What does this mean?

The thing to remember about the Enigma machine is that it had four-state transitions. So, if someone typed "T," the second state transition could be "Z." When the letter "Z" is submitted to the plugboard, the next letter could be "B." The letter "B" is what would be sent via radio telegraph.

When the receiver would type the letter "B" on a similar Enigma machine, the internal transition would come out to "Z" via the one of the three wheels of the Bazeries Cylinder and then the "Z," Wheel 1 would come out to "B," Wheel 2, then transition to "A," Wheel 3, and finally transition "E" on the plugboard. So the state transition is T-Z-B-A-E-T.

The problem is coded for searching for a substring with T-?-??-???-????-T. Also, as other four-state substrings as added to compare and solve the algorithm, the "?" and "??" can be determined. However, it took a few substrings to use as a seed.

What is the algorithm? The algorithm starts with a state of either 1-4 like in Turing's state machine. Next, a substring is selected as "T-?-??-???-????-T." A method to solve the problem is to work backwards. So, what setting is needed on the plugboard to transition X (internal coded character) to "T?" The process compares various substrings in State 4, and the first backward solution is "T-?-??-???-B-T."

After the plugboard is solved, the next state is State 3 on the third wheel. The original search substring of "T-?-??-???-????-T" is now changed to "T-?-??-???-B-T." In a way, it is like a Keno game. In a Keno, after determining one set of numbers in a betting string, the process becomes cooperative to finding other solutions in an easier manner.

In State 3, when a substring message is found beginning with "B," a combination of trials is set to determine what possible settings from the plugboard to wheels 3, 2, and 1 could lead to a transition going backwards from "T-B-wheel 3 setting - wheel 2 setting - wheel 1 setting - T" from a set of sample words in the message.

The process is repeated backwards until the plugboard and wheels 1-3 are solved for State 1. Then the same method is used in State 2. When State 2 is solved, the same method is used in State 3. Which means the plugboard and three-wheel settings are determined. The solution would look something like this:

```
Wheel 1: A- E
Wheel 2: E - Z
Wheel 3: Z - (
Plugboard: (- A
```

If one were to consider that there were 32

setting for three wheels and the plugboard, the combination is (2^5) ^4 or 2 ^ 20 combinations. However, by knowing two of the transitions, the combinations needed to be solved are: (2^5) ^2 or 2^10 combinations, a speed-up of 2^10, which allows a solution within an 18-hour time limit.

In Pascal like pseudocode, the code would look like this:

```
1. Program breakEnigma;
2. // © 2022 Diana K
3. Var
4. subCrypts: array[1..3,1..5] of string = (('T-?-??-???--X-T'),('A-?-
➥??-???-P-A'), ('C-?-??-???-Z-C'),('Q-?-??-???-B-Q'),('G-?-??-???-Q-G'),(
➥<second set for state 2>), (<third set for state 3>);
5. msg: string;
6. i, j, k:integer;
7. settings: array[0..3] of integer = (0,0,0,0);
8. maxWheel: array[0..3] = (32, 32, 32, 32 );
9. state:integer;
10. completed:Boolean;
11. function decrypt1(cryptMsg): Boolean;
12. var
13. I, j, k:integer;
14. Tmp: string;
15. Solved : Boolean;
16. Begin
17. Tmp:='';
18. Solved := true;
19. For i:= 1 to length(cryptMsg)
20. Do begin
21. J:=(I mod 4);
22. // plugboard
23. Tmp[1]:=chr(((ord(cryptMsg[i])+setting[j]) mod maxWheel[j]);
24. // wheel 3
25. Tmp[2]:=chr(((ord(tmp[1])+setting[(j+1) mod 4]) mod maxWheel[(j+1)
➥mod 4]);
26. // wheel 2
27. Tmp[3]:=chr(((ord(tmp[2])+setting[(j+2) mod 4]) mod maxWheel[(j+2)
➥mod 4]);
28. // wheel 1
29. Tmp[4]:=chr(((ord(tmp[4])+setting[(j+3) mod 4]) mod maxWheel[(j+3)
➥mod 4]);
30. Solved:=solved and (cryptMsg[i] = tmp[4]);
31. End;
32. Decrypt1:= solved;
33. End;
34. Procedure solvePartialSubCrypt(state:integer; I:integer;
➥settings:integer; subCrypts: string[][]);
35. Var
36. I, j, k:integer;
37. Begin
38. // convert pseudocode lit to pascal like pseudocode
39. // a challenge to the reader, easy to do
40. End;
41. begin
42. writeln('Program Break Enigma');
43. write('Enter Encrypted Message? ');
44. readln(msg);
45. writeln;
46. writeln('…Starting Solving');
47. for state:=1 to 4
48. do begin
```

```
49. for i:=4 downto 1
50. do solvePartialSubCrypt(state, I, settings, subCrypts);
51. end;
52. // check work
53. Completed:=true;
54. For state:=1 to 3
55. Do for j:=1 to 5
56. Do competed:=completed and decrypt1(subCrypts[state,j]);
57. // show result
58. If not completed
59. Then writeln('A Solution was not found')
60. Else writeln('A Solution was found');
61. Writeln;
62. Writeln('Settings: \tPlugboard \tWheel 3 \tWheel 2 \tWheel1');
63. Writeln('\t'+settings[0]+'\t'+settings[1]+'\t\+settings[2]+'\
➥t\+settings[3]);
64. Writeln
65. Writeln('…Program Completed');
66. End.
```

What is interesting about the Enigma is that even today with a laptop computer, it takes about one hour to break an Enigma code - faster than 18 hours, yet still long enough for a message to become invalid if a decision is made an hour later after decoding.

The primary advantage of encryption is not the method itself; the primary advantage of encryption is how long does it take an opponent to read your message, and can your opponent read your message in time, while the message time is still valid?

Is It Time to Change Our Approach to Security?

by Cr0wTom

If you try to remember how everyday life was in 1984 (the year *2600* was founded), most of you will not remember at all, with some of you not even born at the time. This was when the "digital" space was kicking off, and a new generation of hackers started appearing. People with passion about technology, and creating and destroying things. But from this small collective, it started becoming a whole industry, until we reached today and an era where we see one critical RCE 0day after the other. But in order to see this amount of 0days, we need technological advancements and wide adoption of them from users. Which is the reality of today. Despite our expectations for flying cars and ovens that will take raw materials as input to output ready-made dishes, our technological leaps are enormous, and you don't need me to prove it to you.

Just look at your pocket, your garage, your TV, or even your toothbrush.

Our life is getting more and more connected. With the excuse of "efficiency" and "practicality," companies got (almost) all our devices connected to the Internet. And this is not a bad thing, but "with great power comes great responsibility." It is one of the biggest clichés ever, and it applies perfectly in this case. Companies want us to use their connected products and services. They need us to do it and they will do everything for it. Unfortunately, most of the time important aspects of the product development cycle will get bypassed, with one of those aspects being safety.

Safety Critical Devices and the Path to a Better Future

You might not think about it that way, but what will happen if someone hacks and disables your fire alarm? What about your fancy Roomba, which happens to mop your whole apartment? Your car, which you expect to act "smart" and "assist" you with its ADAS (Advanced Driver-Assistance System)?

You guessed it right. If some of these (or thousands of other) devices are developed with weak security, or even in cases where a product gets rushed into market with the mindset that it will be finished and polished at a later stage (*yes* Elon, I am looking mainly at you), then the impact is not only on the security side of things, but also on the safety,

with possibly devastating results.

Should this have been considered when evaluating security findings? Should it potentially increase the severity and the impact of those findings?

Our answer is not clear. It comes mainly from the automotive sector, where safety can be the most impactful characteristic with connected and autonomous vehicles already in the wild. But what we are sure of is that a reevaluation of the scoring systems has to be performed.

Different versions of CVSS (Common Vulnerability Scoring System) as an example, are released and embraced by security professionals and security-oriented product teams.

But is that enough?

Case Study

Unfortunately, I cannot talk about specifics. But I will give you an example of an OEM in the automotive industry where I was called to perform a complete security assessment on their product. Following standard testing methodology targeting the testing unit, I found several security "issues" that an unauthenticated user could trigger to perform physical actions in the vehicle (e.g. gas, brakes, etc.). Those findings were applicable only with physical access to the vehicle, which meant that an attacker had to physically access it to perform the attack, but after the initial foothold, all the actions could be performed remotely.

On this assessment though, we were "forced" to use the beloved CVSS scoring, which did not reflect a really important aspect: the physical safety of the driver and passengers. As a researcher, I can accept that a rating and a standard have to be used in order for all the parties to have a common understanding of the severity of the issue. But big corporations use these ratings and, depending on the policies, they reflect it on the final decision of "if" and "when" they will mitigate this finding.

Back to the actual finding though, the OEM took the resulting CVSS rating and chose to not mitigate the issue in the end, regardless of the safety implications....

As a researcher, my ultimate goal is to make the world a safer place. I tried to explain in detail how this finding can be used in an exploit chain, and how all the other interfaces that are connected to this functionality can be compromised and result in devastating outcomes. But security ratings have their place and huge corps do not (and will not) change their policies overnight.

Should There Be a Shift?

How should I feel now? Is it my problem if the brakes engage when the car is running at 120 kilometers an hour? Is it my problem if the assisted driving fails completely at the same speeds?

Yes and no, and that's why I am here writing this article. We need to start thinking about security in a different way. We need to start approaching exploit chains with safety in mind. Data, privacy, integrity, exploitability and everything is good, but we have to make sure that people will not die out of outdated practices, beliefs, policies, and cut corners (now I am looking at you Boeing).

Let's make the world a happier and safer place. There is still a chance.

Disclaimer: The finding got fixed, but we are sure (and we know) of many occasions in which companies act irresponsibly regarding critical safety components. Many times we find ourselves having to defend our findings in cases where we should not have to. Automotive and safety critical industries are new to the connectivity game and some mistakes will be made, and that's why we, as professionals, should be here to help them create better and safer products.

Will You Let Your Car Drive Itself?

By E.V. Rhodes

"Wanna see something weird?" is not a question I usually ask passengers when I'm driving, but in February 2022, as we headed north for a ski weekend, I explained to my two companions how I'd previously noted some odd, even alarming, behavior when using the cruise control feature on my new Tesla Model Y, and I asked, did they want to see if it would do it again?

In my previous experiences, the cruise control had properly maintained the car's speed for long periods of driving. It also accurately kept a set distance back from any vehicle ahead. But several times it had suddenly and dramatically slowed. I could not tell if it had detected a threat, for it gave no reason for slamming on the brakes. After this happened several times, I simply stopped using the cruise control feature.

This is not Tesla's much-touted "Full Self-Driving" software (at the time a $10,000 upgrade which was an easy "no thanks"), but simply their standard "Traffic-Aware Cruise Control" which they say "is designed to slow down Model Y as needed to maintain a selected time-based distance from the vehicle in front, up to the set speed... primarily intended for driving on dry, straight roads, such as highways." I explained to my passengers that I wanted their consent before trying it again, as well as their observations and insights should anything happen. With their agreement, I engaged the cruise control, set the speed limit, and removed my foot from the accelerator. The day was sunny and clear, the highway traffic was light, and the car continued carrying us towards the distant mountains. I remained in the right hand lane, alert and driving as usual.

But not 20 minutes later, it happened again!

I'm not someone who resists technological progress. Years ago, I built a ZX-81 computer kit and used it to control a simple robot arm. In college, I worked at a Fortune 500 company writing "expert systems" software to optimize manufacturing processes, and later I helped to develop an autonomous robot which could locate and navigate to its recharging station, and stay "alive" for weeks at a time. So when it comes to software for self-driving cars, I appreciate the challenges, and have great respect for the programmers and the results they've demonstrated.

In 2014, Tesla began offering limited self-driving capability on some of their vehicles. With frequent, incremental software updates, development proceeded rapidly. By January 2016, Tesla's CEO stated that the their autonomous driving system was "probably better" than most human drivers. Of course, "probably" is difficult to quantify. The real world presents autonomous systems with incredible complexity; ever changing weather, illumination, and surroundings, not to mention the unpredictable behaviors of people, animals, and other vehicles. Self-driving cars must reliably and accurately generalize from highly variable data, and be prepared for an enormous number of situations which might occur incredibly rarely, if ever. The fact that self-driving cars can travel on public roads at all represents an astounding technical achievement. But they are only safe until they are not.

After explaining my previous experiences with the cruise control, my companions agreed to trying it, and to watch closely should anything happen. After engaging, we drove for 20 or 30 minutes without incident - until my car suddenly slammed on its brakes and decelerated rapidly! The driver behind us swerved to avoid a collision and sounded their horn. Why had we slowed? There were no obstacles or vehicles ahead of us. The road was straight and clear!

I immediately stepped on the accelerator, disengaging the cruise control and resuming our speed. End of experiment! One of my passengers thought a section of the road may have been resurfaced, and perhaps looked slightly darker than the rest. Did that register as a threat to the software? (Unfortunately I did not capture a dash cam recording of the event.)

I have never enjoyed being an unpaid software beta tester, and I'm even more reluctant to be a guinea pig where problems could result in injury or death. I have not used the cruise control since that day, but I recently learned that our alarming event was not unique. Many other Tesla cruise control users have also experienced sudden, inexplicable braking. On May 4, 2022, the U.S. National Highway Traffic Safety Administration (NHTSA) issued a letter to Tesla stating "This office has received (758) seven hundred and fifty-eight reports of unexpected brake activation in certain (MY) 2021-2022 Model 3 and Y vehicles." With that

many people concerned enough to actually file a report with a government agency, how many others (like myself) had not reported their experiences? Thousands more, I suspect.

Now don't get me wrong. The Tesla Model Y is an excellent car with great performance, comfort, and tons of amazing features. The very same NHTSA gives it five out of five stars for overall safety. Rising gas prices make owning an electric car increasingly affordable, and if you have solar panels you can easily produce all the fossil-free energy it needs right at home, making them good for you, your wallet, and the planet. (End of EV plug.)

But, if adding machine intelligence to a fairly standard feature like cruise control (first offered on a Chrysler production car in 1958) presents such mysterious and life-threatening difficulties, what about the much greater challenges facing fully self-driving cars? They already have been involved in many reported injuries and deaths with everything from drivers stupidly defying important operating instructions, to innocent individuals tragically hit on roadsides. Self-driving vehicles pose risks not only to the drivers who knowingly accept them, but to potentially anyone in their presence: other drivers, passengers, pedestrians, motorcycle and bicycle riders, highway workers, police and emergency responders - in short, almost everyone.

It surprised me to learn that the USA currently has no federal laws governing self-driving cars. In 2016, the NHTSA did publish the "Federal Automated Vehicles Policy," a set of guidelines which they say provides "a proactive approach to providing safety assurance and facilitating innovation." This allows developers to act quickly and develop solutions rapidly with fewer legal obstacles, however it can also be seen as placing profits before people, since nothing legally requires them to hold my safety as their highest concern. How can we know in an objective, fact-based way, when self-driving vehicles are actually able to increase the overall safety of our roadways? Perhaps we must simply accept that automobiles are dangerous, and that some amount of injury and death must be expected. We already tolerate that with human drivers, why not machines as well?

Well, because the goal of self-driving vehicles is to make our roads safer, not less safe. Determining if and when they actually are safer will require an army of highly trained, detail oriented investigators, drilling deep into vast amounts of real-world self-driving vehicle data, verifying their findings, and standing behind their conclusions.

Interestingly, we have just such an army: the worldwide auto insurance industry, valued at over US $700 billion in 2019. Insurance actuaries assess the risks existing at the dynamic intersection of human behavior, government regulation, and automotive technology. The field is overseen by government agencies which monitor insurance rates, coverage, and incentives. At present (in California anyway, your state or country may vary), pricing discounts are offered for good driving, good student grades, being away at school, and having multiple vehicles on the same policy.

Insurers currently do not offer any financial incentive for using self-driving vehicles. Such adjustments can only come after a long period of rigorous statistical study that objectively proved such systems actually helped reduce accidents and save lives. Those studies would be used to support the creation of legislation authorizing insurance companies to offer such discounts. This presents a chicken-or-egg type safety conundrum: there can be no incentives for self-driving cars without extensive real-world studies, and there can be no extensive real-world studies without putting lots of self-driving cars on the roads before they are definitively proven safe.

For an inexact comparison, look at the history of seat belts which, starting in the 1930s, were clearly shown to save lives, but which did not become mandatory equipment in U.S. cars until 1966. Even then, their actual use was not enforced until much later; New York passed the first "click it or ticket" law in 1984, and all other states followed suit by 1995 - except for New Hampshire which, at present, only requires seat belt use by persons under 18 years of age. (As it says on their license plates: "Live Free or Die.")

A long road lies ahead for widespread acceptance of self-driving cars. Until then, the path will be paved with varying degrees of danger and uncertainty. Should major insurance companies someday offer me cash discounts for using autonomous systems, I will take that as a solid indicator that self-driving cars have finally achieved true safety and reliability improvements.

Until that time, I'm keeping my cruise control disengaged, and my foot on the pedals.

Special thanks to Alex K for insights into how the insurance industry contends with new developments.

The Hacker Perspective

by XCM

Up until the age of ten, my curiosity would typically translate to destructive behavior towards any mechanical object or small electrical appliance I could find. Of course, I would only experiment on things I felt nobody cared about. My judgment over time turned out to be accurate within an acceptable degree.

Sometimes I even managed to put things back together. When this occurred, they would mostly work again.

And then one day, out of the blue, it happened. I was given a computer.

I don't remember how I felt initially.

Of course, the first thing I did was to press on the two metal levers on the side of the chassis and slide the metal cover open.

I had no idea what I was looking at, but it felt great. It felt like an important milestone.

After a few moments considering whether I should proceed dismantling the thing, I decided against it. At least for the moment.

I put the cover back on, pinched a finger in the process, and switched the power button on. You know, a real, mechanical switch.

Of course, there was no need to re-apply power beforehand as I had not bothered with disconnecting the mains before opening the machine.

Now imagine "Also sprach Zarathustra" by Richard Strauss. Got it? Good. The emotion conveyed by those notes describes quite accurately what I felt when the monitor slowly started throwing loads of text at me.

I could see things. Lots of writing. Arcane messages. It felt as if the being was trying to communicate something to me but I was too inexperienced to understand.

It did not help that my knowledge of the English language was zero at the time. Besides, had I been able to read that text, the whole experience would have taken a less mystical flavor.

When the creature finished saying what it had to say, it looked like it stopped, waiting for something from me.

And so my exhilarating journey through MS-DOS began.

I remember the sales representative who sold us the computer that morning handing me a plastic box with a bunch of what he called "floppy disks" inside.

Looking me in the eyes sternly, he declared: "Here you have one hundred games. Now there is no need for you to go elsewhere and risk getting a virus."

I opened my hands, solemnly receiving that mysterious box and I could not help but thinking: "Wait a minute. Is there an 'elsewhere?' Is there a place where I can get things to put in my computer? I absolutely must find this place."

This is how my 30 year quest for computer knowledge started.

Access to information was very limited at the time, especially technical. The Internet was not mainstream yet and public libraries did not have much material on computers.

This left me with commercial bookstores and a meager budget.

After lengthy consideration between a bunch of video game magazines, sweets, and a book, I finally decided on a book on programming

I read the whole thing from cover to cover. After two days, I put the book down, typed "EDIT" at the command prompt, and started hammering away at the keyboard.

Of course, I also quickly went through the disks given to me by the generous computer sales guy. Alas, soon I discovered with the utmost disappointment what foreign words such as "shareware" meant. All of the games on those disks belonged to that category.

I then quickly discovered the joys of decompressing games with ARJ from floppy disks exchanged at school - some of which had the tendency of playing the dreaded sound of the damaged sector at around 90 percent of an eight-disk decompression process.

I believe this is how my informal

exposure to the English language began. I learned to guess the meaning of random words such as “missing,” “failure,” “bad,” or similarly ominous terms.

An important milestone in my journey was when I decided to have a proper look at a couple of curious files I had noticed some time before: CONFIG.SYS and AUTOEXEC.BAT.

There were a lot of sexy looking instructions in those lines with some intriguing values after each of them.

I spent some time messing with the numbers, thus enriching my vocabulary with new words that the computer started to uncooperatively bark at me - things like “abort,” “incorrect,” or “invalid.”

Then one day, things started falling into place and I realized that I could reduce the computer boot time by disabling only the lines that did not completely break the boot process.

That led to a sizable reduction in time for a grand total of around five seconds.

I am sure that in the following months I just about got the time back that I invested in getting to that “optimization” to begin with.

After this major accomplishment, I discovered that by altering those files, I could also optimize some games and make things go smoother.

Once I ran out of options for software tweaking, I started looking at possibilities for hardware upgrade. This was potentially a sore point as I definitely did not have the budget for expensive electronics.

All I could manage was a one megabyte bank of memory miraculously salvaged while rummaging through a pile of trash at a car boot sale. Things looked brighter for a bit, but then it dawned on me that more RAM does not mean faster games.

It was then, with great excitement, that I learned one of the most promising words I had come across in a while: “overclocking” - the arcane art of squeezing extra CPU cycles by shorting some random pins on the motherboard.

Again, this was a totally trial and error process as there was no tutorial (and no Internet, to be precise).

However, after the occasional self-shutdown or freeze, I reached an acceptable balance by leaving the case permanently open with a small desk fan constantly blowing air at the dissipator.

So what are the most important lessons I have learned in all these years?

One aspect that I miss from my early computing experience is how intimate the relationship between human and machine was. Well, at least for me.

Computers had mechanical switches. Things made noise - they took time to “heat up,” as a friend of mine innocently revealed to me.

Now the whole approach is different. My MacBook is never really powered off. There is no proper switch. It’s silent and its inner workings are mostly hidden behind a pretty user interface.

Even modern Linux distros feel somehow more abstracted, colder, distant.

One useful fact that I learned is related to my memory of when I bought my first book about coding, which I wrote about earlier.

Looking back, that was the most focussed and productive learning effort in my whole life. Surely, it was all new and exciting and my brain was nearly 30 years younger, making things easier. But there is a specific element that made this possible: information scarcity.

While this might be counterintuitive at first, I am convinced that being in my room with that book, and that book only with no distractions, allowed me to focus 100 percent on my objective.

Imagine doing this today: you can get an online subscription to access thousands of digital books. The Internet overflows with information on any topic you could desire. And then, of course, we have smartphones to steal as many brain cycles as possible from us.

I don’t know about you, but I still remember as a kid sitting on the toilet and reading the shampoo ingredients list, rather than a smartphone. OK, when I ran out of labels to read, I started taking books with me to the toilet, but that gives you the idea.

This cacophony of data, at least in my experience, results in an overabundance of stimuli that makes the process of focusing on a topic extremely difficult. It creates what I believe is called “information overload,” which for people who are thirsty for knowledge is a very insidious threat indeed.

And it can get addictive, too - up to the point where our brains cannot cope with this constant influx of data and we experience a sense of being overwhelmed

that can manifest itself in various areas of our lives in the form of anxiety.

I know this concept is possibly complex to grasp by someone who is starting this fantastic journey today, but I believe there is a valuable suggestion here: resist the temptation to hoard more information than you can absorb. It will not make you more knowledgeable. It will just highlight your limitations as a human being.

Some people are OK with that. I, however, reacted differently. I experienced a dreadful fear of missing out. Anything that I could not read was information that I would forever be ignorant about.

Also, this constant switching between books, articles, videos, and the like further reduced my attention span, as our brains are not made for multitasking, really.

And before anyone says: "women can multitask." No. Women cannot multitask any better than us men can. Women just get shit done and do not complain.

Also, thinking about that period of my early life, I would define it as "boring" under today's standards. Little access to information, limited sacrificial gear to experiment on, and a sense of loneliness as none of my friends at the time spent their afternoons in the company of screwdrivers, pliers, and an emergency one kilogram hammer.

Over time, I was constantly coming up with lots of questions and little answers. All of these questions kept cramming in my little head with no outlet to direct my desire of knowledge to.

I am convinced, however, that being bored was a great catalyst to develop my imagination and aide experimentation. Being bored forces you to find something to do with what you have - to repurpose things in unexpected ways to pass the time. It forces you to become a hacker.

These things do not occur easily nowadays and similar opportunities are lost, due to the multiple distractions we are constantly surrounded by.

Another important lesson I learned over time is that whereas there might be shortcuts in life, they rarely bring the most favorable outcome. Most of the time, the hard way is the best way. Cliché as this might be, I believe it really is a valid point to remember in life.

One additional advantage of those initial experiences is that I feel a lot more confident about learning. I see so many people, at different stages of their lives, who dread having to learn new things. And this is a real shame as, in a way, knowledge still is power. The moment we stop learning, we really become at risk. Not only professionally, but we also lose so much potential as human beings.

I always say to people who are daunted by learning that acquiring information is easy. I confidently tell them that they can learn anything, given the right dedication.

I am often met with a look of disbelief. They do not appreciate the simple fact that we are all born ignorant and inept. Those people all have one thing in common: they were never given the opportunity of a safe environment where failure was acceptable. They never broke things to see how they worked. Therefore, they were never in a position where they could fix what they had broken.

In few words, they lack self confidence.

This is what hacking is about. Constant excursions outside of our comfort zone because of actions we willingly took, most of the times completely oblivious of the consequences.

And every time we learn from our actions, every time we fix what we ourselves have broken, we feel we have reentered our comfort zone.

What we don't realize, at times, is that what really happened is that our comfort zone has just expanded. This will only happen when we push the boundaries hard and often enough.

I am so glad that I was given the chance to go through this process. It is one of the most fundamental steps in my formation and I am striving to offer the same opportunity to my children.

I really hope it will be valuable for them as it was for me.

XCM can be found consulting for various organizations on designing and implementing certain cyber security solutions. In his free time, he loves reading classics and challenging his kids to think critically about the reality they are exposed to. When the youngsters challenge his beliefs, he realizes he must be doing something right in life.

A Ripple Story

by Cryptopian

I worked at an unnamed crypto company in San Francisco and got a close-up view of this controversial industry.

On second thought, let's name it. It's Ripple, the "enterprise" crypto blockchain.

Ripple was a funny place to work. Most startups have a consistent cast of characters, so that one startup's staff is almost interchangeable with another's. Not Ripple.

Back in the day, Ripple was hiring oddballs, in bulk. The theory went something like this. Crypto is a new industry, created by the collision of very different elements: cypherpunks and banking, independent developers and enterprise software, etc. So our people should reflect this.

For our purposes here, let's focus on developers. There were people who were super into Bitcoin, who often combined a consultant's mentality - "whatever gets the job done" - with a libertarian ethos (note: that's different today than what it was). There were traditional software developers, with pedigrees from elite institutions and blue chip work histories. There were people who wanted to break into the industry - and found their way in. And finally, there were journeymen, who'd been in the industry shoveling away for years, hopping from one job to another.

There were also programmers at different levels of mission-critical. There were the protocol developers, who were C++ (the language) rock stars, and frankly, bored. They were all extremely skilled, so skilled in fact that they ran out of things to do: the blockchain worked, they had optimized it, and more ambitious goals were walled off by management. You know those algorithms that Google tests you on? They had invented some of those. Then there were the front end developers, who became more standardized over time, but were a real grab bag back then (and didn't have that depth of knowledge).

Over time, the traditional developers edged everyone else out, and the other groups either found a space on the margins, or quit, or were pushed out. One of the groups that experienced the most tension was the Bitcoin people, who seemed to be itching at this question almost daily: If you really believe in a decentralized crypto future, what are you doing at a fully establishment, centralized one? Those were some of the first people to go.

In the beginning, that wasn't a problem, because Ripple, theoretically, was everything and anything you wanted it to be. It really depends on how far back you go, because its history changed a lot, and is a trip in itself.

It started off - the software equivalent of the Cambrian Age, so far back even the "early people" barely remembered it - as Opencoin. This bumped along for a little while, maybe of interest to people looking to get in early on something that hadn't yet taken off and become "too expensive" like Bitcoin, then in the tens of dollars (ha).

Ripple, in the words of recruiters - which is how most hires found out about it - was crypto which was going to be the future (this was long before it saturated the media-scape, before Ethereum even existed). It was fintech. It was going to help the unbanked - from a comms perspective, the hook into the disruption and revolution perspective that was so popular at the time.

As time went on, Ripple evolved, as a company, from "kind of a crypto play (emoji shrug)" to "enterprise blockchain." You might say, "Wait - I thought they were a cryptocurrency?" And not only would you be right, you would have hit on a fundamental tension that was never really resolved. Ripple *was* a cryptocurrency company, but it was also supposed to be selling banking software to enterprise companies, which sometimes led to the funny sight of Ripple talking about its own product in the third person, as though it was an infrastructure provider when its own bag was the "infrastructure."

Ripple did have market fit, in a way. But it wasn't a market Ripple really wanted or truly loved.

Ripple, for whatever reason, had caught on in a big way in Asia. What happened was that brokers would buy up large amounts of XRP, then resell it to investors. They promised the investors they sold to that, even after a huge markup, the could become rich. As it happens, they were right: Ripple's price was so much lower back then that this strategy was ultimately

vindicated. If you crunch the numbers, then yes, you could have bought XRP from these brokers at five times cost, and still made two to ten times (or more) on your investment.

a famous zinger about this

At the time though, that seemed almost unimaginable; we would laugh about Ripple passing one dollar (it eventually, briefly, passed $2.50). The wholesale sellers were a third party we never talked about that much. Sometimes one of them would sweep in and do a tour (including the founder of a very famous project, now). We also knew the users they sold to got hacked at a horrendous rate, though to be fair that wasn't due to security flaws in the protocol.

If this sounds like indifference, it wasn't personal. The core problem was: their speculative cottage industry could never float Ripple at a valuation the venture capitalists could accept, so the search was on to find something that could. The idea that got the most mileage then was that Ripple would replace SWIFT, the world's international banking rails, which... yeah.

So because Ripple didn't have a real business, and didn't have a product market fit (that it wanted or could love), it was totally dependent on personal power and politics, on a knife edge of "value that could be delivered" as opposed to "value being delivered now" (because there was nothing concrete that any desirable customers wanted from it). Ripple's mission then was about finding something that would combine fintech and cryptocurrency into something even better; the cryptocurrency was the Trojan Horse that was supposed to get Bank of America to buy XRP like bonds. But why would they, or their peers, do this? They didn't need us; in fact they thought we should be paying them for the validation their logos would give our brand.

So Ripple never found any real enterprise banking customers, and the only paying customers were the speculative XRP paying kind, who never really had a full place in the overall vision.

There was a small community of people at the company who did care about cryptocurrency, who never really fit in comfortably. But of course, since Ripple recruited a lot of people with the cryptocurrency promise, it had to have some kind of story for them. You could get a sense of this in the very strange internal XRP buying process, which you had to ask about, which wasn't volunteered, and which wasn't especially popular among employees. Of course, that was par for the course of the time; we'd heard stories about employees at one crypto company who'd accepted payment in Bitcoin when it was in the mid hundreds, then got whiplash when Bitcoin sank to the 50s, so much so that the policy was discontinued. (At the time I'm writing this, Bitcoin is about 30k.)

So Ripple muddled along, as the industry evolved and spread its influence into the culture at large. And then Ethereum came on the scene.

Ethereum was vaguely talked about in Slack, which was a newfangled thing at the time. I remember meaning to look it up, forgetting about it (that's how infrequently it was discussed), and then remembering "oh yeah - I meant to buy that" when I saw a price quote for it on an early exchange, which has probably disappeared by now. It had reached $10, at which point I thought: I missed that boat - I'll catch the next one.

But Ethereum went on to become a legend. XRP is still hanging on in the top ten of coins. Meanwhile, the cryptocurrency industry keeps evolving. You never know where tech is headed, or where it will end up; cryptocurrency was the most niche of niche things back then, and now it's unavoidable. Computers themselves have gone from toy to center of the economy in my lifetime. What will happen after that? Technologists will still be telling their stories a hundred years from now. This one was mine.

I hope you learned something from it - and thank you for your time.

Hackers - What is Our Mission Statement?

by ScreamingYellowFish

Recently I have been thinking quite a lot about what appears to be an ever growing and widening chasm both within the readership and the hacker community writ large over several concerns that cast a pall over in an ominous and foreboding way:

- Have we lost our mission of staying on track as a font of technical information?
- Have we become too political, or indeed even too polarized or partisan?

What troubles me more, however, is the notion that these two vexing questions are somehow antithetical, or worse, that discussion of this topic has in and of itself become too toxic to approach. That, to my mind, seems to have already had the corrosive effects that our detractors from our past would never have imagined could do more damage than their worst machinations.

This alone would warrant its own article and, in fact, I have already written and submitted one to this fine publication. Instead, I thought it might be instructive to take a step back and shine some light on a more recent turn of events that sadly ties the two together in a more insidious way that clearly highlights the numerous problems at hand, and then some of my own thoughts and questions about who we are as a community, and what we can do to course correct while we still have the opportunity to do so.

In our professional lives, whether we are employees or contractors, self-employed or part of a partnership, at some point we have all come across and have signed myriads of documents. Maybe you scrutinized them carefully with full attorney review. Maybe you blindly signed them with nary a thought. Example of these might be non-disclosures (NDAs), non-competes, invention assignments, previous employment disclosures, etc. Upon leaving employment, you may have to sign termination agreements or separation agreements. In disputes, you may even have to sign arbitration agreements, settlement agreements, and the like.

Let's now imagine a world where you create a nifty algorithm or app or whatnot. Maybe its entirely your own, or maybe you borrowed from open source, or some derivative idea, or collaboration. Maybe it's all entirely original. Maybe you did a prior art or copyright check. Maybe you or your employer got a little lazy. Here's where things start to get murky and worlds collide.

Our imagined place of employment occurred in the nutmeg state of Connecticut. You are a contractor, and you run your own corporation and bill corp-to-corp. Congratulations, you figure you are protected from harm under a corporate umbrella and, should anything go awry, you can shut down your company and start again. Maybe that might be true if it's a civil matter... but what if your work was based off of stolen intellectual property (IP) from someone else? You may be wandering into criminal territory, particularly if it happens to be federal or, say, military. What if you didn't know? Does that matter? What if it was a client of your client that did this, like a cousin once removed? Does that change the nature of crime?

Let's change the scenario. You are an employee instead. Are you protected now? Not necessarily. Assuming you are a bit-head who just wants to write cool apps and you got caught in the middle, does that mean you are off the hook if you were ignorant of the circumstances?

Let's go to the next level. You found out and reported this. Supposed you are ignored. As a contractor, things truly get murky at this point. Are you ethically required to walk away? Can you walk away? What if there is a severe financial penalty for quitting early or for not finishing the project?

As an employee, you dutifully report your findings to you manager. Nothing happens. You might even be told to leave it be. You then kick it up to HR. Again, nothing. What do you do now? Now let's suppose that they try to "incentivize" you to leave by making it a hostile place to work. Eventually you are "let go." Can you do anything? Connecticut is an at-will state, so not really. You could pursue the hostile workplace issue, but that just paints a target on your back. You could pursue Connecticut's whistleblower protection act, which makes termination illegal. Even under those circumstances, if you win, are you still protected from criminal liability?

All we wanted was just to write "kool code." All we got for our trouble was legalese in places where the sun don't shine. Worse, this is where what should be a streamlined process across the country becomes a nightmare game of whack-a-mole. Everything I laid out here is all state law context dependent. We lack any federally mandated guidelines that define a clear set of coherent rules and policies by which we can figure out how to navigate this mess.

It gets worse. I pointed out in my last article the dangers of the new Texas abortion law, where Texas lawmakers successfully managed to ban abortion in the state of Texas by end running the Constitution. Here's how they did it: The new law allows any private citizen to sue Texas abortion providers who violate the law, as well as anyone who "aids or abets" a woman getting the procedure.

Imagine now a scheme where any state can pass laws allowing a vigilante citizen or group of disgruntled citizens or corporations to come after anyone who may be in violation knowingly or otherwise of patent or copyright law, be they contractor or employee of any state or territory in the United States. You can run, but you cannot hide.

With the proliferation of software products and applications to countries around the globe,

this has become an even bigger issue. Think this doesn't affect you? Let's take another look at your nifty app. Let's say right before the war in Ukraine, you had arranged with a major distributor in the Russian Federation to sell and disseminate your application. After the war began, sanctions kicked in, but you no longer have or maintain control of your application. That doesn't change the "boots on the ground" reality that any sale of your application is in violation of the sanctions.

I'm no lawyer, nor do I profess to be. I don't claim to have profound expertise in contract law, employment law, or even international trade law. That's not the point of this exercise. What I want the takeaway to be is why talking about laws and politics matter - why talking about more than just coding and algorithms matter.

I have been an avid reader of *2600* since pretty much the beginning. Before *2600*, I was an avid reader of *TAP*, and before that it was *YIPL*. I suppose I've always assumed that the technical, political, and legal worlds were always intertwined. I think, maybe, the problem might stem from what may seem like an obviously clear mission statement, especially to older readers, but might not actually be so. Even the masthead, *2600 - The Hacker Quarterly*, does not really capture the point and purpose of what the hacker community has always been about and even where it is going. I've seen so many attempts to define the hacker spirit, the hacker ethos, etc. While so many attempts have been made to define what hacking is, maybe it's high time we start to have a discussion about why we are engaged in this endeavor in the first place.

Allow me to start with a few talking points:

- Intellectual curiosity about how and why things tick
- The belief that there is always an option C, D, E, etc. even if it flies in the face of "conventional wisdom"
- Desire to continuously improve existing systems and processes
- Desire to create new and unimagined systems not yet dreamed of or thought possible
- Expand our minds to new ideas and concepts to the exclusion of rigidly held beliefs and values

OK, that's the low hanging fruit. I think where we begin to deviate is how we define hack and hacker. If we can let go of the "bits and bytes" and "geek" for a moment, it soon becomes immediately obvious that there have been reams of pages throughout the magazine written on privacy, on individual rights, and on challenges to the status quo. Hardly the stuff of CPU cycles or JavaScript. Let's look at how that plays out in the last year:

- Protecting against ransomware attacks
- Penetrating into Russia with news to bring truth to its citizens
- Preventing false and misleading information on social media such as anti-vaccine narrative
- Protecting against both government and corporate intrusion into personal and private lives of citizens

In short, if we have the skills, ability, and imagination to take flight with the former, it would seem a moral imperative to become the wheel of change for the latter. I'm thinking that is the hacker ethic and spirit.

We live in an ever-changing dynamic reality - one of power and regime change, of war and pandemic - but one thing remains constant. We are the voice for those that don't have a voice.

How to Double-Spend a Bitcoin

by 0x80

First, sorry for the sensational title. No, I haven't discovered some amazing way to subvert the blockchain's integrity properties and perform an on-chain double-spend. Rather, this is a social engineering attack which takes transactions off-chain, enabling a double-spend.

But please bear with me. I think this will be interesting to many readers.

What Does It Mean to "Own" Bitcoins?

"Ownership" is a messy concept to define for Bitcoin and similar cryptocurrencies. The easiest definition of ownership is "the ability to spend." If you can spend the bitcoins, they're yours, right? But what if someone else also has the ability to spend those same bitcoins? Let's look briefly at how Bitcoin transactions actually work.

Bitcoin transactions have inputs and outputs. Transaction outputs are the closest thing to instances of bitcoins existing (and inputs spend the outputs from previous transactions). These transaction outputs are locked away with little programs which one must cause to return true (or, more precisely, a non-false value) in order to claim the output's value and transfer it to a new output. Usually this locking script returns true if and only if one can demonstrate (with a cryptographic signature) that they have the private key corresponding to an address contained in the script.

Bitcoin's scripting language isn't limited to just asking for signatures; it's possible to

make lots of different programs. It's possible, for example, to make a transaction output which can only be spent by someone who can find a SHA-256 collision[1] or someone who can provide a specific file, such as a Bitcoin-themed parody of a Western Union ad.[2]

And it's entirely possible that more than one person has the requisite file, or that a hash collision is known by multiple people. (Maybe none of them knows or cares that they can get a reward in bitcoin for it.) Even if the challenge is to prove ownership of a private key, it's always possible that multiple people know the same private key. The key could have been generated with insufficient randomness. One person could have compromised another's device. Even if two people do everything right, it's within the realm of possibility (however astronomically unlikely) that they just happen to randomly generate the same private key or that a hashing collision causes their private keys to yield the same address.

Until a transaction output is actually spent (and another is made to replace it), it's impossible to say with absolute certainty who "owns" it. Arguably, ownership can only be defined retroactively: if you spent it, you must have owned it when you spent it.

With this in mind, I thought of an interesting scheme. Of course, I would never do this, and neither should you. But what hacker doesn't look at a system like this and start to think of ways it could be exploited? So please, dear reader, play make-believe and enact this scheme with me.

Double-Spending Physical Bitcoins

For this scheme, we'll be minting physical bitcoins. These are a real thing, by the way. A Bitcoin user called Casascius made a bunch from 2011 to 2013 before stopping due to legal issues.[3] They're fundamentally just "paper wallets" (private keys written down), but in the form of metal tokens. The private key (or a seed used to derive it) is protected by a tamper-evident sticker, and the Bitcoin address (or its seed) is readable on the outside of the sticker. A transaction is created which locks away 1 BTC (or some other amount represented by the coin) such that it should only be spendable by someone who has the private key.

This enables the physical coin, representing a virtual coin, to be traded. Since the address is visible, anyone who observes the physical coin can check the blockchain to verify that a still-unspent virtual bitcoin is represented by it. However, they can't actually spend that bitcoin until they remove the sticker, exposing the private key and permanently marking the physical coin as used.

You might be thinking that when we mint these physical coins, we're going to simply write down the private keys and spend the virtual coins later. But that would be too easily detected. If we sell a physical coin to Alice and then spend the corresponding virtual coin, Alice can check the blockchain and see that her coin is gone!

No, instead, we're going to do something more subtle, which relies on the fact that these coins are collector items. Collectors like to keep things in mint condition. They're more valuable that way. Thus, it seems likely that many of our customers will not want to spend the virtual coins. Anecdotally, I know someone who has a small collection of Casascius coins who has told me that they would probably never remove the stickers. Empirically, at the time of writing, only about 27.5 percent of the Casascius physical bitcoins (counting by number of discrete physical units, not total BTC value represented) have ever had their virtual counterpart spent.[4]

We'll specifically target our sales to collectors we believe will not spend the virtual coins. Suppose we have two different customers, Alice and Bob, and we believe that neither will spend the virtual bitcoin, instead treating the physical coins only as collectables backed by virtual coins. Suppose that we also believe Alice and Bob will not compare their physical bitcoin collections. (We might choose pairs of customers in different countries with no apparent connection to each other.) In this case, we can create two coins representing the same private key and sell one to Alice and one to Bob.

Interestingly, since ownership is so messy, as long as neither party actually spends the virtual bitcoin, both Alice and Bob might be considered rightful "owners" of the same bitcoin, and to each, it will appear that they are the owner. And just like that, we have double-spent a bitcoin!

References

[1] bitcointalk.org/index.
➥php?topic=293382.0

[2] See transaction
200f3f6f8a91ae438d1924e5cedca98c
➥ea7f0197b9eba11343948b5621ca19ed
which provides a gzip-compressed jpg to spend one such output.

[3] en.bitcoin.it/wiki/Casascius _
➥physical _ bitcoins

[4] casascius.uberbills.com/

EFFecting Digital Freedom

by Jason Kelley

Clearing the Fog

A year of digging into the location data marketplace led us to a company that allows police to access millions of people's location data - and reconstruct their lives with a few clicks.

When EFF began filing public records requests with police agencies last year, we wanted to see if we could learn whether location data pulled from our mobile devices was being exploited by surveillance technology companies. Included in one of the responses was promotional material from a company called Fog Data Science, LLC, which offered access to the precise and continuous geolocation of hundreds of millions of Americans.

We'd never heard of Fog and the company had almost no public online presence. So we requested more records about the company, specifically from law enforcement across the country. What we uncovered was a widely-used mass surveillance technology that raises "significant Fourth Amendment search and seizure concerns," according to Rep. Anna Eshoo of California.

What we learned is that Fog Data Science offers a sleek search engine called Fog Reveal that allows cops to browse through that location data as if they were Google Maps results, and a "device search" feature that provides historical location information for a single device going back for months or possibly years.

People's location data ends up with Fog after it's collected through smartphone apps and then aggregated by data brokers. Often these apps are unassuming - they might tell you the weather, for example - but meanwhile, they collect your location data as well. Data brokers buy bundles of this data and it can include a wealth of private information about you, such as your year of birth, gender, what search terms you use, and perhaps most importantly for Fog, your location. Each of these bundles of data has something called an ad ID attached to it, which is a random string of letters and numbers associated with your device, and which data brokers can later use to group them together to form a more complete picture of your behavior. This data allows companies to target ads to very specific groups of people - say, everyone with an interest in *2600 Magazine*. It also allows Fog to offer a service that they claim in marketing materials has "billions" of data points about "over 250 million" devices. With a few keystrokes, a Fog user is able to access an exhaustively detailed account of a person's life - often regardless of whether that person is under any suspicion or whether police have obtained a subpoena or warrant.

A pitch by a Fog official trying to sell his company's surveillance to law enforcement highlights how dangerous this product could be. To demonstrate a proof of concept, the Fog representative relayed how New York City experienced high COVID infection rates during the first few weeks of the pandemic, and it made leaders of nearby states nervous about New York City residents traveling and spreading the virus. The governor of Rhode Island had recently proposed banning all travelers from New York.

Fog's demo illustrated how its data could be used to help enforce such a ban. The company ran a dragnet query on its dataset, looking for anyone who had traveled between Port Chester, NY and Newport, RI between March 5 and March 22. It found 52 devices. Fog then narrowed in on one of those devices and ran a "pattern of life" analysis on it, querying for every GPS ping associated with that device for the previous 90 days. It found over 24,000 pings - more than 266 per day - locating the device across Rhode Island, Massachusetts, New York, and Connecticut. It showed how the device had taken multiple trips across New England, stopping in the New York City metropolitan area and near Rochester at different times. And it revealed the device owner's likely home, near Providence, and several other common destinations nearby. All of this was done without a warrant and with no apparent

law enforcement investigation. The person's private data appeared to be used as a sales pitch.

We were also able to analyze the app's public-facing code to get a better understanding of how its product works for the law enforcement end users. Fog Reveal, like Google Maps, is a web application that runs in your browser. To research its functionality, we locally reconstructed the app based on the web resources available by visiting `www.fogreveal.com`. This was possible at the time because, upon loading the page, without logging in or even clicking anything, the site automatically requests nearly all the javascript/HTML needed by the fully functional app.

By saving Reveal's frontend files and organizing them into directories mirroring their original URL paths, we made a local reproduction of the site's resources. From there, we wrote a mock backend server to serve the files and handle API calls made by the frontend, and then systematically worked out the format of data expected from that API. Note that because we had no access to Fog's backend server, we made several educated guesses and had it only return fake location data. So it's possible that our mock website differs from Fog's functionality. Once this was done, we had a semi-functional local reproduction of Reveal that made no requests to Fog's actual server, and yet allowed us to explore its features.

After signing in, Reveal presents a Google Maps view of the U.S., as well as a toolbox. Users can "geofence" an area with a shape such as a circle, or they can carve out a more detailed area, such as the shape of a building. The frontend circle tool will allow queries with a radius of 2500 meters, allowing up to nearly 20 square kilometers when performing a "signal search." It's possible that the backend imposes further limitations.

The user can also specify a date and time range for their query, and it seems that these ranges can stretch back over several months: a copy of Fog Reveal's user manual received from Greensboro Police Department claims that date/time ranges can extend up to 90 days, and can be searched "back to Jun[e] of 2017."

After specifying a geofence and date/time range, the user can run their query. Queries return a set of data points which represent where a device was at a given point in time. The user can then do further analysis on these signals, such as grouping them by the device that produced them, or displaying the path taken by the device over time.

We also discovered that if certain user parameters are set, Reveal will update its logo to display "Reveal Federal," and enable the frontend to request a much more powerful suite of query tools from the backend. These federal users have access to an interface for converting between Fog's internal device IDs and the device's actual advertiser ID. We don't know if this feature is operational but, if so, it would contradict statements Fog makes in other materials that its proprietary FOG IDs can't be converted back into advertiser IDs. And, if users could retrieve the advertiser IDs of all devices in a query's results, it would make Reveal far more capable of unmasking the identities of those device's owners.

Fog is a Fourth Amendment violation. First, police should not be able to use Fog's "device search" without obtaining a warrant, and public records show that many agencies did not get warrants before using this feature. Even when police obtain warrants before using Fog to perform geofence area searches, they would still violate the Fourth Amendment for all the same reasons that courts have held other geofence warrants unconstitutional.

Police use of Fog is a privacy disaster - it shows how location data taken from our devices is exploited and later used against us via police surveillance. We urge you to speak up to Congress and demand that lawmakers pass a meaningful and comprehensive data privacy law that allows all of us to control when and how our data is used. Such a law would stop this police surveillance at its source by preventing data brokers from obtaining and selling your data without your explicit opt-in consent.

Three Rules Against Tech Exposure and Dependency

by LVundertone

Imagine you start living with a roommate. Carl is fun, smart, and a good friend. If you need help fixing a running faucet, planning a trip, or even finding a hookup, he'll be happy to help. And he'll do it well. Want to relax? Carl can chat, Carl can tell jokes, or Carl can recommend the perfect movie. Soon enough, you share everything with him and invite him to come with you every time you go out, be it to attend a conference or just grocery shopping.

Now, you know nothing is free in this world, and Carl can't always be there for you and afford rent. How does he do it? Well, Carl works for the CIA and various private companies, reporting all your conversations, selling snippets of your life for these entities to use as they want. Otherwise, why would he put so much effort in holding your attention? And it's not just you, almost everyone you know lives with such a roommate.

While this is an exaggerated parallel, the world we live in isn't that different. Online services and smartphones hijack users for their own benefits, and eat up any data they can get, from messages to audio recordings. The average *2600* reader probably takes measures to protect themselves. But I find that more can be done even among informed people.

In this article, I will share a few simple rules one can use to protect themselves from tech's spying and attention draining.

Store Your Phone(s) Away

Of all the information a phone gathers, audio is one of the most important, since it is often not willingly that we feed it pieces of our speech. It is voice assistants which usually tune in, triggered intentionally or via the common false positives. Sometimes, it is apps which were granted invasive authorizations.

While the privacy-concerned individual might not have to worry, it all changes when spending time with friends or family. Your guests might not care about such issues and could expose you to espionage by carrying their smartphone into your home.

My solution is to require them to be left at the entrance, in a dedicated space. At home, my phone is used like a landline, and I expect the same from my guests. If you're lucky enough to live in a large house, it is rather easy to create a network connecting your phone(s) to a distant speaker to let you hear a ring even when you're in the attic or garage.

Some might refuse. Explaining your reasoning in more details can help, especially if you romanticize the issue and adapt to your interlocutor (depending on the person, the threat can be Big Tech, the government, or the lizard people). If that's not enough, you at least have raised some awareness and reminded yourself that there will be a third party forcefully added to your conversations.

Of course, other devices can listen in. But it's easier to unplug a mic or store away a laptop (which people usually don't hide in their pocket). As long as you don't collect smart devices, you've made a step towards more privacy with the added bonus of better focus and attention.

Cancel Your Phone's Internet Plan

A smartphone usually comes with an Internet subscription, granting an access to the web and online services from anywhere. While many find it useful to check maps, a calendar, or to find info on the go, it is rarely required. Maps can be downloaded, planner books have always been convenient, and one can usually wait a few hours to confirm a piece of trivia.

Still, plenty of people happily share their location, busy schedule, and more with Google and Apple. Even if your OS and the services you use are open-source, you are centralizing potentially sensitive information in a single device. And when everything is encrypted and uncompromised, you're still tying yourself to your device, reinforcing checking habits.*

Nowadays, it might be hard to find a phone plan without Internet data. But a compromise can be made with minimal data (where I live, many cheap plans only offer 100 MB) or the will to turn off your phone's data.

Avoid Social Media

Modern social medias are tailored to be addictive, designed to monopolize attention, and made to accumulate information about its users. Some members happily overshare, disclosing their whereabouts, purchase habits, and more.

While it is possible to not share anything superficial, it is also best to avoid interacting on those platforms. Instead of liking or commenting, you can reach out via different means (emails or face to face, for example) which allow for focused and richer interactions. This prevents exposure to dark patterns, and

diminishes your online presence. The benefits are an escape from deceptive design, and reduced chances of doxing.

If you really need to follow some accounts, you can easily create an RSS feed for them.

No matter how simple those measures are, they are important. I've met countless people who are concerned with privacy and security, or/and have been involved in legally questionable acts yet didn't consider the risks involved in their tech use. Malicious designs and data gathering can lead to grave consequences, yet are ignored for the sake of convenience.

This is not a plea against smartphones, which can be great when used thoughtfully. It is a reminder that what you don't care about is better hidden than public. With the recent Roe v. Wade reversal, many have realized that something as innocuous as period tracking apps were potentially dangerous. And no matter what your political orientation is, what you've shared with private companies or the public could get you in trouble in the future.

Privacy mindfulness isn't enough; you should also practice it.

* link.springer.com/➥article/10.1007/s00779-011-0412-2

Sneakers: 30 Years of a Cult Classic

by GI Jack

I've done two things this week. Watched *Sneakers* again, and picked up some old issues of *2600*. In the Autumn 1992 issue was a review of *Sneakers*, which was then a new release. Both this issue and the movie deserve a second look.

The movie has aged like wine. While a lot of the computer hacking and encryption are depicted with tasteful Hollywood magic, a lot of the other elements of the movie are spot on. Reverse engineering hardware, lock picking, a bunch of ex-blackhats working for a small pentesting firm with companies such as banks as clients.... International intrigue involving state and sub-state actors. Data being the new weapon, as discussed in 1992, more striking, topical, and pertinent in 2022 than it was in 1992.

It starts with Bishop, a college hacktivist who barely escapes arrest by just happening to step out for pizza as the police raid his setup. Flash forward years later. Under a false name he is now working for a pentesting gig with a bunch of other shady characters. An ex-CIA agent played by Sidney Poiter, a blind phone phreak (i.e., a Hollywood-ification of Joybubbles), and a hardware expert (Bishop), played by *Ghostbusters*-era Dan Aykroyd.

While the encryption cracking is bogus, there is a lot of the technique from social engineering (using disguises and distraction), lock picking, war dialing, numbers books, and of course, voice verification hacking that is reasonably accurate for a movie. The big kick is that the voice verification hack did not exist in 1992, but only decades later, when real voice authentication systems became common, was this actually used. The dialog about information being more of a weapon than guns rings more true in 2022, especially in the age of weaponized shit-posting.

The small team of people with shady pasts in a small company doing pentesting for banks and other companies should also hit some notes. Not nearly as visible in 1992, this today is a good percentage of the hackers that would have mocked the concept back then.

Another interesting but overlooked minor detail is the "machine that cracks all encryption," which was originally thought to be "an impossible device," but when it's revealed it does not crack Russian encryption, only American, it starts wandering back to Earth. In 1992, there were only so many encryption algorithms in use in America. You could count them on one hand. Blowfish wouldn't be written until the following year. DES (known exploits), IDEA (known exploits), and RC4 (known exploits) were common ciphers. Even if the exploits weren't known to the public at the time, it was very plausible that someone could have been sitting on some epic zero days. It's also now known that the NSA paid RSA to weaken a cipher, so it's plausible - very much so - that someone would have a device that breaks all U.S. ciphers based on insider knowledge. Most of these ciphers were *not* open source, and the concept of public, trustable, community encryption had not come to fruition. On top of that, it was hard coded into a chip in a black box to restrict distribution, and to prevent copying. Smart.

Of course it's not all accurate, and Hollywood takes the typical liberties in adding car chases, clandestine rendezvous, shootouts, and of course making computer use look good on the screen. Mix in some late 80s, early 90s costumes and the movie continues to charm its way to "perennial cult classic."

Internet Landscape in Germany

by Patrick patrick@pahem.de

I really love the international nature of *2600*. I haven't seen any other magazine with contributions from all over the world. In particular, I like to hear about other countries' Internet and telephone infrastructure for end users. Sometimes "Telecom Informer" writes a little bit about this topic. In this article, I would like to briefly explain to you the Internet for end users in Germany. It's not a scientific paper. Please read it more like a subjective view from me living in the northwest part of Germany.

In mid 1990s, the telephone monopoly by Deutsche Telekom (previously Deutsche Post) ended and every company was able to provide telecommunication services to end users. Some of the new providers used the last mile from Deutsche Telekom and some installed their own cables. Later the cable TV companies started to provide Internet access via the TV cable. A few years ago, fiber to the home got big hype and a subsidy program was founded by the government. Now, the local authorities are in charge and it takes a long time. Some other providers, mostly serving a limited area, even started to install new fiber cables at their own cost, which usually comes with a shorter realization time.

What Internet access bandwidth is available for you highly depends on the available providers and what cables your building has installed. With old copper lines, you can get DSL (ADSL or VDSL) with bandwidth between 1 Mbit/s and 250 Mbit/s downstream and 0.1 Mbit/s to 50 Mbit/s upstream. This depends on the equipment the provider has installed in the telecommunication cube down the street and how far away your home is from it. With a copper line from some provider (mostly Deutsche Telekom), you can also choose from a variety of different access providers which use the Layer 1 (cable) or Layer 2 infrastructure (bit-stream access) from the provider who owns the last mile cable. You can order Internet access from the cable TV company that's in your building for up to 1,000 Mbit/s downstream and 50 Mbit/s upstream bandwidth (DOCSIS 3.1). With the new fiber installation, you will see AON networks with active termination in the cube down the street or GPON with passive infrastructure until the next bigger aggregation facility. The offered bandwidth on this fiber installation is up to 1,000 Mbit/s in downstream and 1,000 Mbit/s in upstream, but mostly still asymmetric like 1,000 Mbit/s in downstream and 300 Mbit/s in upstream. For an apartment building in Cologne, I have seen an installation which uses fiber to the basement and then reuses the old copper lines with G.fast from it to the flats. Recently, 4G/LTE access or combined 4G/LTE with fixed line became available. Wireless point-to-point or point-to-multipoint connectivity isn't a big thing for end users. Some smaller citizens' initiatives are using wireless technologies to connect areas where no provider wants to invest. But nowadays, with the subsidy for fiber installation by the government, these self-help initiatives may not be needed anymore.

All of this access comes with neutral Internet access to any services and mostly without any traffic limits. Some providers have a fair use policy in their terms of use and can terminate the contract if it's violated. Also, a hard limit from some providers is in place. This will slow down your access to the Internet after a certain limit is reached, like O2 on their DSL products. But most of the fixed line access comes without any limit on traffic or services. For the mobile networks, this is another story. They have traffic limits with slowed down speeds after the limit is

reached, and also unlimited traffic to specific services like music or video streaming is available as a paid add-on.

In Germany, there is a big difference in the backbones of the providers. After the purchase of cable TV company Kabel Deutschland by Vodafone, they had a lot of problems with slowness during high traffic hours and after a massive amount of new customers resulted in oversubscription in access nodes. I had a cable TV Internet connection during this time and it was really bad. Video streams stopped for buffering multiple times. But luckily these times are over.

Deutsche Telekom is also a little bit special because they have a restricted peering policy and are usually not available for peering in big Internet Exchanges. They had a big fight with Google about YouTube traffic, and for quite some time you had slow access to YouTube during high load hours from Deutsche Telekom. Another story about Deutsche Telekom I heard from a small local provider recently: the small local provider had only business customers and, during the coronavirus pandemic when people began to work from home, a lot of their customers complained about slow VPN access for their employees. The customer's VPN gateway was in this local provider network and the customer's employees at home most often were connected with Deutsche Telekom to the Internet. The local provider had no direct peering with Deutsche Telekom and the reason of the slowness was unknown to me - maybe latency or bottlenecks in the network path. Anyway, to solve this issue, they had to establish direct peering with Deutsche Telekom which they had to pay for.

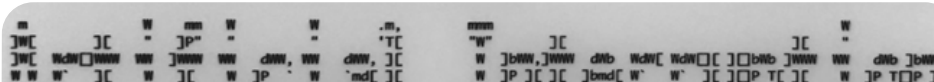
The price range for Internet access is from 20 euro per month for the lowest bandwidth and for 1,000 Mbit/s about 120 euro. Most of the Internet service plans come with unlimited domestic telephone calls. The telephone services have mostly migrated to VoIP. Almost all of the providers offer a router for a monthly fee of two to eight euro or a one-time reduced price. Popular brands are FRITZ!Box from AVM and Speedport from Deutsche Telekom. But it's also possible to use any router with the ordered services. After some back and forth, a law was established which let you choose the router on your own and set the demarcation point of the provider to the last passive connection point in the building - see Router Freedom.[1] For this, each provider has to provide a technical interface description of it. An example is the Schnittstellenbeschreibung nach § 41c TKG from EWE.[2]

Since a little more than one year, my current Internet connection is fiber with AON technology from a local provider. In the beginning, I had a FRITZ!Box 5530, which comes with a fiber SFP BiDi module, and was able to reach the provided 1,000 Mbit/s in download stream and 100 Mbit/s in upstream. I'm now on 75 Mbit/s download and 25 Mbit/s upload, which is enough for my current needs and cheaper. But I can highly recommend the fiber connection instead of DSL. Before I had a VDSL connection, and my first hop latency dropped by around 20ms to 3ms after migration to a fiber connection. Everything just feels a little snappier. I replaced the FRITZ!Box 5530 with an OpenWrt instance in a virtual machine on my home server and I terminate the fiber from the provider in a MikroTik five-port switch with a 1G SFP BiDi from `fs.com`. With this setup, I can use OpenWrt without an additional hardware router. The only negative was that my latency increased by 1ms. I think this is due to the virtualization, but I haven't checked this in detail. Maybe it's the MikroTik switch.

Thanks for reading, and I hope I can encourage some people around the world to write about the local Internet in their country.

[1] `fsfe.org/activities/routers/routers.en.html`

[2] `data.ewe.de/-/media/ewe/documents/02-privatkunden-telekommunikation/04-broschueren-und-infomaterial/schnittstellenbeschreibung-p-41c-tkg.pdf?cb=E2CC7123`



by Alexander Urbelis

Disconnection as Being

alex@urbel.is

For those not familiar with the concept of the Proustian moment, according to the American Psychological Association, it is "the sudden, involuntary evocation of an autobiographical memory, including a range of related sensory and emotional expressions." The term comes from Marcel Proust, a 19th Century French novelist and critic. In Proust's most famous work, *À la Recherche du Temps Perdu*, (translated as *Remembrance of Things Past*), at the outset, Proust's protagonist eats a tea-soaked madeleine cookie. The smell and taste of the madeleine evoke strong memories from his childhood of him doing the very same thing with his aunt. From taste and scent of this buttery morsel doused with lime-blossom tea, long-forgotten memories come back vigorously and vivaciously, giving the protagonist the ability to recall details buried within his mind, the minutiae of his home, the streets on which he used to play as a child, his town square... many memories that were lost in time came back into being.

I had a Proustian moment of sorts last week. What evoked my involuntary memory, however, had nothing to do with French pastries but was an older Richard Linklater movie, *Before Sunrise*, set in Vienna in the 1990s. I had both a flood of memories and a yearning for a time where, despite being disconnected, perhaps we were more connected to each other and the moment.

My Vienna story is from the spring of 1998, and, like the plot of *Before Sunrise*, also involved trains, chance meetings, and the limitations of 1990s technologies.

I'd taken an overnight train from Venice to Vienna. Living and studying in England at the time, I was traveling with a girl from Oxford who was, for that moment at least, my girlfriend. I don't recall very much at all of the Vienna train station, except for the money-changing kiosks in the terminal.

Hardly uncommon for 19-year-olds, I'll freely admit that I had a wandering eye. While my girlfriend was waiting in the queue to change U.S. dollars into Austrian schillings (remember, this was several years before the Euro, when each European country had its own, unique currency), I locked eyes with a gorgeous girl, waiting on the same kiosk, one place ahead. Shortish brown hair that was angularly just below jaw level, she had a look that was distinctly American. Accompanied by an older gentleman who sounded like he spoke German well, I wasn't sure if she was with her father or an older boyfriend. Furtively, we glanced back and forth at each, but nothing came of this. How could it? My girlfriend was right next to her.

That evening, the girlfriend and I were walking along a back street looking for a place to eat that wasn't touristy or obscenely expensive. Coming straight at me, on the very same sidewalk, was the girl from the train station. I couldn't let us pass like ships in the night so I pointed at her and said "train station," as she passed. We both looked behind us, me as I continued walking backwards and pointing at her. "Wow," was all she said as she smiled and continued on her way. What a weird coincidence, I thought to myself.

The girlfriend and I stayed in a little pensione outside of the city center, well off the beaten path. This was primarily to save money because we were taking the Eurail around for several weeks and still had a way to go. It was the sort of place that backpackers and students would frequent and I recall a strange, outdated, greenish theme running throughout all the rooms, matching the equally dated linoleum floors.

The night passed. We took breakfast in the pensione: a coffee and some fresh breads. As I was walking back to our table, I saw the girl again, sitting right there diagonally across. "Hello again. This is weird," I said. We all started talking. The girl informed both my girlfriend and me that she was a student from Arkansas and that she was traveling with her father. There was a connection between the two of us for sure. We commented on how uncanny it was to run into each other three times in a single day in Vienna, and especially so in the odd little pensione we found ourselves. We exchanged no details for staying in touch. We departed.

The girlfriend and I went on our way, westward, to Germany. Train to Munich, then to Frankfurt, then to visit some friends in Heidelberg. Everything was great. I sometimes thought of the girl from Vienna, but that was long gone by now and a few weeks past.

We eventually went back to England. The girlfriend eventually went back to the United States. We stayed together doing the long distance thing for perhaps a month, but eventually broke up.

The night after this breakup, I decide to go to the Oxford Union to listen to, if memory serves me right, Aleksander Kwasniewski, the then-President of Poland address the student body. After events such as this, the custom is to rush to the bar to grab a few Union-subsidized pints.

There was a massive influx at the bar. Though I remember nothing of what Kwasniewski said, I do recall quite vividly that I was ordering a cheap pint of Tetley's when I looked over to my right and immediately standing next to me was the girl from Vienna. "What're *you* doing here?" I asked. After a brief moment of disbelief, she screamed

and hugged me and asked me the same thing. It turned out that both she and I had been living in Oxford the entire year and never saw each other. What are the chances? It must be fate, we both thought. We exchanged phone numbers. We made plans for drinks. We were both excited.

I apologize for the anticlimax here, but nothing ever happened. The girl from Vienna had an overbearing boyfriend very skeptical of our Viennese connection. Like the girlfriend I had when I met the girl in Vienna, she too eventually went back to the United States. I had only her local phone number in Oxford and, after she left, we never spoke again.

All of these memories, the glances, the chance meetings, the slant of light on the street the evening we passed each other, that intense feeling of recognition when I saw the girl from Vienna next to me at the bar several countries away - they all came flooding back when I was re-watching *Before Sunrise*, a story of two travelers and their chance meeting on a train.

In the movie, Ethan Hawke plays Jesse, an American student, who meets Céline, a French student played by Julie Delpy, on a train en route to Vienna. An awkward fight between a married couple in their train car gives them cause to catch glances and, in due course, speak to each other. There's flirting and a connection, and they decide that they will disembark in Vienna together to wander the city. Unlike my anticlimactic story, Jessie and Céline have an engaging evening of conversation, self-discovery, and climactic sex in a park. They decide that their meeting and encounter was meaningful but decidedly fleeting, and they agree to part ways forever the following day. As they are saying their goodbyes, which proved more difficult than anticipated, Jessie and Céline agree not to exchange any contact details, but to meet in that same spot six months later. The movie ends while we watch them separately journey onwards towards home, alone, and we wonder whether they will make good on their promise of reunion.

Though there are trains and Vienna and chance encounters in common between my story and the plot of *Before Sunrise*, those details were not the sole reason why I had the Proustian moment that I did. As I watched Jessie and Céline, I remembered what impermanence felt like and recalled how short-lived and fleeting life's encounters were. Before the days of relentless social networking, we often met people and then said goodbye, forever.

It may be difficult for young readers today to understand that a goodbye at a train station was the end of a relationship. Today, every chance encounter is followed up by a LinkedIn request, inextricably connecting you to all of your acquaintances forever. Today, Jessie and Céline would surely have followed each other on Instagram. In the early 1990s, there was no LinkedIn, no exchanging of Instagram profiles, no Facebook friend requests, and barely any email.

Even email was ephemeral. Students often had university email addresses, but those were never permanent. Email permanence is a function of services like Hotmail and Gmail, with which we struck a dubious bargain: an email address forever in exchange for the right to datamine our communications.

With our identities attached to every encounter, to our locations, and to every interaction, there is an ever-increasing feeling of responsibility and accountability for everything we do, and this, in turn, leads to a sense of permanence of self from which it has become impossible to escape. It has, in other words, become impossible to stop being you.

This, however, leads to an ironical conundrum. Because we are stuck being ourselves, all the time, forever, that permanence prevents us from truly being and knowing ourselves. We cannot experiment, explore, or extricate ourselves from our online identities, and the full measure of data that represents our past actions and present identities. It is the very interconnectedness of the world, and the permanence and accountability that goes with it, that is holding us back rather than propelling us forward.

Perhaps that is because the permanent bonds and connections we make via social media are cheap and common. They are not meaningful. And the ease with which we connect, and stay connected with others, denigrates the value of all of our other relationships.

What would become of the encounter with the girl in Vienna today, or the chance meeting that set the stage for *Before Sunrise*? I would have connected with her on Facebook, browsed her pictures, realized she was at Oxford, and that lasting and inimitable feeling of recognition when seeing her at Oxford Union would have never happened. Jessie and Céline probably would have never locked eyes on that train to Vienna because they would have been staring at their phones.

The Proustian moment I had while watching *Before Sunrise* was in some sense a remembrance of the freedom that came from living in a disconnected world; it was at once a recognition of my fortuity to have matured in an age where I was not accountable for my every second of being, and of the tragedy that my children and their children will never know that feeling.

With this sense of self and being in mind, I do not think it is hyperbolic to state that the Internet has not only failed us, but in some ways has also broken us. If we are to recapture the beauty of the fleeting moment, the chance connection, the sense of uncertainty of ever meeting again, we need to fight for unaccountability, for anonymity, for privacy. The fight is not about data - it's about concepts more fundamental, powerful, and beautiful: about experiencing life, not as a profile or a data set, but as a human being.

What's Old is New Again: PDF Malware Part Deux

by lg0p89

Years ago (yes, "Get off my lawn!") when the industry was growing by leaps and bounds with new vulnerabilities weekly, and businesses were getting pwned for bragging rights and not tens of thousands of dollars, the innovation was to weaponize PDFs. This worked for a while, and defenses were put in place. This held for the most part until recently. The attackers are using the PDF in a slightly new way. They secure a target list, which these days is relatively easy and cheap. There have been so many breaches over the recent years, this isn't a problem. This coupled with some company websites listing their management with their email addresses makes this much less complicated.

With this in hand, the attackers send an email with the ill-intentioned PDF. This nuance started to be seen in 2020 and used the title "Remittance Invoice.pdf". That should have been enough to keep the users from opening it, but you know.... Within this is an embedded word document titled "has been verified. However PDF, Jpeg.xlsx, .docs". As this has been used over the last two years, the file name may have changed to something still catchy that would entice the user to click, double-click, or even triple-click the file. Yes, users still re-open the same files even after they know overtly and clearly that they are infected. I once ran an international phishing campaign for a global company. There were users who clicked the blatant phishing email, received the "You've been caught" landing page, and still went back clicking away. I guess they just wanted to make doubly sure they screwed up.

I digress. The PDF file name needs to be something that will draw the attention of the targets. You could also use "IRS Notification," "Proposed Bonuses," or any title that makes people believe they'll be able to see some data or information that they shouldn't have access to (thank you social engineering!).

Let's address the Word document title. This is embedded in the PDF file. The name itself is a little odd. For all the available choices, why this one? This all becomes clear operationally when you open it. Normally, when the user attempts to open it, Adobe Reader displays "The file [file name] may contain programs, macros, or viruses that could potentially harm your computer." When the user opens this, the message then reads "[File name] has been verified. However, PDF, JPEG, xlsx, .docs" may contain programs.... Let's say your PDF name is "The file Nobody may contain programs, macros, or viruses that could potentially harm your computer." When the user opens it, they see "The file Nobody may contain programs, macros, or viruses that could potentially harm your computer has been verified. However, PDF, JPEG, xlsx, .docs". See what it does?!

For a user that doesn't know to look for this or is too tired from working too much, the sneaky aspect of this might not be caught. They may breeze through the warning and check and find out too late what they did.

In the instance when the file is opened, which is completely plausible, it disables the protected view and the user is a happy recipient of malicious activity. Within the Word document is a URL used to load an embedding object (OLE). This contains code written to exploit CVE-2017-11882 for remote code execution. The code directs the system to download fresh.exe, which is a keylogger (snake). Curiously, you could use this method of delivery for other malware.

For the users thinking PDFs are safe, no worries, just open them, share this with family and friends - not so fast. This is still an issue. While this uses an old framework, the low-tech yet creative addition has the opportunity to really mess with your users.

What Does "Impossible" Mean?

by XCM xcm@tuta.io

I have recently come across another attempt at creating, or simulating, a perpetual machine.[1] According to Wikipedia, "A perpetual motion machine is a hypothetical machine that can do work infinitely without an external energy source."[2]

You will find it repeatedly stated everywhere that this kind of contraption is impossible because it would violate the first two laws of thermodynamics, or at least one of them.

This got me thinking. What does "impossible" mean? Is it something that anyone, or anything, will never be able to achieve? A goal that has not been reached yet? Or can we place this concept somewhere in the middle?

In the case of this marble machine, even to a layman like myself, it is evident that, in standard conditions, the gravitational pull alone will not be sufficient to propel the marble to its original position because the same force will be applied in the opposite direction when the object starts climbing. This would also be exacerbated by other forces, such as friction against the rails and air itself, which would dissipate some of the energy the ball needs to counteract gravity.

However, this reminded me of how often specific events are labeled as impossible, just because they would contradict what was previously observed or, even worse, one's biases.

Questioning, in a scientific setting, is generally frowned upon. It is sometimes perceived as anti-science. I find this attitude paradoxically anti-scientific. The scientific method itself relies on counter arguments to achieve accurate results. Blind faith is not science. It is just faith. At times, we seem to forget that the history of science is full of dogmas that were later superseded by more accurate understandings.

Now, I am not suggesting that we scrap the laws of thermodynamics. I would certainly have no clue how to come up with something better (or to even get started, for that matter). I am not a qualified scientist, either, but I feel that at times, egos can get in the way when interpreting data. It looks like questioning should be at the very core of the scientific method: "[...] when testing an hypothesis or a theory, the scientist may have a preference for one outcome or another, and it is important that this preference not bias the results or their interpretation."[3]

Unfortunately, questioning one's opinions is hard. Admitting that what we have worked for or believed in for years might be flawed is really, really difficult. Dismantling our beliefs is akin to rejecting parts of our own identity.

Naturally, if an outcome is considered impossible, most might be discouraged from attempting to prove otherwise. I am not proposing we should all start hoping that a bunch of monkeys hitting random keys on a keyboard will eventually produce the work of Shakespeare.[4] Even though statistically possible, this would clearly be so unlikely, its probability so close to zero, that nobody would be blamed for terming it impossible. What I am suggesting is that we should question as much as it is healthy to do so. It would be great if the efforts of scientific research, for example, were applied not only to prove the scientist's theory, but to equally disprove it. I think this approach would dramatically increase the quality of drugs in the pharmaceutical industry, for example.

What if one day we determined that the scientific method of today is in itself insufficient to prove reality? What about those processes that are not repeatable nor observable and for which we have no prior statistical data? How can we determine their likelihood? Who can scientifically state whether life on other planets is probable or an impossibility? Who can say that it is impossible that anyone would like Nutella on pizza?

Of course, I do not have answers to these questions, even though I have tried Nutella on pizza. I can barely decide what I will be doing tonight. All I am saying is that a healthy dose of questioning is the only way forward. Inquisitiveness gets lost with age in societies where the education system mostly focuses on sciolism and conformity rather than nourishing independence and critical thinking. At the same time, if everything around us was enough as it is, or any alternative was deemed impossible, there would be no progress and no way forward. Let's keep questioning, understanding, relearning, and teaching others how to ethically do so.

References

[1] YouTube - Perpetual marble machine project - final product (youtu.be/sMjHbDXfrV4)

[2] Wikipedia - Perpetual motion (en.wikipedia.org/wiki/Perpetual_motion)

[3] Rochester University. Introduction to the scientific method (teacher.pas.rochester.edu/phy_labs/AppendixE/AppendixE.html)

[4] Wikipedia - Infinite monkey theorem (en.wikipedia.org/wiki/Infinite_monkey_theorem)

Freedom of Speech: Terms and Conditions

by James Nagle

We've all seen it. Fact checks, disclaimers, and the worst of all, "misinformation." But who is checking facts, writing disclaimers, or judging information as incorrect? We live in a society that is arguably more divided than at any time in American history, and the attack on civil liberties is well underway. Partisan politics would like to continue to pit one side against the other but the truth is our rights and liberties as citizens have always been under attack from both sides. Both sides want you to believe that the cause is just while the truth is as far removed as can be. The old adage is true: "There's three sides to every story - yours, mine, and the truth."

The First Amendment to the United States Constitution is tricky. Fundamentally, it protects the right of American citizens to exercise freedom of speech, religion, and the press. However, the problem with this right is that over time, legal challenges have whittled away the intended broad sweeping protections afforded to citizens. Restrictions have been placed on free speech and this whittling away of our rights continues to erode the value of being an American citizen. Add in the continually churned sieve of politics intended to further divide the populace and you end up with a scary situation which fundamentally threatens liberty as a whole. Any time a majority of a population has been swayed by fear or coercion to take a firm stance on a topic or subject, all rational thought goes out the window. Given the information age we live in now, evidence to support one's own biases is easily found from a plethora of - sometimes even credible - sources. This leads to the possibility of a majority believing a particular topic which becomes a supermajority very quickly and ultimately ends up with reason becoming less and less valuable.

Given the information age in which we live today, it is ever important for those in real power to understand the big picture. And by referencing those in power, I mean those in real power, not the political puppeteers of our government. In the information age, those who control the information also control the narrative. Social media platforms have replaced more traditional sources of information where it counts and the fragmentation of thoughts and ideas has become prevalent. Echo chambers and silos rule the day and nobody is listening to one another anymore.

The result is, in my opinion, one of the most dangerous times of our modern existence. I'm talking about real world danger here, not just the danger of losing one's voice. The moment we end up in an artificial supermajority fueled by fear, ignorance takes over and innovation dies. Dissent is squelched and bad ideas become trending norms. Mob rules at its worst and the weakest minded individuals pay the price just as much as some of the sharpest and smartest minds of our time. Nobody gets a pass on the results of this catastrophe.

To make matters worse, true technology innovators aren't necessarily governed by the rule of law and aren't required to uphold a patron's constitutional rights. Given the transition of information platforms, this will be the fatal blow to our First Amendment rights as free thinking individuals. Our rights and liberties have been traded for the Terms of Service of your favorite platform and the bottom line of your favorite provider will dictate which information is acceptable for you to consume. You have been determined to no longer have the mental faculties needed in order to judge for yourself. Make no mistake, this is the beginning of another dark age.

We can argue details all day about what content is acceptable for a private information platform to allow, but the truth of the matter is it's right and wrong at the same time. Remember the three sides of the truth? The private information platform's truth is they should have the right to control content. The fear driven supermajority's truth is they should have access to reliable information. Unfortunately, the real truth is that information should not be prejudged before allowing others to make up their own minds about it.

How do we fix it? There's no quick and easy solution. Getting here was a natural evolution based on mostly good intentions and getting out of it will be a substantially difficult process spanning generations. It will require both current and future innovators and technology leaders to get back to basics and change their way of thinking. Ultimately, it requires a fundamental change of culture across our society that requires a big picture view.

People vs. Corporations

by Dark Phiber

Part 1: Robot Wars at the Big Box Stores

Disclaimer: This article is for entertainment purposes only and is not endorsing any of the behavior recommended herein. Any resemblance between references in this work of fiction and real-world entities is coincidental.

Corporations are not your friends.

They don't care about you. They only have one mandate: Create value for their owners.

That's it. Contrary to what you've heard, they aren't here to improve the quality of your life. They're not here to make you look cool, or healthy, or successful. They exclusively exist to siphon as much value as they can. They don't have any mandate to be moral or ethical. They don't care about the environment, living wages, or their employees. They only care about money.

The *only* thing that keeps corporations from being totally immoral predators isn't the invisible hand of the market. It's government regulation (despite all the arguments against government, there is nobody else out there protecting citizens to a comparable degree). Yea, that seems confusing since you've been told over and over (by corporate media) that government is the bad guy. Go figure? Government isn't what's bad. Bad people in government are bad. Meanwhile, collective bargaining (a right often protected by government) and centralized regulation is the only thing keeping most people from being worked and exploited to death. And what few rules and regulations we do have are at least trying to keep corporations from destroying what little habitable environment we have left.

Corporations do all sorts of sneaky-yet-slightly-legal tricks to increase how much money they make. They mislabel and misrepresent products. They make promises they never intend to honor. They constantly lobby to reduce their accountability to anybody but their shareholders. They buy politicians. They buy scientists. They produce their own "studies" showing their products are perfectly OK. They outsource as much as they can to reduce their costs. They hire more employees than they need in order to avoid having too many full time people they have to provide benefits to. They replace people with machines wherever possible, because robots don't complain about not having healthcare or a living wage.

In this episode of *People vs. Corporations*, we're going to talk about the robots. How instead of hiring people to handle checking things out for you, you have now become conscripted in harmony with the surveillance state point-of-sale robot to scan your own products, pay for, and bag them.

It's funny that the big box stores now have almost completely switched over to robot point-of-sale. Half the time these machines aren't working properly. Half the time you need assistance because robots can't be trusted to exclusively transact certain restricted items, but the humans they do manage to have around are even less capable than the checkers the robots replaced. It's a mess. And there's often somebody ahead of you in line who can't figure out how these things work, or wants to turn check-out into a 45 minute life lesson for their six-year-old. These machines end up taking more of your precious time so corporations can make more money.

Corporations screw with you in all sorts of ways. For example, have you ever tried to price-compare two similar items in a grocery store? Maybe it's two jars of peanut butter and near the price tag you have a "unit price" of say, x cents per ounce. Then you try to compare it to a nearby jar and it says x cents per pound. Hey, they gave you the unit price. They deliberately switched it up to keep you from being able to easily figure out which product is the better buy. They do this all the time. They also do shady things like mislead you into thinking that a six pack of one item is more expensive than a 14 pack of the same item. Unless you do the math, you may find buying in quantity isn't always cheaper, even though most people think it is. There's bags of chips with printing that obscures the fact that 75 percent of the bag is empty. Even the placement of items on shelving is scientifically designed to get you to pay more. They have monetized the act of convenience. They have even figured out how to sell broken/defective products, knowing a certain percentage of people won't return them.

I think of myself as an ethical person. I abhor stealing. But years and years of watching these corporations and their minions fuck with me has made me become quite the cynic, and I finally found something to do to ease that tension. It's my way of taxing corporations for forcing me to do their work. It's getting back at them for doing everything they can legally (and often illegally) get away with to make a little more money. Let's call it: POJ instead of POS. Not point-of-sale. Point-of-Justice.

What is POJ? It's the defiant act of getting over on the robots and their corporate overlords. And it's incredibly easy to do, and relatively safe. You just basically act like the kind of idiotic consumer they treat you as - and you can win all

sorts of prizes! Even if you get caught, just admit it was a mistake - no harm no foul, even though it's highly unlikely you will get caught.

Getting Over on the Robots

The robotic point-of-sale machines have all sorts of anti-theft technology. But there are plenty of ways to defeat/confuse the system. I can't go into details of how any particular machine works, but I can cover some of the basics of how these machines try to ensure the sales transaction works the way *they* want. (For example, they employ scales on the bagging area and know the weight of each item. If you scan a product that weighs ten ounces, and then don't put that item in the bag (on the scale), the machine will alert the robot manager to take a look - note that I've never seen the opposite happen, of accidentally scanning an item twice and the machine letting you know it's under-weight! Go figure?)

Some machines also use video "A.I." (another bastardization of the term "artificial intelligence") to examine your motions to see if you're picking up and putting things down appropriately. So all your motions in front of the robot should be fluid and normal. There are some tricks you do *not* want to do, especially since you're on video. This includes scanning one item twice like a cheap bottle of wine, when you have two bottles and didn't scan the more expensive one - it's easier to get caught doing that.

And of course, there's RFID tags in certain items, usually expensive or small items that can be easily hidden. Avoid trying to sneak out any RFID'd stuff. You never know where sensors are.

Here are some specific techniques:

The setup. You typically want to limit the items you try to get past the robot. Don't pick something obvious. Don't pick something too expensive. Don't pick a single of something. Don't pick something large. Don't pick something that can't be bagged with other stuff. Start a normal checkout and have at least one or two bags partially filled with things in the bagging area. Then execute your POJ....

The Double Dip. This is by far one of my favorite tricks. Take two items that stack or nest (like half cans on top of each other, or two stacks of things that you handle as if it's one stack: paper plates, tortillas, or small boxes of things). Know where the UPC symbol is before you grab the stack so there's no fumbling. Pass both the items over the UPC scanner in one smooth motion - it will only register once, and put both of the items in your bag. But at the same time you drop them in the (mostly full) bag, grab the bag and transfer it from the bagging area to your basket. This fakes out the scale. (This is why you have one or two mostly full bags set up before you do the double dip.)

If you're creative, you can find some pretty expensive products you can do this with, like crab meat. Although I'm happy just being able to get a 2-for-1 as payment for my otherwise freely-exploited point-of-sale services I had to provide.

The Miscount. If you're buying three or more of something, I heartily recommend you always miss at least one item. You have five storage boxes? Ring up four. You have ten cans of cat food? Ring up eight. If you get caught, well, you thought the machine rang up everything - sorry I'm not a checker, I'm a consumer. This especially works well with larger items you don't have to bag. Be sure to go through the motions trying to scan everything - the wireless scanner works good for this because half the time it doesn't register so you're always looking like you're trying to scan more than the number of items on video.

The Stowaway. This technique works well in a variety of situations, even when dealing with an actual cashier. Hide an item underneath another item, but make sure the heavy/large item on top has the UPC showing so it isn't moved around. Also, make sure whatever you're hiding underneath the item doesn't have an RFID tag. You'd be amazed what can be "accidentally" found underneath a 40 pound bag of dog food. Again, just remember if you try to do this with something too expensive, it probably has an RFID on it and you'll have problems. But there's lots of stuff that won't.

The Hookup. I routinely do this in big box hardware stores just to see how lazy humans can be. For example, I just picked up some plumbing parts. Different adapters. I attached several of them together with only one UPC tag obvious, and they didn't realize it was three separate items. Even easier to double or triple-dip with the robots.

Now let's talk about exiting the store.... If you're shopping at a store that forces all consumers to wait in line and have the number of items checked and individually counted, this trick is a lot harder to do, and I don't recommend trying in those stores. These are usually the "membership clubs" which actually require you to agree to such exit-gestapo tactics in return for being a member. Regular retail outlets can't "detain" you like this - you didn't sign an agreement to shop there; you didn't pay a membership fee. Once you bought your stuff, you are free to go.

For the non-membership stores, it's really quite simple: just leave the store. Yea, there's sometimes a "receipt gestapo" near the exit, but *never* volunteer to stop and hand your receipt to them. Just blow through the exit, not making

eye contact and holding your keys in one hand, receipt in the other like a good little efficient consumer. If they're checking somebody else's receipt, blow by them and head outside. It's perfectly normal. They are not expected to check everybody's receipt, and most of the time they are not allowed to chase after shoppers who don't comply - that's a liability issue for them. Most big box stores even have a policy to not chase obvious shoplifters. If you're stopped by the receipt gestapo, let them take a look. They are unlikely to do a full audit of your basket - they'll just look for obvious items on the receipt. They aren't paid well enough to give two shits that you paid for three cans of soup but have four in the basket - not that they'd catch it anyway. And if they do catch a discrepancy, you simply say, "Really? I thought I scanned that." Big whoop. Go back and scan it. That's the worst that could happen.

Additional guidelines: Do *not* be greedy. The objective here isn't to generate a lot of money. The objective is to penalize the corporations for their anti-worker, pro-profit-at-any-cost mentality. If I can get one item free every time I go to the store, I feel like I've "won" a small skirmish. It's now a point of personal pride to hone my skills in this respect.

It's important to note that every big box store has an allotment of acceptable "loss." They can lose inventory a thousand different ways, and they don't really care. They make up for it a million other sleazy ways as I've explained earlier.

For those that say, "Don't do this. It will only cause product prices to increase and you'll end up paying for it later." Ha ha... not buying it. This notion is predicated on the bullshit idea that shareholders should make their money first and foremost before they'll ever cut consumers any break, and is the whole reason why more people should be doing this. If we're second class citizens and the rich people getting richer is the priority, all bets are off. I'll serve my own interests before yours every chance I can get, just like you'd do to me. It'll cost you more to "pass it on to the consumer" one way or another. I *refuse* to accept it as a universal truth that executives will always get paid while the little man gets the shaft. And you shouldn't buy into that notion either. That's the same mentality that claims unions hurt workers more than they help. It's BS.

Good luck with your POJ training!

An Atavistic Freak Out, Episode Six

by Leon Manna

This story is a work of fiction.

I have dark circles around my eyes.

Leon holds up... I know that. I don't know why though. They still think that's who I am and apparently haven't even considered the fantastic possibility, or the reality, that I'm *not* Leon. I just can't figure out how. It doesn't make sense. Did I really fine tune him to be that believable? They didn't get my DNA before I "died." Maybe some bureaucratic error fucked it up? Paperwork got shuffled wrong, or placed into the wrong file cabinet, or a shredder, or an evidence room that caught on fire? But why question a good thing?

They had Moe take an MMPI test - Minnesota Multiphasic Personality Inventory - and he matched the personality type I had after they did a profile. So close, in fact, that I see them as morons for not considering if we knew each other beforehand, because we did. Moe was one of my best friends in high school. He did me one last favor: he didn't tell the FBI that I was actually named August, I faked my own death when I was 19, and I've been living under a synthetic identity since then. He didn't lie; he just neglected to tell the truth.

…

Pierre was a tall guy Lenny knew down at the bottom of the U.S., the Atlantic southeast. They were friends when he was there, I believe. He had black hair and a smile on his face. You're in good company. He insisted that he wasn't French, despite his name. I think he was Irish.

And now we had Georgia's best compulsive boat thief. It was his specialty, his art. Usually he disables the GPS on the boat, drives it around, and then puts it back where he found it. He never keeps the boat. I guess he's just a nice guy. He's also a math genius, which I think helped his navigation skills. I watched him hash a string by hand with a pencil and paper. It took him seven minutes and the hash was correct. And he could get us to Cuba. Somewhere else from there, maybe....

We were driving through this tropical jungle in Savannah, Georgia when Lenny suddenly started shouting to pull

over. I did, and we were outside of this construction site for an almost finished house. Lenny reaches over and honks the horn for me. Thirty seconds later I see Pierre shamble to the doorway with a gasoline can, leaving a trail behind him. Holy shit, I thought, I think I know what's about to happen. He tossed the cigarette on the trail, and walked up to the car with that smile.

"Who the hell is this?" I asked Lenny.

"Drive! Drive, motherfucker, drive!"

I knew better than to stay. As I floor it and the car bursts forward, the great red bang of the house's final breath went into the air, shattering my ear drums and any sense of peace. I took two hydroxyzine tablets. He filled the basement with gasoline.

"I used my lucky cigarette. Last one I'm ever smoking," he said. "Ever."

They got us in Miami. There we were, standing on this dock, the three of us, drinking some rum because we had *just* made our grand escape and now we were off to start a new life as we had a ride to Cuba. And we were just ready to get on our way when I saw someone walking down the pier towards us. Me and my attorney squint to see who it was, and it's some guy around my age wearing some joggers and a hoodie. He comes up to me and shakes my hand, says, "Leon?"

And so I said, "Who might you be, you... Fuck?"

"Are you Leon?" I look at this hoodlum who can be no older than me, thinking, what harm could it do? He doesn't *look* like a cop, he's just some dude. Maybe Lenny knows him.

So I look at Lenny, who stares at me silently, and I look back and say, "Yeah. That's me."

From behind me, I hear Lenny say, "Idiot."

And then, all these years later, it hits me that this is Moe. This is Segev, that many years older, with a sharper jaw and a beard, and now he was wearing his glasses. It's been so long, I didn't recognize him. You know, I wasn't even mad I was getting arrested. I saw my old friend again, even if he's taking me to prison.

And so he throws some cuffs on me and says he finally got my ass when it hits me, and as I look behind me I notice he's taken his badge out. I'm pretty drunk at that point. Immediately my attorney jumps towards him, screaming about probable cause and demanding that he take the cuffs off me at once.

"They have someone coming for you too, don't worry."

Lenny cusses at him and cites some legal code that I didn't know. Moe made a weird face, and said, "Whatever. But you're not going in the same car." I turned around to see what Pierre thought, but there was nobody behind us. Just an empty harbor, the waves churning peacefully.

In the back of the unmarked car, we drove towards a police station somewhere... I don't remember. Me and Moe made eye contact for a second through the rearview, and both chuckled. We had been making frequent phone calls, which started out as him trying to convince me to turn myself in but turned into friendly conversations and then a verbal backhand from me at the end before I abruptly hung up.

"I finally got your ass."

I said, "You know, I shouldn't have doubted you."

"You should have seen the office after what you did. First our computers stopped working... heh... and then, when the evidence room caught on fire, the front desk guy... he.... Hahaha.... He shat himself!"

I'm starting to see a pattern. It's like my presence, or even the very *ghost* of my presence makes people shit themselves. Or maybe I'm just schizophrenic. "That wasn't me. It was Luke. Luke Lemon."

He smirked. "You're so fucking dumb. Hehehehe...."

"I lied, his name was Nash Nashville. He was from Memphis, Tennessee."

Moe chuckled.

"No, actually, it was a man named Austin. Austin Texas."

When the unmarked car got to the station they had both - this time deviating from the pattern - vomited from laughing so hard. But the taxes paid for the car to be cleaned. I don't think they ever really got it all out, and there was a little ketamine in my vomit so the car is forever tainted when it comes to evidence.

Our story is almost over. There's one more part I have to tell you before I say goodbye.

Are we going to prison? Maybe! Find out next time!

Inconvenient Truths

These last few years have been difficult for all of us on so many levels. And we keep thinking we're almost at the end of it when more bad stuff happens. Sometimes it's directly related to the pandemic; other times it's something entirely new. What helps to get us through is support from those around us and fresh ideas on how to tackle these challenges.

As we approach our 40th year, things look especially daunting for us. We've been through hard times before, whether it was another distributor making off with half a year's income, lawsuits from some of the most powerful entities on earth, or unjust and inhumane government prosecutions of those close to us. But what we're facing now is probably the biggest threat we've ever had to our continued existence.

Being a printed magazine has been especially difficult for a couple of decades now. Being one that takes no advertising made that challenge even greater. We saw independent bookstores forced out of business by big chains. And then those big chains went out of business, leaving nothing in their place.

COVID-19 made all of this even worse since lots of the issues we had already printed never made it to the newsstands because they weren't open. And many of them never reopened. Even though people were looking for our magazine, there were significantly less places to find it.

In 2022, things got even worse as the price of paper skyrocketed, which made our profit margin practically nonexistent while inflation drove prices for almost everything else upwards. It hasn't exactly been a cheery time.

One bright spot in all of this has been our Kindle edition, where sales were significant since its launch in 2010. This digital platform offered another way to get *2600* into subscriber hands without the cost of printing. But as we go to press with this issue, we've been informed that Amazon has decided to discontinue magazine subscriptions on the Kindle, except for the biggest mainstream publications. We can't say we're surprised - we always warn our readers about letting big companies call the shots. But this was a case where we were able to reach a great number of people in a convenient manner and it really helped offset the printing expenses, even after Amazon took their cut. This loss couldn't have come at a worse time.

But there is hope. Literally. The last few HOPE conferences have been able to help support the magazine and keep things from becoming too dire. Of course, COVID threw a monkey wrench into that as well when we weren't able to hold an in-person conference in 2020 and were forced to limit attendance in 2022 due to health concerns. Ironically, in 2019 we had thought our biggest challenge would be finding a new home after losing the Hotel Pennsylvania. We had no idea what we were all in for.

Happily, the most recent conference at St. John's University went better than we had ever hoped. We are extremely fortunate to be able to continue and build future conferences in such a venue. But, because of the fact that we had to make things smaller due to the pandemic, we didn't wind up where we needed to be in order to help support *2600*. The timing was just really bad, which seems to be a recurring theme lately.

So how bad are things? They're bad, no question. Those of us who can afford not to get paid haven't been for the past few months. We love what we do and we will make many personal sacrifices if it means that we get to stick around and do this for longer. We may have to make difficult decisions down the road, but we're really hoping to stave that off with the help of the community.

Here's where things can turn around.

We have a great biennial event with the HOPE conference. If we're able to get 1500 in-person attendees and 1000 online attendees each time, most of these problems will vanish. Note that the in-person number is actually less than what it was in past years because we don't want to recreate the overcrowding that occurred back then, even though we have much

more space now. Offsetting that decrease with paid online attendees who participate digitally could add a great deal to the conference, with more participation from all over the world. (We're also not opposed to growing into a bigger in-person crowd in future years as we use more facilities.)

There has even been talk of making the conference an annual event due to how smoothly it went this last time. We won't know if that's doable until we see how the next one goes, but if we are able to reach that stage without overworking ourselves to death, then we will be on very solid ground indefinitely.

But we're more than a year away from knowing if this will be sustainable. 2023 is going to be a pivotal year and we need to come up with more immediate solutions to help get us through all of the challenges that are being flung at us.

Ideally, *2600* should be self-sustaining. While this has become quite difficult with the cost of printing and the shrinking number of retail outlets, it's not impossible. The one thing readers seem to be most adamant about is the continuation of the printed edition. We believe following the trend of many magazines and only having digital editions would be a big mistake for us. People value the physical copies and those tend to live forever. It's a true gift to be able to do this year after year and we really don't want to give it up. But we need to make some serious progress if that's going to happen.

We don't see a way to get *2600* into more retail outlets if there simply aren't any more of them. We experimented with supermarkets during the pandemic and it was a disaster. (Apparently, grocery shoppers aren't interested in magazines about hacking. We know this now.) The loss of so many bookstores, especially the independents but also the chains, has hurt our entire society and we're now living through yet another consequence of that.

More physical subscribers would certainly be a good thing, but due to the volatile costs of printing, packaging, and shipping, it's not really an economic boon for us. What really would make a difference at this point is a dramatic upturn in digital sales. We would need around 3500 digital subscribers to offset the losses from Amazon alone. And since Amazon won't share the subscriber info with us, the only way for us to reach our current Kindle subscribers is through the words in the magazine itself. We hope they're all able to see this and to act upon it. But again, that only addresses the Amazon problem. We still need to add more subscribers to help address the shortfalls brought about by everything else described above.

We believe this is doable, as there are so many people who react with amazement and enthusiasm when discovering that we are in fact still around. Since we don't advertise and since so many establishments where we were displayed have disappeared, it's very easy to lose track of our existence. The entire zine community has been hit with this reality and we're one of the few survivors, which is a painful reality for us. Assuming we make it through this latest crisis, we intend to do everything we can to help other independent publications find new visibility.

At press time, we're still trying to put together a digital subscription option that works the way we want it to. We've actually been trying to do this for years, but have run into software that insists on using DRM (copy control which we do *not* want) or that doesn't know how to generate unique URLs for subscribers. It's annoying, but we're determined to solve this. Hopefully, by the time you read this, we will have.

But what really comforts us is knowing that hacker ingenuity is on our side. There are people reading this now who have ideas that we've never thought of which will prove immensely helpful. The power of the hacker mind, determined to accomplish that which they have been told is impossible, is our greatest ally here and one which we believe will help us solve problems and get the word out.

We've accomplished so much over the past four decades. It's always been a bit of a struggle. But we truly believe we're the right people in the right place at the right time to take on this challenge. While the reality at the moment isn't what we'd prefer, we're convinced we have the power, ability, and intelligence to change that reality into something a little better.

We're ready for the next chapter.

You Can Use the Dark Web for Good

by Djilpmh Pi

One of my earliest memories of trying to figure out how things work and what makes them tick is when I was nine or 10 years old and my parents left me alone in the house. I took a dinner knife and disassembled the Big Ben mechanical alarm clock. It had two windup handles, one to wind the spring to keep the clock running, and the other for the bell clapper. Very cleverly the "quiet alarm" mode had a lever that slipped a thin piece of leather between the clapper and the bell housing so it was not as annoying as a full on alarm. I could see the gears and levers spin and slide; it was wonderful. It kept working even though I had a few parts left over which I could not remember where they were supposed to go back. I only got into trouble the second time I took the clock apart into more pieces, and it no longer tick-tocked. No matter, figuring out how things worked was in my blood, and this hacker never looked back even after my spanking.

Today my Big Ben is to figure out and explain to people how the Dark Web can be put to legitimate and beneficial uses. For too long, it has been yielded to the "dark side" for evil purposes. It is, after all, only a technology and, on its own, tech is not inherently good or evil. Whether something is good or bad should be judged by the motivation of our actions and the harmful or helpful outcomes.

Everybody Knows the Dark Web is a Bad Place

The Dark Web is well known as a playground and hiding place for criminals including drug dealers, sex traffickers, and every kind of bad people. It is painted by popular media as the dark alley everyone should avoid because you will get mugged and worse if you go there. Taking a closer look, it is a powerful tool that can be used for good in spite of its evil reputation.

The U.S. Navy created the technology behind the Dark Web initially to protect American spies in hostile locations. See `en.wikipedia.org/➥wiki/Tor_(network)` for its origins.

Power Tools Have Two Sharp Edges

Power tools and power concepts are two-edged swords: free speech protects hateful speech, anonymity protects privacy but encourages trolls, and airplanes can be used by terrorists to take down high rise buildings. Unintended consequences and uses are the second sharp edge of powerful ideas.

If we say that "good honest people" should stay away from that dirty Dark Web because icky bad people use it, we could also say that criminals use guns, cash, and cars, so honest folk should not use those icky things - who knows where it's been! You have to decide whether the good honest police should use guns or just stick to the billy clubs for law enforcement. Oh wait, criminals use sticks too. As with any power tool, the Dark Web can be used for both good and evil. Unfortunately, its legitimate use by honest people has been overshadowed by its icky reputation.

Good Honest People Can Benefit

Good honest people who don't want their network activity to be tracked, victims of domestic violence, and whistleblowers can all benefit from using the Dark Web.

Anyone who is interested in privacy can use the Dark Web to protect their personal information. These uses will be explained below. Having a basic understanding of the Dark Web, or Tor (the technical name is "the onion router") can be helpful to understand how and why it works. Recognizing the imitations of the Tor software is as important as understanding its power. For an explanation and resources see `torproject.➥org`.

Use Cases for Dark Web (Tor)

These are my hacks of the Dark Web, figuring out how to use it for the benefit of honest people in these ways:

1. Avoiding tracking: protecting the privacy of your Internet use
2. Protecting the location of victims of domestic violence
3. Protecting anonymous whistleblowers

Standard Disclaimer

Seek professional advice and talk with people you trust. You are responsible for your own actions. Be skeptical and verify anything important.

Tracking and Privacy

Tracking collects information about your Internet use, what you search for, what you buy, and what time of day or night you use the Internet. That information is sold to advertisers who pay very well for that information. If you don't already think it's creepy and invasive, you've missed something basic about intrusions into your privacy.

What Google Knows About You

We've all observed that a random Google search for vacations in Glacier National Park will shortly generate advertisements for tour packages and hotels in the area. The simple explanation is that your free use of the search engine has tagged you as someone who is interested in the area, and that information is sold to the hotels and tour providers around Glacier. Early in the use of tracking and advertising, a parent discovered

their daughter was pregnant because diaper and maternity ads started to appear in the browser and computer used by the family.

Defeating tracking of your every action can feel insurmountable. Corporations already know every intimate detail of your life: what ice cream flavors and brands you like, whether you use ice cream as a celebration or consolation. It's creepy to know that complete strangers - not even limited to your country of citizenship or residence - know everything you buy and read, and at what time of night and which days you like to shop. It should be annoying to people that a website already knows your "consumer score" to set your place in the helpdesk queue and probably to decide what deals to offer you, individually. See `sift.com` and `nextroll.com` for examples.

Private Browsing

To remove tracking of your web searches, it's possible to use a private search engine such as DuckDuckGo or StartPage. Both proxy your search request, so your IP address is initially protected and cookies are not passed through. But if you click on the search result directly, your computer can become visible to both the service provider and the website unless you are careful to use the "Anonymous View" link in StartPage.

Without using "Anonymous View," DuckDuckGo or other search engines connect you directly to a website and your IP address, cookies, and other tracking mechanisms kick right back into action.

If you use a VPN, your real IP address is masked by the VPN provider, but you have to trust them to keep that information private, and VPNs don't do anything to protect you against cookies and other tracking methods.

What If You Had Some Friends...

Defeating tracking can actually be easy. What if you had a group of friends help each other by randomly mixing the traffic up among the members of the group, so it's no longer clear who was shopping for cars, a particular medication, or pregnancy tests? Those searches and connections would be randomly changed and no longer linked to your individual identity. You still have to deal with cookies and other tracking, but your location information is no longer usable to track you.

If your group of friends were distributed all over the world in many countries, that would fool some websites nicely.

Randomizing Internet Connections to Defeat Tracking by IP Address

That group of cooperating friends who allowed you to use their shared Internet connections could make the IP address detected by the Internet web server or store different for each visit. If there were hundreds, or even thousands of these friends, that would confuse the tracking tools to the point they wouldn't know your real IP address or location.

Your New Friends

This is my first hack of the Dark Web. Let me introduce you to your new friends: a group of people who volunteer to do just that for you, for free, because they all believe in and support privacy. Surprise! They operate the Tor (the onion router) relay computers that make up the Dark Web.

Tor is the technical name of the Dark Web, and its only purpose is to hide your real location by passing your traffic through a series of friendly relay routers between your computer and the website you are accessing. Tor does nothing else. But even that little help from your new friends can do a lot to defeat tracking.

Protecting Victims of Domestic Abuse

Some victims of domestic abuse leave town for fear of their safety and for their lives. It is most important to keep their location secret from their abuser.

Finding Someone's Location

If the attacker finds an email that was sent by the victim to family or friends telling them all is well, it is trivially simple to find the IP address from which that email is sent. As explained in `www.lifewire.com/how-to-find-➥email-server-ip-address-818402`, this method can be used to check the authenticity of an email message, or flag it as suspicious in origin. If your cousin lives across town, why are they sending email from Norway?

Sadly, the same method can be used by an attacker to find the location of their victim. Geographic location is used by website and online store owners to validate the physical location of a potential visitor or buyer, so if an order is connecting from France, it would be inconsistent to have the item sent to Iowa, or vice versa. At least it would be worth getting additional verification that the purchase is legitimate. A diligent website owner could use geolocation to reduce fraud. Another example would be comments on a political activity website of users claiming to be local residents that are traced to geolocations in Eastern Europe or Far East. `www.➥iplocation.net/` and `en.utrace.➥de/` are examples of many free online services providing the physical location of an IP address.

Protect Victims From Real Harm

If a victim left town to escape an abuser, revealing even the town or suburb of their current location has made all the effort a waste of money, time, and energy. Such exposure puts victims in real harm's way.

My second hack of the Dark Web is this: using Tails or at least a Tor browser can keep the IP address of the sender private and protect the real location of the victim. Of course, if the email contents describe an address, no technical

solutions will protect against sloppiness of their security.

The best strategy would be to completely isolate from previous contact with family and friends, but that discipline can be hard to keep forever, particularly during significant times such as holidays, family births and deaths, or birthdays. If communications were attempted, at least try to avoid leaking the location of the victim.

Protecting Whistleblowers

Whistleblowers protect our democratic society by shining a spotlight on evil. They are an essential part of revealing abuse of power, avoidance of responsibility, and other things that destroy the civilized part of our modern society. By revealing information about such abuses, they put themselves at great risk of reprisal (snitches get stitches, rats get bats), so it can be helpful if a whistleblower can remain anonymous. Any accusation has to be proven to be true or false by investigation and other information and testimony: that is the responsible action of a conscientious citizen.

If you came into possession of some documents or information that proved illegal, immoral, or unethical behavior of powerful people, what would you do? Many people think twice about being identified as the source because they correctly fear the anger and reprisal of those powerful people and their unthinking followers. This is the case whether the issue is in your neighborhood, in government, or in a large corporation.

It's Hard to Be Anonymous

It is very hard to be an anonymous whistleblower. Conventional email contains the IP address (and thus location) of the sender's computer. What would you have to do? First, get a wad of cash: credit cards and checks will be traced back to you. Pay someone - preferably a stranger or homeless person - to buy a smartphone or laptop from a pawn shop or used computer store. If you enter the store yourself, you will be on the surveillance video for the store. Use your device outside the library and use their Wi-Fi out of view of the surveillance cameras.

Is that enough? Probably not. But it's a good start. What is a better way? Use the Dark Web, in the same way American spies communicated with their home team.

Better to Use Tor (the Dark Web)

If you use the Dark Web and avoid the known pitfalls, you can be as anonymous as it is possible to be today. Tails is a USB-based operating system that boots from the USB drive and does not touch the host computer's hard drive, and leaves no footprint revealing that you were even on the computer. Tails can be obtained through `tails.boum.org/` and is free. It is the method recommended by news organizations worldwide for submitting tip information anonymously.

This is my third hack of the Dark Web: helping whistleblowers stay anonymous if they wish.

Media Outlets Use SecureDrop

SecureDrop is Dark Web software that allows whistleblowers to send information to news outlets and exchange messages between the whistleblower and the journalist. Many global news and other organizations use it - the list is found at `securedrop.org/`.

Thorns and Roses

The sweet smell of roses in the world of privacy comes with its own thorns.

Removing tracking from your Internet use by using Tor does give you better privacy. But it can be inconvenient. Because Tor relays are spread out over the world, you might see a French language landing page because the last relay was in a French speaking country. Web pages take more time to load because all the traffic is passing through several additional routers instead of going straight between your browser and the web server.

Loss of discipline in correctly using Tor can leak your anonymity; for example, if you give your real identity to a website.

It's Still Worth It

In spite of these drawbacks, it is necessary and important to support the use of Tor in the protection of everyone's privacy.

Private communications are essential for resistors under oppressive regimes. Syrians fighting Assad cannot use ordinary email systems; they would be found out in no time. Iranians organizing resistance to their government would be wise not to use conventional messaging tools offered by local companies.

Just as free speech is important to a free society, it allows some to express hateful ideas. In the same way, privacy can be used by good people and abused by bad ones. But in the end, the value of free speech is higher than what it allows, and the value of privacy is higher than what the abusers can make of it.

Degradation as DRM

by Nikolaos Tsapakis

Information available is for educational purposes only, views expressed are my own and do not necessarily reflect those of my employer.

Long time ago, while I was searching for interesting Digital Rights Management systems on games, I came across FADE[1]. The protection allows the player to use the game normally. Then it gradually degrades certain game features over time, like decreasing the accuracy of the player's weapons, eventually rendering it unplayable. It seemed to me like an interesting exercise to introduce a similar custom protection as a binary patch in a game. I selected *LZDoom* [2]. After downloading, you need to place a .wad[3] file inside the main game directory in order to start the game.

The idea is to drop the game frame rate on a computer which is different than the game owner's computer based on an event. That event is the player typing the "idkfa" cheat string during game play. A different computer is been detected by the CPUID[4] instruction. That hardware check is not very strict, but I believe it is fine for the purposes of the current article. In order to discover which game code triggers on player cheat string input, I started the game and entered "idkfa", then noticed the string "Very Happy Ammo Added" on top of the screen. Break pointing for read access on that particular string pauses game execution on code which gets executed in an event of a player cheat string input. For dropping the game frame rate, I found the game's main loop and introduced a delay. Delay may be introduced in different places inside the game's main loop.

The file for binary patching is `lzdoom.exe` having an MD5 value of `61a2cd931fd➥3aaaae976e4131c512728`. Binary analysis and patching was done using x64dbg[5]. Running tests between two different computers was done using a physical and a virtual machine on VBox. Following are the patches, description, and file raw offsets to patch. You may use any hex Eeditor to apply the patches.

patch_1:

```
; file offset 0x281FD6
;  goto  patch _ 2  player  cheat
➥string input event check
E9290F4500  jmp  lzdoom _ _ _ _ _
➥prot.patch _ 2
90 nop
continue _ 2  :  <original  game
➥instructions>
```

patch_2:

```
; file offset 0x6D2F04
; save original registers
50 push rax
66:9C pushf
; rax points to cheat string
; compare string with "Very"
813856657279  cmp  dword  ptr
➥ds:[rax],0x79726556
;  if  no  string  matches  then
➥continue game
75  0F  jne  lzdoom _ _ _ _ _ prot.
➥continue _ 1
; if string matches then get delta
E8  00000000  call  lzdoom _ _ _ _ _
➥prot.delta
delta:
58 pop rax
; rax points at the end of data
➥section
48:05 DC745700 add rax, 0x5774DC
; set flag for later h/w check
C600 01 mov byte ptr ds:[rax],1
; restore original registers
continue _ 1:
66:9D popf
58 pop rax
;  execute  stolen  code  due  to
➥patch _ 1
48:8BF8 mov rdi,rax
48:85FF test rdi,rdi
; continue game
E9  AFF0BAFF  jmp  lzdoom _ _ _ _ _
➥prot.continue _ 2
```

patch_3:

```
; file offset 0x253C0
; go to patch _ 4 hardware check
E9  67DB6A00  jmp  lzdoom _ _ _ _ _
➥prot.patch _ 4
90 nop
90 nop
90 nop
90 nop
continue _ 4:    <original    game
➥instructions>
```

patch_4:

```
; file offset 0x6D2F2C
; save original registers
66:9C pushf
50 push rax
53 push rbx
51 push rcx
```

```
52 push rdx
E8 00000000 call lzdoom _ _ _ _ _
➥prot.delta _ 2
delta _ 2:
58 pop rax
48:05 B9745700 add rax,0x5774B9
; check if flag set by cheat string
➥check
; If not set then continue game
➥else check h/w
; processor info and feature bits
8038 01 cmp byte ptr ds:[rax],1
75 17 jne lzdoom _ _ _ _ _ prot.
➥continue _ 3
48:33C0 xor rax,rax
48:FFC0 inc rax
0FA2 cpuid
; If h/w check fails introduce
➥frame delay
81F9 0322989E cmp ecx,0x9E982203
74 07 je lzdoom _ _ _ _ _ prot.
➥continue _ 3
B9 00101101 mov ecx,0x1111000
frame _ drop:
E2 FE loop lzdoom _ _ _ _ _ prot.
➥frame _ drop
; restore original registers,
➥execute stolen
; code due to patch _ 3 and continue
➥game
continue _ 3:
5A pop rdx
59 pop rcx
5B pop rbx
58 pop rax
66:9D popf
57 push rdi ; stolen code
48:81EC 80000000 sub rsp,0x80 ;
➥stolen code
E9 5C2495FF jmp lzdoom _ _ _ _ _
➥prot.continue _ 4
```

[1] forum.exetools.com/showthread.
➥php?t=13232
[2] github.com/drfrag666/gzdoom/
➥releases/download/3.87b/
➥LZDoom _ 3.87b _ x64.zip
[3] github.com/Akbar30Bill/DOOM _ wads
[4] en.wikipedia.org/wiki/CPUID
[5] x64dbg.com

This is a tale of caution. Most all of you hacker-types reading this already know to always wipe any old hard disk before disposal - ideally, multi-pass drive wipes follow by partitioning as a LUKS volume with drive encryption. These baselines are out of scope for this article, to tell you the real story.

When I found this data on the Windows trashed laptop, I wrote my findings in a notebook, then multi-pass wiped the laptop disk. These files were not even deleted, so no NTFS recovery needed to review drive contents.

Enter the Dragon

This tale starts by my walking home from working in a major metropolitan city near the East Coast. Walking along, I saw a trash management employee giving someone else a laptop.

I went over to learn more. Talking to the sanitation workers, they told me people throw away multiple laptops all the time. They noted seeing a dozen laptops a week in the trash, easily. I struck up a conversation and was given a free 17 inch HP laptop running Windows 7 with a dead laptop battery. Two minutes later as I loaded lappy into my backpack, they found a matching power supply. I added that into my bag.

Game On! Time to go home and check this out!

I got home, grabbed one of my favorite Linux Live USB sticks (Ubuntu, Kali, Tails, TempleOS, Hannah Montana Linux).

Once booted up, your favorite hacker mounted the Windows volume, then browsed the "C:\Users\%username%" folder.

These details are facts I obtained. I was so stunned that I called my wife over to confirm this event was real. This is the story of a restaurant with zero data integrity.

The disk was reviewed and wiped in September 2019 (pre-COVID - the world seemed so simple then).

The Goods

I recognized the company name. I ate dinner there a few months ago and laughed

when I recalled why the place sounded familiar.

On the desktop, files of note:

- `check.jpg`: The back of a signed check. Front account and routing numbers visible.
- `HVAC.pdf`: Floor plan for HVAC install.
- `Desktop\Drawings`: Building plans, high definition AutoCAD design files, building engineering documents.
- `Desktop\Employee Documents`: Current and past employee info, full names, driver licenses, scanned copies of Social Security cards, W4, I9, and direct deposit forms.

The archive data went from 2015 to February 2018. Digging more, this laptop had been in use since 2013.

Data, Data, More Data

Found an advertisement for Valentine's Day 2018, food menu specials, and payroll details for January 29, 2018 to February 11, 2018 - names, positions, hours worked, hourly pay, net pay.

- $3.00 an hour for servers.
- $9.00 an hour for bussers.
- $12.00 an hour for counter employee.
- $13.00 an hour for food runner.
- `January 2018 Sales Report.pdf`: $29,101.35 grand total. Including GC, SC, tips $31,882.07.
- Back to the desktop folder, we have `Desktop\Music` which was empty.
- Old Catering Menus. TeamViewer 10 was also installed.
- `Desktop\Permits`: Deck and outdoor business permits. Address of the business owners.
- `Finance Docs`: Scanned checks, client catering agreements.
- `Heather\Bank Statements`: AMEX, PNC Card processing statements going back to July 9th, 2012.
- Equifax report.
- Fire inspection documents.

Pause to reflect. This is a ton of data and I have more. Please wipe business and personal details. I could have committed tons of fraud with this data.

I still have a few more cringe details to wrap this article up. I appreciate your patience as a reader.

- `incident report.doc`
- `insurance questionnaire.pdf`
- Quickbooks (but only has the 2009 templates).
- W2 reconciliation Dec 2015
- Symatec folder with a CD key and a bunch of 80s music.
- Taxes: Tax returns, payroll taxes in .xls files dated from 2010 to 2015.
- `VerizonUSerID.docx`
- Comcast business contract
- Credit card statements.

Some files ask for a password to open, most files do not.

- `discover.csv` (for listing of transactions).
- Residential leases agreements from October 2011.
- `Local Inquirer Ad.pdf` dated January 29th 2012.
- `koldwalkInCooler.pdf`
- `Landlord Letter.docx` (vouching for tenants).
- Commercial construction building contract.
- PR statement from August 6th, 2013 grand opening.
- Zagat 2013 review.
- `Tag Organizer.pdf`
- PNC bank settlement documentation.
- `scan.pdf` (inventory of office cleaning cups).
- Even more direct deposit and bank details found in a bank details folder.
- Health inspections.
- `staff.xlsx`
- `monthly.pdf` (February 2017 generated nearly $80,000 in one month).
- Scanned Documents. 164 files.

Writing this out was longer than I expected. May this article go easy on the *2600* editorial staff. Redact names if necessary, but I felt sharing that I had both owners' names solidifies the concern in the discoveries. *Wipe* and/or encrypt your disks.

Might I suggest amateur forensics to learn more.

Also, if using Linux, create a LUKS volume with an encryption passphrase to encrypt the whole disk. You can then create ext4 data volumes.

12 NEW *2600* T-SHIRTS!

You read that right. We now have an additional 12 (!) shirts in a variety of sizes for your wearing enjoyment.

Each shirt has the full color artwork from one of our covers that was printed in the past three years. People have been asking us to do this for years, but it wasn't until now that we were able to accomplish it in a way that we were happy with. And we're certain you too will be quite pleased with these shirts.

They all contain an entire cover image without any masthead or barcode. Whether you choose the Ukrainian payphone picture, evil social media image, ransomware message, or any of our other designs, we're quite confident that you'll be happy strolling around town wearing what might be the coolest, most provocative t-shirt in miles.

This is also another way of supporting 2600. We intend to design more hacker-related shirts in the months ahead if we get a decent reaction to what we've released so far. Please be sure to send us your feedback!

All shirts can be seen and ordered at ***store.2600.com*** *along with hats and sweatshirts!*

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm on Shaw Island, one island over from the home of ToorCamp, and it is snowing. That's rare here, but it has been an unusually cold winter so far. There have been windstorms and snow and ice, all of which have wreaked havoc on our aging and rickety outside plant. I'm here tasked with figuring out what, exactly, we're going to do about it. Who am I kidding, though? The answer is probably nothing.

A phone line, conceptually, used to be a single copper pair, which ran all the way from your phone to the frame in the central office. In reality, it was far more complicated than that: you owned your inside wiring (which was your responsibility), which would interface with the telephone company's outside plant at the SNI or TNI (typically a box on the side of your house). On the telephone company's side, a drop cable would run from your premises to a splice enclosure (these usually look like a post, serving multiple houses in a neighborhood), which will then connect via a distribution cable to a serving area interface (these are the green boxes you typically see at the entrance to a neighborhood), which then connects to a feeder cable and finally to the central office frame.

So, it wasn't really just one cable - it was a patchwork of cables spliced together, which formed one continuous circuit between your telephone and the central office. That's a long way to push electrons. It might be five miles or more. Both resistance and capacitance exist. Cables are twisted, and this causes further attenuation because the distance is about three percent greater than if cables went straight through. We're also, due to runaway global warming, seeing higher temperatures in the Pacific Northwest than networks were designed for (and this is *every* network, from electricity to cable TV to telephone to wireless networks). In our case, higher temperatures cause deterioration of cable sheathing at an elevated rate. It used to be that five percent of the time, a fault was in the aerial or underground portion of a cable, and 95 percent of the time, a fault was at an interconnection point. That's no longer true; it's now closer to ten percent of the time that the fault is up a pole, or somewhere underground. These faults are harder to find and much harder to fix. Why? Nearly every outside plant component of the telephone system - from poles to cables and beyond - is past its useful life.

What's more, there are capacitors inline throughout the network and, if you own an old electronic device, you have probably experienced a capacitor that has failed from age. This happens in the telephone system too. Fortunately, these failures are easier to find, but due to supply chain disruptions, the parts can be very difficult and expensive to come by. Naturally, phone companies dramatically reduced inventories of spare parts to save money starting in the early 2000s. I have heard of cases where outside plant technicians will, when faced with a shortage of spare parts, borrow capacitors from a part of the network with fewer subscribers (potentially causing an outage) in order to restore service in an area with more subscribers.

Overall, it's really complicated to run a network that is outside in the weather, with trees falling on it and deer pissing on it and the occasional meth head stealing copper from it (yes, this really happens). Funny story about that. One genius thought it was a good idea to cut a 2400 pair PE-89 cable. These are 24

gauge, filled with icky pic, and weigh over ten pounds per foot. When his buddy cut it, it dropped straight down and clocked him in the head, splitting his forehead open. The techs found him in the gutter, bleeding, and out cold. Miraculously, he survived.

If all of this sounds unsustainable, it is. And naturally, the company doesn't really want to invest much (if anything) in fixing problems because the network is obsolete. They don't make money selling traditional telephone service. All of the money is in selling broadband these days, which is not only unregulated, it mostly relies on different technologies. Fiber to the node is going in everywhere. The way this works is that new, fiber-optic cable is run from the central office to each serving area interface, where a DSLAM and SIP gateway are installed. The existing copper cabling is used for "last mile" connectivity to nearby buildings. It sounds great in theory, but this plant is still decades old and has been deteriorating as much as the rest of the network (arguably even more), so it's a stop-gap solution at best. Then again, telecom executives seem to be treating fiber optic cables as a future-proof technology that will never wear out or require maintenance, which is completely inaccurate. The lifespan of fiber optic cable is lower than that of copper cabling! All of this stuff will need to be replaced in 30 years, if technology hasn't already passed us by prior to that.

What's the future? Well, right now, on places like Shaw Island, it's the present, which is essentially the past. This will be among the last places to get much additional investment. There's not much here: a couple of convents, a community center, a ferry dock, a general store, and some houses. It'll be far down the priority list. As beautiful as the place is, I really wonder what I'm even doing here.

A more fun outside plant implementation, operated by phreaks at the ToorCamp hacker camp this year on neighboring Orcas Island, was presented by Shadytel. These folks show up and operate a virtual phone company, offering free landline telephone service allowing hackers to make phone calls from their campsites (assuming they solve a puzzle required to initiate service). Two AT&T Definity PBXs were installed, serving as central offices, one each at upper and lower camps. Two trunks ran between them (T1, digital, for switching between exchanges, using HDSL as transport). This provided both redundancy and spare capacity in the event of anticipated hacker shenanigans (such as attempting to ring every telephone at Toorcamp at once).

For local distribution, T1s were run to multiplexers distributed throughout the camp, which were equipped with line cards (up to six per mux, supporting two T1s in total). Each line card supported up to eight subscriber lines, which were then run over Category 5 cable to distribution points throughout each camping area. From there, campers would run their own phone lines to connect to the network.

Naturally, many of the same problems that occur in the real world occurred at Toorcamp. Splicing caused constant headaches. Splices could get damp, or contaminated with dirt, or attacked by raccoons, and connectivity would be lost - potentially to large parts of camp. Power could be interrupted (occasionally by campers unplugging network equipment to run kitchen appliances). Aging equipment sometimes failed under the extreme conditions. Fortunately, the HDSL equipment was equipped with LEDs to monitor the state, and the equipment was colocated with Shadytel operations. When a connection dropped, it was visibly evident: the LED would turn red. Fortunately, copper theft was never the root cause; hackers are a friendly crowd.

And with that, it appears I have a new nemesis: a squirrel. One has evidently packed a splice enclosure full of nuts, and this is the root cause of the outage I'm dealing with. Have a happy and safe winter, don't forget to check your tires, and let the gentle hum of a dial tone be your spirit guide. I'll see you in the new year.

Friendly Fraud

by Lee Williams

Greetings. Lee the Agent here. By now I hope you can recognize my writing style across editions of this magazine and figure out who I am even though I've been writing under different pseudonyms. Now, let's get to the article.

When someone fraudulently takes money out of your bank account, most of the time you have almost nothing to worry about. The bank, whoever that is to you, is required to keep your money safe. When your money goes missing, the bank is never allowed to say "sucks to be you" and then leave it at that. They *have* to insure your money. Therefore, banks have these processes called "disputes" that allow the customer to get their money back when shit hits the fan. You see a fraudulent charge on your account, you make a dispute with your bank, and if you're being honest, they will place the money back in your account.

This goes beyond unauthorized transactions. If a merchant scams you, you can actually go to your bank and tell them that. If you order two snacks at the vending machine but it only gives you one, you can go to your bank and tell them that. The bank has the option to side with you, and if you're being honest, they will. So I went to the vending machine, bought two candies, but only one came out. I told my bank this, and I received half of the money back into my account. That's when it hit me: I can steal with this. If I can file a fraudulent dispute, I can get away with not paying for shit.

There's one specific bank, the one I bank with, who will *always* side with the customer when dealing with disputes. I'm not going to say the name of the bank, but it's one of the largest banks in the United States. Let's call it Digital Dash National Bank. What this means is that when you file a dispute, nothing else matters; They're on your side. My current love interest has family who actively does fraud with Digital Dash National Bank because the bank just enables it. This happens all the time. People realize that when you dispute a charge you get your money back, so people take advantage of it. They would make huge purchases and then dispute the charge.

I found out that my bank sides with the customer when I bought a partially broken knife at a gas station. It broke the same day I bought it. It was partially functional, enough that I still wanted to keep it. I went straight to my bank to tell them that the merchant (the gas station) sold me a broken product. The man on the other end of the phone told me that they're taking my side, and they always will. My bank, which was actually one dollar in negative balance, had the money spent on the knife back in my account, and I was no longer in debt. But there's a catch.

When you do an honest credit card dispute, you have to also, in good faith, make an effort to resolve the issue with the merchant first. When the merchant *won't* help you, then you make a dispute. But I technically skipped the step of trying to resolve the issue with the merchant and went straight to the bank. My bank was in negative balance. Afterwards it wasn't. The knife was partially functional. I just skipped the step of trying to resolve the issue with the merchant. This is around when I realized what I did was technically fraud. Whoops. Thankfully, nothing ever came of it, but I never did it again.

The merchant, however, is allowed to argue the dispute and keep the money. If they don't make a good argument or don't respond fast enough, the customer wins the dispute. Most banks follow this protocol.

This happens all the time, where people will do fraud without serious malicious intent. Perhaps they did what I did, and just skipped a step with no ill intentions. My goal wasn't to steal from my bank; I just wanted my money back. People will dispute charges by accident, or skip steps, and end up committing a crime. But with my bank, there seems to be no chance of them siding with the merchant in a dispute. So what's stopping me from consistently disputing charges, stealing from both the merchant and the bank, a real 21st century heist?

The Blacklist.

Not many people really know *exactly* how the anti-fraud algorithms work except for the bank. But we all know that the algorithm isn't stupid. There are certain things that we know will tip it off, like having a VPN or your zip code, but there are other times where the algorithm just somehow knows that you're doing something wrong. Among other things, the algorithm pays attention to your disputes, how often they happen, when they happen, and other pieces of context about them. There's really no perfect ratio to successfully do a fraudulent dispute. It's more of a guessing game when your intention is to do fraud.

"But Lee, you said your bank sides with customers all of the time! How will they stop fraud? Why haven't they stopped your lover's family?"

Well, even though they side with you, the algorithm can still figure out you're doing fraud.

Once they finally catch on, risk analysis at the bank determines that you're a threat to them and other financial institutions, so they place your social security number in a database I refer to as *The Blacklist.* Other people also refer to it like that; I just like the dramatic effect of *The Blacklist* in italics. Once your SSN ends up in the blacklist, you won't be able to get approved for a loan or a mortgage, and you won't be able to set up bank accounts. You could end up in that database forever, and you're basically fucked for life at that point, as no financial institution will want you because they think you're going to steal from them.

The reason her family hasn't gotten caught is most likely because they successfully fooled the anti-fraud algorithm. If I'm being honest, I don't know the exact details of what they're doing, but it's definitely more than just disputing charges. Thankfully, I'm not in the blacklist, but I almost ended up in the blacklist one time and can no longer bank with a separate major bank. I'm lucky they didn't sue me or press charges, but at that time they thought it was not a malicious act of fraud, but rather I had gotten scammed so it makes sense why no action was taken. That's not actually true, but I'd rather them think that it is and then close my account.

Here are two real life scenarios:

Scenario One: You go to Walmart in another town and buy a burner phone with cash. Then you walk to a cafe, log into your bank on the burner phone, and purchase a brand new pair of black Air Force Ones. Then, a day later on your main phone, you dispute the charge.

Boom, you're in the blacklist because the algorithm knew that you were up to no good, or you messed up somewhere, or some other reason on the incalculable list of reasons for why it got flagged. Risk analysis deems you a threat, you get blacklisted, and the credit bureaus write your name and SSN down somewhere.

Scenario Two: Your bank is in negative balance. You dispute that meal you ate yesterday, claiming your food never came. The algorithm knew. Risk analysis deems you a threat, you get blacklisted, and the credit bureaus write your name and SSN down somewhere.

There's no way to know if your dispute will blacklist you or not. Once you're in, it's hard to get out and your life will be very difficult from there on out.

That said, the only time you should be worried is if you're doing fraud. And if you do happen to dispute a charge in good faith and the algorithm flags it, you can always make a call to the right people ("the right people" being your bank) and explain the situation to them.

"It's always a challenge hiding something sensitive that you might need quickly. Any hiding place involves a trade-off between security and access. Hide something in the sewer main beneath your floor and it's secure, but good luck getting to it. Hide something in your sock drawer and it's easy to get to but hardly secure. The best hiding places are easy to get to but tough to find. The do-it-yourself versions are known in the spy trade as slicks - easy to slip something in, easy to slide it out." - Michael Weston, *Burn Notice*, Season 2, Episode 9.

As hackers, access is everything. If we can get into it, or at it, we will. It is in our nature. And this isn't always to cause millions of dollars of damage by *looking* at something (also, fu Sun Microsystems). I remember laughing when I first watched *Freedom Downtime* and seeing the scene where the FedEx truck driver found several cases of beer in a drop box, because they use the same combination on all their drop boxes. Funny and entertaining.

On the other hand, I used to do tech support for the Microsoft point of sale systems, and remember one customer that literally built their server *into* a wall to prevent access to it. But this meant when that server was dying (likely due to overheating due to lack of ventilation), it was frustrating and sad because these people were at a high risk of losing the system they used to run their livelihood on.

But it's our very nature as humans to want to keep our own devices and areas restricted to ourselves. Today this can range from encryption programs to hiding a yellow floppy disk in an air vent in our bedrooms. *But* many governments require encryption programs to register a public key with them in order to do business in their country, and if you need to flee quickly, you may not be able to get that disk out.

But one thing that many people overlook is *compatibility* with modern devices. I still have a 512MB flash drive from college that used USB 1.0 to connect to systems, and will still connect to my USB 3.0-only desktop system. Again, we have used this to our advantage (honey pot USB sticks left in parking lots, anyone?). But this means our tech can be plugged into a system used by those we do not want to have access in order for others to access it. I can still access my late 90s/early 00s buggy C++ and Intel x86

assembly programs with no issues. They are also common and easy to pocket and walk away with (who reading this hasn't "found" a USB drive somewhere and then found it later in their pocket?).

Let's look at the retro. CDs and DVDs are great: stable, easy to hide, hold a decent amount of data, but hard to rewrite. Meaning, in most cases, once your data is written, it might as well be in stone. And yes, I know CD-RWs exist, but honestly, I have had nothing but bad experiences with these, and often by the third rewrite the data is so horrible that it might as well be lost. This puts a barrier on data upkeep.

But wait, I mentioned floppy disks earlier. What about them? Can be written to many times, not the largest amount of storage space, and a bit obscure to use (when was the last time you actually needed to use a floppy disk or even found a system with a reader installed?). And many of the older style disks are rather stable and built to last. The ones from the 90s are often where quality was sacrificed on the altar of profits. However, while it will not auto launch, most systems with a drive can read them, and they still make and sell 3.5 inch USB floppy drives.

Well, wait a moment. Only as long as the disk was written in a compatible system on a compatible drive, can it be read. Anyone from the 8-bit or early 16-bit system days may remember that those who used the same OS (say, CP/M) may not have been able to read disks on a different model system despite running the same code. Sure, there are devices that could be attached to increase compatibility, but can we use this to our advantage? Yes, but even some systems back in the day could get around this.

But if we take it a step further, what if the drives were not compatible because they were physically built differently?

Let's take a look at the most popular system ever sold, the ones built for the masses, not the classes? The Commodore line of systems. Their drives were wired differently (for instance, an IBM 3.5 inch disk drive could not be used in the Amiga systems or the 1581 drive without modification because the pin outs were different).

In addition, accessing a disk in a lot of systems is easy. But while many of those in the scene from the later years may or may not have knowledge of DOS commands, how do you access drives on the Commodore? I am sure many of my fellow Boomer and Gen X hackers may remember the `LOAD "*",8,1` command.

And while you can look this command up, again, the accessibility is not there. Not everyone has a Commodore available. Not many people would keep the old while they move to the new. Heck, the first Commodore I bought was just a few years ago from a pawn shop. I got it cheap because they thought it was only a keyboard. This means that many today may not even recognize the system. So, set up right next to my eight core i7 64GB RAM with two terabytes of storage space I have my one megahertz 64K RAM system with zero native storage.

Now, while many may see a gap, there really isn't. I have cartridges and devices I can plug into my C64 to attach to a LAN to access disk image files on my server, or to get onto my network to access BBS systems. I can communicate between systems *with the proper knowledge*.

And even today, people have designed and developed - and *sell* - systems that allow these older devices to work on modern devices. This means I can access and use my Commodore disk drives on that i7 system I mentioned earlier to read and write files if I don't want to hook up the ole CRT monitor to see what I am doing.

Not good enough for you, you say? Lots of people still have disk drives? How about going even older and using cassette tapes? Needing to remember the counter on the tape to find the specific data needed, and it is *slow*! Worried about people getting files quickly? Yea, not happening, they would need to take the tape, and then you may notice it is missing.

Or go the Amstrad route and use the three inch disks, something I do not think were ever really used on IBM systems (which became modern PCs), adding another layer of access obscurity to your security....

So, by embracing the old in the age of the new, I feel secure in my data since many do not know how to use my data or even what to look for. Between the encrypted USB flash drive I always keep on my person to the out-in-the-open "how do I access this stuff" media, I feel relatively secure in my data. Will this keep a determined individual out of my stuff? No. But I have a higher bar than many because of the obscurity of the mix of media I use.

Want more proof that this is not a crazy idea? Until 2019, the United Staes Air Force used eight inch floppy disks to control systems related to ICBMs, nuclear bombers, and tanker support, because the disks were stable and required physical access to the media and drives to interact with, adding a level of protection between those authorized to use the system and those from outside it who should not have access but may want it. And per Lt. Col. Valerie Henderson, spokesperson for the U.S. Defense Department, "It still works."

And yes, my Commodore can run *Crysis*, because I wrote a BASIC program and titled it "Crysis" just so I can answer "yes" to this question.

Current Bulletin Board Systems: How It's Done

by warmfuzzy

Of all the things I've loved and lost, I miss my board the most,

but now it is back online, and this corner of the net is mine,

the speed is a thousand fold, my storage is even more,

I'm back in the scene, behold my 1337 system is hardcore.

- warmfuzzy

Hosting Benefits: Self-hosted systems (full control) vs. vServers (cheap and reliable) vs. dedicated servers (massive capacity and offsite reliability). Recommended home-based systems are the "nano computers" which are very small form-factor systems that you set up and leave to run. vServers are available at IONOS.com, recommended dedicated servers are available at www.hetzner.com. With all of these hosting options, it is fully recommended that you use the Linux operating system, as it is more capable than the Windows or Mac alternatives.

Storage: HDD vs. SSD (SSD gives no speed advantage due to the limits in the Internet service.) "Toasters" are recommended; they are HDD docking stations that look as if the HDD is toast and the docking bay is the toaster. Recommended model is the "Sabrent 4-Bay USB 3.0 SATA 2.5″/3.5″ SSD/HDD docking station (DS-U3B4), which goes for around $100 USD. Recommended HDDs are the Western Digital RED NAS 5400 rpm drives. One thing to note with these drives is that they can get really hot due to the density of the platters, so you may need to buy a fan to cool down the several drives that you should buy. The eight terabyte WD RED NAS drive is recommended, which will cost you around $250 USD or less if you get a deal.

Famous Systems and Personalities:

- *Agency BBS*: Avon, agency.bbs.➥nz:23(telnet) / 2024(ssh)
- *Black Flag BBS*: Hawk, blackflag.acid.➥org:23(telnet)
- *Fishingnet BBS*: warmfuzzy, fishingnet.➥phatstar.org:7777(telnet)
- *HyperNode BBS*: MaxMouse, hypernode.➥ddns.net:23(telnet)
- *KANSIT WHQ BBS*: cr1mson, whq.➥kansit.com:23(telnet) / 22000(ssh)
- *Necronomicon BBS*: necromaster, ➥necrobbs.ddns.net:23(telnet)
- *Raiders Inc. BBS*: cr1mson, ➥vintagebbsing.com:1337(telnet)
- *The Bottomless Abyss BBS*: StackFault, bbs.➥bottomlessabyss.net:2023 (telnet) / 2222(ssh)
- *The Quantum Wormhole BBS*: MeaTLoTioN, bbs.erb.pw:23(telnet) / 45022(ssh)

Echomail Nets (all the below networks use the fresh binkp echomail protocol):

- FSX (Fun Simple and eXperimental), 21:*, Avon, avon@bbs.nz
- AgoraNet, 46:*, Accession, access@➥pharcyde.org
- Retronet, 80:*, necromaster, retronet2016@yahoo.com
- Whispernet, 316:*, cr1mson, cr1mson@➥phatstar.org
- Sp00knet Echomail Network, 700:*, society@phatstar.org
- Fishingnet Echomail Network, 701:*, society@phatstar.org
- The Investor's Network, 702:*, crewmate, crewmate@crewmate.tech
- TQWnet, 1337:*, MeaTLoTioN, ml@erb.pw

Art Groups: Blocktronics (blocktronics.➥org), Impure (and others) (16colo.rs/), and ansigarden.com (custom and stock artwork for a fair fee)

ANSI Editors: PabloDraw (picoe.ca/➥products/pablodraw/), Moebius (blocktronics.github.io/moebius/), and Mystic BBS's Internal ANSI Editor (mysticbbs.com)

Modding Groups: PHATstar Society (phatstar.net), DoRE (*Dreamland BBS*), Phenom Productions (phenomprod.com/)

Documentaries and Commentaries:

- *The BBS Documentary* (www.➥bbsdocumentary.com/order/)
- *Back to the BBS Documentaries* (erb.pw/➥bttb) Al's Geek Lab YouTube also available.
- *TexTalk.news: Going Full-on Mad Retro* (textalk.news), *The Textmode PODcast*
- *Textmode Magazine* (textmodemag.com); a future project that is on hold for the time being.
- TelnetBBSguide.com: The central location for a BBS system directory.

Client Software: NetRunner (www.➥mysticbbs.com), SyncTerm (syncterm.➥bbsdev.net), mTelnet (no link)

Server Software: (all of the below software suites work on both Linux and Windows + Mystic's ARM

- Mystic BBS (www.mysticbbs.com) (straightforward configuration and most modable). Recommended for most users as it is basically plug and play with easy configuration

- Synchronet BBS software (www.synchro.➥net) (easy to use and open source, more difficult to modify)
- Enigma 1/2 (enigma-bbs.github.io/) (excellent for the programming community)

Code Pages:

- CP437/ANSI-BBS (around 250 or so usable "characters" out of 256 characters)
- iCE ANSI (an improved ANSI that offers a greater color selection in place of flashing colors)
- UTF-8 (with foreign language support)
- ASCII (plain and simple text based communications)
- Rarely used protocols: AVATAR, RIP

Plain Old Telephone System:

- SEXPOTS: Synchronet External Plain Old Telephone System. Allows you to receive connections from the POTS and redirect it to any arbitrary Telnet BBS server, works on Linux and Windows.
- Connect your favorite RS-232 US Robotics 56k v92 vEverything External Modem via Serial to USB 2.0 conversion cable. Recommended cable: DTECH USB to RS232 DB9 serial adapter cable 16 with FTDI Chip, DB9 9 Pin USB 2.0 (a converter adapter with the FTDI chipset) which will cost you around $20 USD for a 16 foot cable. Recommended modem: US Robotics 56k vEverything external serial modem which costs around $30 USD plus shipping from eBay.com.

Connection Protocols:

- TELNET: plain text with no encryption, very easy to "sniff" the traffic. It's recommended for speed, but should have no function to login to system functions or the sysop password could be sniffed.
- SSH: commercial-grade cryptographic protocol. Can easily be added to Mystic BBS with a free crypto library.
- RLOGIN: not used very much, but is an alternative for non-standard setups. It is used to connect to the Doorparty door game server.
- RS-232/Serial: the protocol used by POTS modems going into the connecting computer.

Instant Messaging:

- Multi-Relay Chat: at the time of this writing there are over 100 boards that are connected to this instant messaging service. It works quite well and has been a boon for the scene, however there is currently no secure communication capacity in the present version. To fix this gap in secure chat is MeaTLoTioN's Matrix server which is end-to-end encrypted (riot.erb.pw).

Fun Times:

- *[P]hone [i]n [M]y [P]ocket BBS*: MeaTLoTioN's BBS running off of his Android phone Pimpbbs.erb.pw:18023 (telnet) PIMP BBS: *"No pocket fluff was harmed in the making of this BBS."* -ML
- File Servers: BBSes can now connect to file servers through the TELNET-OUT function available in modern BBS software. You connect to your favorite BBS system, go to the "file area," select the server of your choice, telnet with the push of a button to that file server, and you're good to go. Systems include Anonymous Archivers File Distro Network (phatstar.org), Silent Partner FDN (phatstar.org) accessible from AAFDN, and ArchaicNet FDN (sysop@➥archaicbinary.net).
- Door Game Servers: You can now play online games with thousands of others using a game server where people can log on to a BBS, open the game server portal, and be presented with many dozens or hundreds of games, having all those games in one spot to play with fellow gamers on a single system. BBSLink (bbslink.net) and DoorParty (www.throwbackbbs.com/).
- Quantum Radio: The scene's Chiptunes and Tracked Music streaming radio station (radio.erb.pw/).
- The Weekly MeaTup with MeaTLoTioN on Multi-Relay Chat (MRC) at 20:00 UTC on Fridays. MRC is accessible from BBSes that have the MRC BBS mod installed; this works on all the major BBS software (www.➥meatlotion.com).

ARE YOU READING THIS ISSUE ON A KINDLE?

There is important information for you in the editorial ("Inconvenient Truths")

Intercepting Google CSE Resources: Automate Google Searches With Client-Side Generated URIs (for free)

by Renan de Lacerda Leite

From an OSINT perspective, Google Search has been an indispensable tool for collecting data about companies, sites, persons, leaks, i.e., any kind of relevant information for countless investigation purposes. Although mostly used by analysts on targeted research, there are actors who would take advantage of developing a fully automated discovery process using Google's search engine as one of its most important sources of data.

Nowadays, Google already offers to the public a service that facilitates the development of automated searches, which is called Google's Custom Search JSON API. In order to use it, one needs to create their own Programmable Search Engine - a very useful Google service, created to help developers embed Google search boxes in their websites, increasing their users' experience by helping with more focused searches - and they must ask for an API key to consume Google's JSON API. However, this API has some free usage limits: after making a hundred (100) queries in a day, you'll be charged a fee of five American dollars per 1000 queries, limited to 10,000 queries a day if one does not want to use their restricted JSON API version.

That's where this article comes in. Exploring a client-side generated API URI, it was possible to consume Google's API data without needing to use any personal CSE API key and, consequently, without being charged for queries, as we avoid its traditional JSON API methods.

In order to consume this observed Google CSE API, a Python proof of concept module named CSEHook was developed, with the help of libraries such as Selenium Wire (a library that enables access to the underlying requests made by a browser) which was used to intercept Google CSE API URIs, requests (an HTTP library) to consume the content of those previously intercepted URIs, and other publicly available resources.

Thought Process

Google's CSE, now called Google's Programmable Search Engine, is not news anymore. It's already well known by web developers who use it to embed Google search iframes in their sites' pages, investigation actors who want to search predefined focused domains in order to collect particularly interesting data, and other kinds of individuals and professionals. This is a useful, widely spread public tool, first made to facilitate the embedding of Google search boxes in sites and the use of more specific, personalized, and focused search engines, but which happens to be an incredible tool for people who have a ton of research work to do.

Despite being truly helpful on its own, there are some things in its bundle that are not so handy for people who depend on heavy automated tasks to do their job: the CSE JSON API limits. For this reason, attempts to find alternative paths, for curiosity purposes, were made in order to contour those obstacles.

All the demonstrations were made with a personal Programmable Search Engine, focused on searching terms on Pastebin site pages.

Observing how the client-side of a Google CSE URI interacts with Google's backend resources, a couple of interesting behaviors were noticed when a query is made:

- A request is sent to an ads URI (`cse.➥google.com/cse_v2/ads`), which responds with advertising content.
- A request is sent to an element's URI (`cse.➥google.com/cse/element/v1`), which responds with text content containing a function call that takes a JSON object as an argument.

Even though the Ads interactions could be consumed and parsed to some extent, what really calls the attention is the second behavior. The response contains a call to a client-side JavaScript function, which receives a JSON object that was sent to the client from a Google server. This function will parse the JSON object, which will always contain up to ten search results at a time (per page), up to ten maximum distinct pages, and exhibit the results in the CSE page that is being used.

Despite the frontend generating an individual URI for each performed query, what was noticed is that those URIs could be reused to query different terms, i.e., there was a possibility to later automate the collection of data by intercepting the generated URIs, changing their query strings, and then requesting new results and parsing the collected content. In order to achieve this, CSEHook was developed.

As the content to be consumed is a response of a dynamically generated URI that depends

on the execution of client-side JavaScript to be generated, it would be useful to use a browser instance in order to generate those interesting URIs. The traditional Python solution to this kind of issue is generally Selenium; however, Selenium alone would not be able to track those client secondary network interactions that need to be intercepted. That is why the Selenium Wire, an extended version of Selenium that monitors the requests that were made by the browser instance, was chosen to help in the effort to catch those URIs.

A ChromeDriver will be needed so the Selenium Wire library can do its work. This driver should fit the installed Google Chrome browser version (used version: 91.0.4472.114 for x86_64).

Additionally, Geonode proxy service was used in order to avoid Google's detection systems and diffuse the requests made to its resources. This was implemented because, during the first implementation tests, it was observed that those URIs had a specific limitation to the amount of requests that could sequentially be sent to it. Apart from limiting the quantity of requests made to those dynamic URIs by re-intercepting those resources from time to time, it was preferred to spread the source IP addresses' geolocation that would be sending those requests as well.

Also, to avoid User-Agent pattern-based detections, a list of Google Chrome User-Agents was picked from tamimibrahim17's repository. This list was utilized in order to randomly choose a User-Agent and place it in the request headers just before sending a request to Google's resources.

Finally, to prove that it would be possible to surpass Google's official CSE JSON API limitations with the approach of this article, the Python library named English-Words was chosen so it could be demonstrated that the CSEHook proof-of-concept could effectively iterate through all sets of English words in a relatively short time, i.e., searching lowercase English words in order to obtain results from the already created Programmable Search Engine without calling Google's detection system's attention.

All the previously specified libraries and resources can be found in the References section. A link to their own respective websites was left there as well.

PoC Structure

To achieve the data collection intentions cited before, the project is structured in the following way:

- A config file, which contains some of the PoC configuration variables.
- A driver directory containing ChromeDrivers for Mac, Linux and Windows operating systems.
- A CSEHook directory, which contains the proof-of-concept necessary modules. Here are found a utility class named WiredDriver, which interacts with Selenium Wire library and ChromeDrivers, and the main CseHook class which contains the main PoC code.
- A *__main__* file, which has instantiations to the previously named classes and iterations through the English Words set in order to search those words with the intercepted Google's URIs.

This structure can be better visualized at the project's GitHub repository.

Configuration

The configuration file has the following variables in it:

- *CSE_URI*, which is the URI of the previously created Programmable Search Engine.
- *DEFAULT_DRIVER*, which is the file path to the downloaded ChromeDriver.
- *USER_AGENTS*, which is a URI to the Chrome User-Agents of tamimibrahim17's project.
- *RENEW_CSE_DEFAULT*, which represents the amount of requests the application can do with the five intercepted Google client-side generated URIs. When the application reaches this limit, it will make more requests to the Programmable Search Engine URI in order to collect new client-side generated URIs. This is tunable, but Google will ban the main Programmable Search Engine URI searches if too many requests are made to the same client-side generated URIs, so this must be kept in mind before altering this configuration.

Wired Driver

This is the class that interacts with the Selenium Wire library. Not too much to detail: an instance of this class will be used in order to interact with the Google Chrome browser so it can be possible to intercept the client-side generated URIs.

CSE Hook

Here is where the main logic is placed. Its explanation will be broken in different fragments in order to detail its functionality.

The class has three internal inherent attributes that do not depend on its initialization:

- *_MAX_PROXY_RETRIES*, which establishes the amount of request re-attempts it could make with the in-memory previously downloaded proxies before requesting for new ones to GeoNode.

- *_STANDARD_SLEEP*, which is just the amount of seconds it would keep sleeping if, and only if, Google expires the client-side generated URIs before the application renews it, which would be unexpected behavior.
- *_TIMEOUT*, which is just the amount of time the Requests library should wait for a response while requesting with proxies.

Inside the class initialized components, there are the following attributes:

- *self._amount_of_words*, which specifies the amount of words to be queried to the main Programmable Search Engine in order to collect the same amount of client-side generated URIs, i.e., if it searches for five words - which is its default value - it will search the main URI five times and intercept five different client-side generated URIs.
- *self._word_size*, which is the amount of characters each randomly generated searched word would have in order to obtain the client-side generated URIs.
- *self._cse_uri*, which represents the Programmable Search Engine URI that will be used so it can intercept the client-side generated URIs.
- *self._is_cse_uri_valid*, which checks if the specified URI is a valid Programmable Search Engine URI.
- *self._wired_driver*, which just saves the specified wired_driver instance.
- *self._cse_api_pattern*, which is a pattern for the first URI characters of the targeted client-side generated URIs so it can identify those URIs in the intercepted URI's list of the Selenium Wire instance.
- *self._cse_regex*, which is a regex that will form the groups necessary in order to catch the JSON inside the JavaScript function call of the client-side generated URI response.
- *self._cse_api_uris*, which is an empty list that will contain the client-side generated URIs intercepted by the code.
- *self._pages*, which just maps the page labels with its *start* required offset.
- *self._proxy_list*, which receives the results of *self._config_proxy_list*, a method that is responsible for requesting GeoNode for new proxies.

The next four methods listed inside the class are responsible for the following activities:

- The method *self._get_modified_uri* is responsible for parsing the received URI and returning a string which is a modified version of the same URI. The query parameters *q* (query) and *start* (start offset/page) are the ones that are changed by this method.
- The method *self._config_proxy_list* is responsible for requesting GeoNode for new proxies. It will return the list of data offered by GeoNode's endpoint.
- The method *self._get_random_words* is responsible for yielding randomly generated words on demand, based on the previously defined attributes *self._word_size* and *self._amount_of_words*.
- The method *self._config_new_cse_api_uris* is responsible for configuring the intercepted client-side generated URIs. It will: iterate through the words yielded by *self._get_random_words*, modify the Programmable Search Engine URI using *self._get_modified_uri* in order to place the word in the *q* query parameter, use the modified Programmable Search Engine URI to query a word just to intercept and collect the client-generated URI, and append the found client-generated URI to the *self._cse_api_uris* list.

The fifth method is called *self._get_response*, and its responsibility is to request an endpoint using the specified URI, headers, and proxies. If the request raises a timeout or any other exception, it will check if the amount of retries - which is passed as an argument as well - has achieved its limit. If this limit is achieved, it configures *self._proxy_list* with a new proxy list retrieved from GeoNode.

The sixth method is named *self._search_page*. This method receives the arguments URI, query, and page and returns the JSON retrieved from the modified client-side generated URI response, i.e., the results from Google that it wants to collect with a specific query term.

This is the most complex method of the class, and what interacts with most of the other already declared methods.

While the response is not received from Google, it will: select a random User-Agent and define it in the request headers; choose a random proxy from the *self._proxy_list*; form the proxies dictionary with the information of the *chosen_proxy* so it can be used with the requests library; get a response using the method *self._get_response*; if the response is not satisfactory, it will pop the *chosen_proxy* from the *self._proxy_list* and increase the *error_count* by one and will continue the loop. The *error_count* is the value passed as the argument *retries* of the *self._get_response* method.

If the response is received, check if the *status_code* of the response equals 403 (HTTPStatus.FORBIDDEN). If it does, return

a dictionary with the key-value pair. If it does not, find the JSON inside the client-side generated URI response with the *self._cse_regex* compiled regex, catch it, and assign it to *api_json*. After assigning, return *api_json*.

The last method of the class is named *self.search*, which is the only public method of the class - and the one that is used by *__main__*. This method receives both *query*, the term that one wants to search using the client-side generated URIs, and *renew_cse_uris*, which is a boolean that determines if the client-side generated URIs should be refreshed as arguments.

The responsibilities of this method are the following:

- Quote the received query string so it can be correctly placed in the client-side generated URIs.
- If the *self._cse_api_uris* list still has no

```
def search(self,
           query: str,
           renew_cse_uris: bool = False) -> _GoogleCSEIterator:
    """Get Google CSE results using our CSE API URIs.

    Return: an iterable object with all available Google CSE pages.
    """

    query = quote(str(query))

    if not self._cse_api_uris or renew_cse_uris:
        self._config_new_cse_api_uris()

    first_page = self._search_page(
        random.choice(self._cse_api_uris), query
    )

    error = first_page.get("error")
    while error:
        # If we were temporarily banned, return False.
        if isinstance(error, str):
            return False

        # If old CSE API URIs start to fail, refresh them.
        sleep(self._STANDARD_SLEEP)
        self._config_new_cse_api_uris()
        first_page = self._search_page(
            random.choice(self._cse_api_uris), query
        )

    first_result = iter((first_page.get("results", []),))

    if len(first_page.get("cursor", {}).get("pages", [])) <= 1:
        return first_result

    # If more then one page available, yield them all on-demand.
    yield from chain(
        first_result, (
            results
            for p in tuple(self._pages.keys())[1:]
            if (
                results := self._search_page(
                    random.choice(self._cse_api_uris), query, p
                ).get("results", [])
            )
        )
    )
```

The last method of the CseHook class

client-side generated URIs or if it is explicitly told to renew them, execute *self._config_new_cse_api_uris* so it can configure new intercepted client-side generated URIs.

- Request the first page using the *self._search_page* method. The arguments passed to *self._search_page* will be a client-side generated URI randomly picked from the *self._cse_api_uris* list and a quoted query string.
- If the first page already returns an error key, it can mean two things: the Programmable Search Engine URI was temporarily banned or the client-side generated URIs got old and need to be renewed. If the main Programmable Search Engine URI was temporarily banned, return False and pause execution. If the client-side generated URI just got old, renew them and request for another first_page.
- If the cursor returned by the first page says that only one page is available, return an iterator with the results of the first page. If there are more pages to iterate through, proceed with execution and yield the iterator with the first page results plus an iterator with the results for the next pages - only if they return more results.

```
from random import randint, shuffle
from time import sleep

from english_words import english_words_lower_set

from config import CSE_URI, RENEW_CSE_DEFAULT
from csehook import CseHook, WiredDriver


if __name__ == "__main__":
    wired_driver = WiredDriver()
    amount_of_requests = 0
    try:
        cse_hook = CseHook(CSE_URI, wired_driver)

        english_words_list = list(english_words_lower_set)
        shuffle(english_words_list)

        # When reaches 0, its time to renew client-side URIs.
        requests_to_reload_cse_uris = RENEW_CSE_DEFAULT

        for word in english_words_list:
            if requests_to_reload_cse_uris <= 0:
                pages_results = cse_hook.search(word, renew_cse_uris=True)
                requests_to_reload_cse_uris = RENEW_CSE_DEFAULT
            else:
                pages_results = cse_hook.search(word)

            # It returns bool (False) if temporary ban was imposed.
            if isinstance(pages_results, bool) and not pages_results:
                break

            for results in pages_results:
                print(results)
                amount_of_requests += 1
                print(amount_of_requests)

                requests_to_reload_cse_uris -= 1

    finally:
        print(f"Number of requests: {amount_of_requests}")
        wired_driver.instance.close()
```

__main__ file content

Now that all the attributes and methods of CseHook were detailed, there is only *__main__* left to explain.

Main

The *__main__* file contains the instantiations made to WiredDriver and CseHook, along with a few more things.

The following activities are present in this file:

- A WiredDriver instance is created.
- An *amount_of_requests* counter is initialized as zero (0). This will serve to count the amount of requests made to client-side generated URIs and to exhibit the number at the terminal, so the amount of requests can be monitored without needing to store all the results locally.
- A CseHook instance is created by specifying a previously created Programmable Search Engine URI and a WiredDriver created instance.
- A list containing the English words in lowercase is initialized and shuffled afterwards.
- A *requests_to_reload_cse_uris* counter is initialized with the *RENEW_CSE_DEFAULT* (38) configuration value. This will serve as a negative counter so it can ask the CseHook.search method to renew the client-side generated URIs (intercept new ones and save them in a class list).
- Like cited previously, if the *requests_to_reload_cse_uris* count reaches zero, renew the client-side generated URIs and set *requests_to_reload_cse_uri* to *RENEW_CSE_DEFAULT* again. If it is still bigger than zero, proceed requesting with the already intercepted client-side generated URIs.
- If the returned *pages_results* is False, break the execution because the Programmable Search Engine was temporarily banned. If it is an iterator, proceed with iterations.
- For each iteration made through *pages_results* - i.e., for each requested page, print the page results, sum one to *amount_of_requests* and print the variable value. Next, after requesting a page, subtract one from *requests_to_reload_cse_uris*.
- When the code is interrupted, print its final *amount_of_requests* number.

Obtained Results

To prove that the intercepted client-side generated URIs could be explored on a large scale, the code was left running for 24 hours to see how many requests could be made without interruptions or banishments within

that time frame.

Surprisingly enough, even though GeoNode proxies were used - and a lot of them were not even functioning correctly, which delayed the amount of iterations/requests that could be made in the same time frame without these obstacles - 15,706 requests were made to Google resources, all of them containing real and valid Google results just before the execution was interrupted. It means that the PoC would iterate through all the lowercase English words in less than two days - given that the set has 25,480 words in it.

It also means that it has surpassed the daily quota limits (10,000 a day maximum) allowed by the official Google CSE JSON API - the one without Restricted JSON - by a lot, and surpassed even more the Google CSE JSON API free usage limits (100 a day maximum).

Conclusion

The PoC demonstrated that, within a time frame of 24 hours, 15,706 requests were made and successfully returned Google CSE page values using the intercepted client-side generated URIs as a facilitator, in order to obtain JSON format results. With basic user-agent randomization, client-side generated URIs' frequent renewal and proxy changes, one could avoid Google's detection mechanisms and consume its data without the need to subscribe for its JSON CSE API fees.

References

Selenium Wire: pypi.org/project/selenium-wire/
Requests: docs.python-requests.org/en/master/
User-Agents: github.com/tamimibrahim17/List-of-user-agents/blob/master/Chrome.txt
Geonode Proxies: geonode.com/free-proxy-list
Google CSE: programmablesearchengine.google.com/about/
English-Words: pypi.org/project/english-words/
Regex101: regex101.com/
Custom Search JSON API rules: developers.google.com/custom-search/v1/overview

The Infosec Professional Song

by aestetix

This should be sung to the tune of Gilbert and Sullivan's "Modern Major General"

I am the very model of an infosec professional
I've mastered all security, from digital to physical.
My expertise and training can tell if a threat is credible,
And I'll ensure that my exploits are plausibly deniable.
Blue Team hackers always try to hold bad guys accountable,
In this my record of success is really quite remarkable.
When playing CTF it's true that my teams almost never lose
Because I always know the best and latest hacking tools to use.

It is important that my skills are always up to date and thus,
I passed my CISSP in record time with little fuss.
In short, in making things secure, from digital to physical,
I am the very model of an infosec professional.

I turn on stack protection when I set up a new Linux box
My SSH port knocking sequence comes from Russell's paradox
I'm fluent in syscalling and can speak directly with D-Bus
I write C code with objects and I only need a single plus.
My custom CFLAGs harden code to make the strongest binaries
My system structure layout is superior to systemd's!
I'm so elite that often times my daily life can be a bore -
When I get sick of normal work, I hexedit my Linux core.

I used to be a cracker once but I decided to reform
So now I spend my day job reading Hacker News and Packetstorm
In short, in making things secure, from digital to physical,
I am the very model of an infosec professional.

The Hacker Perspective

by m0xya

I have always known from an early age that I was different, that I (as others have so eloquently put it) was "not normal." My interests from an early age were different to my peers; they were mainly technical in nature. My father was an electronics engineer and the house was always scattered with devices and piles of components. I grew up surrounded by soldering irons, oscilloscopes, and bundles of wires.

He also had a garage/workshop where he had a machine shop. He would tinker away rebuilding cars, boats, even an airplane at one time. Let me tell you, every house should have a lathe. They come in very handy.

I was always encouraged to have a go at things, to play with the tools and equipment, even when I had no idea what I was doing with them. I was always carefully watched, but I was free to play, free to try things, and to make mistakes. I was lucky enough to have been born before the blight of helicopter parenting, where all risks are mitigated and environments sanitized to keep children safe. It was not that my parents were uncaring; in fact, it was quite the opposite. They understood the need for space to grow and gave it to me in abundance.

This level of freedom was very different when compared to some of my friends and their families. However, for me at the time, I did not know any different. Many of my friends had their childhood micro-managed and planned out. I doubt my parents actually knew what they were doing; they were doing what felt right and natural. I was given the space to develop in my own time and in my own way.

One of my very early memories was from Christmas 1981. I was about four years old, and my parents had bought me a Sinclair ZX81, the one that came as a kit and needed assembling. I knew it was from them and not Father Christmas, for two reasons. I knew where things were hidden, as I had found the hiding place one day when exploring. Also, receipts were kept on a spike on their desk, and I could read.

So there I am on Christmas morning, surrounded by small bags of components and with a soldering iron in my hand. My father talked me through what each of the components were and how they worked in very basic terms. I was four after all, and it didn't make much sense to me, but I knew even then that it was fun and that I wanted to know more. It was my first computer and I had built it myself. I would play on it for hours and hours. Typing in example programs from the manual, making mistakes, and trying to work out what had gone wrong. They were my first steps into the world of computing.

In the years that followed, I progressed on to other computers, a Commodore VIC-20, a BBC Micro Model B, and a BBC Master 128. Looking back on it, neither of my parents had particularly big incomes and so must have scrimped and saved to buy these for me. In the early 80s, there was a big drive by the British government to train the next generation in computing and, thanks to my parents, it paid off.

Academically, I suppose I was middle of the road, with a "could do better" being the usual feedback from my teachers. I enjoyed school, with science and math being my favorite subjects. I was also quite good at art and design. Despite all this, I felt detached from my classmates and teachers. I had a constant sense of alienation, that something was wrong. That same feeling of being different, of not being normal.

Even then, I could see what was happening. We were being taught to pass tests, not to think for ourselves, not to question. We were pegs, slowly forced

into the uniformed rack of society. Anyone not quite the right shape would be smoothed out. They would have their rough edges knocked off as they passed through the system. The others who did not fit in were abandoned.

I managed to get into college and university, however, the system was still the same. You fit in or you failed. That sense of being different peaked at university. It had a massive impact on my confidence. That daily reminder of not being good enough, of not meeting expectations, of not being like the others, not being normal. It put me off formal education of any type. It was obvious it worked for the majority, but utterly failed others.

I graduated, just. I have never looked back....

It is at this point I must introduce someone else who had a major influence on me. One of my oldest friends lived nearby in a big old house with his parents and three older brothers. It was always a busy and noisy place, with each member trying to outdo the others. In the middle of this whirlwind of chaos was a very quiet man, my friend's father. He was a medical doctor; however, at the time he ran the medical computing department at Manchester University. He was mildly eccentric and massively into computers. He always reminded me of Doc Brown from *Back to the Future*.

He was also an amateur radio operator. He had huge antennas hanging off the roof and feeder cables running throughout the house. I would spend countless hours sitting on a stool next to him, watching what he was doing. I can still recall the peace and quiet of his room, while from every other direction there was madness and noise. It was an oasis of calm and computers.

You can understand my annoyance then, when at regular intervals my friend or one of his brothers would come rushing into the room saying something like "Come on Dad, he doesn't want you boring him to death." I would be dragged away to do something else, to play a game or run around making noise. I was not bored, I was enthralled, and when I had the opportunity I would sneak away and head back.

At the time, it did not dawn on me, but my friend and his brothers were revealing more about themselves than they realized. They found what their father was doing to be boring and uninteresting, so therefore, so should I. How wrong they were.

Both of these men, my own father and my friend's, gave me the opportunity to explore technology without it feeling like a lesson. I could work things out in my own terms and at my own pace. I could try things out and make mistakes.

It was not until I left formal education that I actually started to learn things. I could study what I wanted, how I liked, and in my own way. There were no teaching plans or targets to reach, no exams to pass. Just learning the way it is meant to be. Fun.

From the age of about 21, I studied whatever subjects and ideas I wanted to. I read up on massively varied subjects: art, medieval architecture, physics, psychology, anything and everything that interested me. However, there was always one subject which drew me in more than any other: computer science.

I had always had a computer of one sort or another, and it had never even dawned on me that I should study it at college and university, something for which I am eternally grateful. My love of the subject would have probably been killed by the formality of education.

You see, I do not learn by rote. I need to understand at a fundamental level what it is I am trying to learn. I am reminded of something Richard Feynman once said: how you can be taught the names of a bird in every possible language, but that you will still not know what the bird is. All you have is its name; your knowledge of the bird is still the same. I need to know more than just the name of a thing.

It is at about this time that I got my first job as a programmer. The interview did not initially go too well. One of the interviewers did not understand how I could do the job without a university degree. He was so blind to the possibility of someone being capable of learning independently that he voted against me. Luckily for me, there were others on the panel who did not share his point of view.

I had been able to answer most of their questions. However, the thing that

gave me the edge, the thing that tipped the vote in my favor was my ability to draw on other subjects. If I had been formally educated, the path would have been narrow. Learning objective A leads on to B and C, etc. During the interview, I had discussed in detail many different technologies and applications. I was not blindly following the path of ABC. I could see connections that were not obvious, as I had both a deeper and broader understanding of the subject. I knew more than just the names of things and their order.

This technique of learning has stood me in good stead and I have not stopped in my quest for knowledge. If anything, it has accelerated since then. It has been almost 20 years since that first interview. I have moved on; I have never stopped learning new things.

Despite not having any formal education in computer science or engineering, I am currently working as a senior security consultant for a global cyber security company. I am drawing on an eclectic range of skills and knowledge that I gave to myself. This allows me to work on a vast range of jobs, from infrastructure and web app reviews to hardware and reverse engineering. I am surrounded by a group of colleagues who all share similar interests and ideas. It is a great mixing pot of knowledge and experience.

Do I still have that sense of being different? Yes.

Do I still have that sense of not being good enough? Yes.

Let me share with you a little secret. It is the same secret most of my colleagues share, but would be unwilling to admit to. That feeling of inadequacy never leaves you; it is always there. It even has a name: "impostor syndrome."

However, it is how you manage this condition that is important. You could give up and accept the fact you don't know enough. You could pretend to be like everyone else and hide away in the crowd. Keep your head down and let that feeling of resentment grow.

Alternatively, you can use it to your advantage. So what if I don't know enough? I can learn new things. Thank you for highlighting that gap in my knowledge. Tomorrow I shall come back knowing more than I do today.

I shall finish off by leaving the reader with a few words of advice. Make of them what you will. They have served me well.

I forget its origin, however, there is a rule I try to follow: "You should always try to be the person in the room with the least knowledge or experience."

That way, you always have the opportunity to learn from others. If you're the master holding court with a room of minions, what chance do you have of growing or learning? Yes, it is a great ego booster but, other than that, I see no benefit.

Try to let go of your ego and let humility be a guiding force. I have noticed as I have aged that being humble opens more doors than it closes. Humility is not to be mistaken as being weak - far from it. The stronger you are, the less you have to prove yourself. You also have a greater chance of people opening up to you and sharing, be that experiences or knowledge.

Accept the fact that you will never know everything (see humility). It is a thrilling sensation, as it means you will never stop learning.

Above all, be yourself. Do not worry what others think of you. Most of the time people are only thinking about themselves, not you.

If you are presented with a problem with no obvious solution, don't worry about thinking outside the box and making alternative suggestions. That ability to think differently, to step back and see the big picture, to not be normal gives you the edge.

I embrace my difference.

m0xya (Phil) works/tinkers at a global cyber security company. He is a HAM radio operator, and in his spare time enjoys repairing old computers and Land Rovers. More information can be found at: https://m0xya.net/

HACKER PERSPECTIVE *SUBMISSIONS STILL CLOSED - STAY TUNED!*

YouTube Is Not a Safe Space

by Men Without Hats

The last few years have been extremely stressful. Given all the scary things going on in the world, sometimes we need levity and a good laugh. To this end, there are a number of themed channels on YouTube, one of which produces family friendly pranks. Recently, no videos from that prank channel were showing up in the general feed. Upon deeper inspection, it turned out that the YouTuber running the channel had had his most recent video flagged by YouTube for not being "safe." The algorithm had determined his video contained both sex and nudity, although it clearly had neither. He appealed, hoping for some common sense, and within 15 minutes the appeal was denied. He expressed a lot of frustration at this, including doubt that a live human had actually reviewed his appeal. He then declared that, after 15 years on the platform, he was jumping ship to another video platform that was algorithm-free.

While the impact of algorithms is not limited to this YouTuber, and seems to be non-partisan and non-opinionated, it is the latest in a decades-long series of attempts to "solve" complex problems with simplistic solutions that look good politically but have all sorts of far reaching negative consequences. In this article, we'll take a look at this history, then at the actual problem YouTube is trying to solve, and see if we can come up with any alternative solutions.

In the 1980s, according to right wing media and talk radio, Satan worship among teens was on the rise. There were allegations of hidden messages in rock music, including rumors that if you played the B-side of a record backwards, you would hear a personal message from the Devil. In response to this "Satanic Panic," Tipper Gore (wife of former Vice President Al Gore) spearheaded an initiative called the Parents Music Resource Center (PMRC) in 1985. The idea was to place labels on rock music to warn parents that it included lyrics that were explicit or worse, so that parents would be able to protect their children from Satan worship.

Naturally, musicians revolted, angered that government imposed labels on their lyrics (their free speech) were preventing sales and creating unfair judgments on their words. This led to a congressional hearing in which musicians such as Frank Zappa brilliantly stated their cases for free speech and made suggestions on how to solve the issues at hand without compromising their art. While the legacy of these hearings left us with the now-familiar labels on music CDs noting explicit lyrics, this is by no means a settled matter, and the arguments at play then are completely applicable today. Ironically, the hearings are also available on YouTube.

The ugly head of "save our children" reared itself again in the 1990s with the rise of underground raves. At the dawn of rave culture, we saw free expression in the form of music, art, and in many cases, free love. Soon, another kind of freedom arrived: drugs. While the vast majority of people were responsible with their use (or non-use) of drugs, a small minority suffered high profile overdoses and even deaths. This terrified parents, who did not want their children doing drugs, and the parents demanded accountability from their politicians. As a result, strict laws began going into place to punish not only the organizers of raves where drugs were used, but also the venue owners, who often did not know the nature of the events. One of the final results was the RAVE Act, passed in 2002, which remains a prime example of a government overreach that is destructive in the name of safety and causes many more problems than it solves.

It's also important to recognize that during this time, the rave community developed a number of self-policing solutions, such as ensuring event organizers had basic CPR training. There were even community-run organizations like DanceSafe that did pill testing at raves to make sure the drugs did not contain poison. A key lesson emerged during this time: many people wanted to use these solutions and claim that they were practicing "safe" drug use. However, others recognized that there is no such thing as safe drug use, and coined the phrase "drug harm reduction." This small but significant clarity of language recognizes an important truth from which YouTube could surely benefit.

Finally, we need to state that those who forget the lessons of the past are doomed to repeat them. After 9/11, many extremely absurd and unconstitutional laws were passed in the U.S. to "keep people safe," including the creation of the Department of Homeland Security, which included the TSA. If the end goal of the TSA is to ensure that airports and air travel remains a "safe space," it is one of the greatest failures of domestic policy in American history. In addition to the endless absurd rules, such as checking ID (challenged in court by John Gilmore),

taking off shoes, or not allowing "liquids" to pass through security checkpoints, the only thing the TSA has been successful with is ensuring that air travel is an absolutely miserable experience that brings lots of profit to corporations funding ineffective security machines at taxpayers' expense. If we attempt to make sense of the endless spider web of contradictory and ever-changing regulations, we are looked upon with suspicion by contracted goons who LARP as law enforcement and somehow have the power to deny our ability to fly on a whim. Another fine example of extreme over-correction in the name of "safety."

We can see from this historical account that what YouTube is doing is not new, but simply the latest in a long line of hammers trying to smash anything that looks remotely like a nail. But in all of this, it's important to ask what a "safe space" is. Perhaps if we clarify this, we can understand where YouTube is coming from.

For our purposes, we'll define a "safe space" as a controlled environment where someone is able to explore difficult or challenging topics without judgment, usually with the assistance of a trained/licensed professional. For example, if we have a fear of frogs, a therapist might play sounds of frogs croaking, show us pictures of frogs, and slowly get to the point of actually seeing and touching a real frog. The idea here is to slowly introduce things that gradually push us out of our comfort zone and make us stronger.

However, this is the opposite of what YouTube is doing. YouTube seems to want to play protector in the name of safety. To really expose this, we need to reframe how "safety" is being used, and show exactly who is being "protected." When George W. Bush was president, he created "free speech zones" to allow people to peacefully protest his illegal invasions of Iraq and Afghanistan. Often these "zones" would be a considerable distance from his entourage, and anyone attempting to voice their free speech outside of these zones would be arrested. In another example, and one that is making an unfortunate comeback, banning books to "protect children" usually helps parents who don't want to deal with concepts they find uncomfortable. This is marginally better than, but not so different from, governments banning books to prevent people from considering certain ideas that might upstage political power. In these examples, both the free speech zones and banning books create a "safe space," but one that is only helpful to a select few.

But maybe we should ask what YouTube is trying to achieve here. After all, why is sex and nudity a problem? Indeed, "safe space" seems to have multiple interpretations. To a Big Tech company like YouTube, it seems to mean a puritan and sterile environment in which to sell ads. But to many people, the exact same phrase means a place to show nudity, whether it be classical artwork, porn, or anything else. And if YouTube is actually trying to use this "safe space" concept to make money from advertisers, have they forgotten the historical mantra that sex sells? Or maybe they are afraid of getting sued by the same people who seek to impose book bans.

We should also take a moment to reflect on what "safety" is. The truth is, just because we feel safe does not mean we *are* safe. Take computer antivirus companies: they ask us to pay a monthly or annual fee to run virus scans periodically. What they do not mention is that the only "safe" computer is one that is turned off and unplugged. Antivirus software can certainly help reduce your chances of getting a computer virus, but the reality is that they are selling the *feeling* of being safe from viruses, much like an insurance company. YouTube seems to be trying to do this too. In using their algorithms to flag and remove unrelated videos in a broad stroke, by the law of large numbers, they will also catch a few videos that are actual offenders. This is a bit like a fisherman who has a huge net that catches 100 old boots and a single fish. Technically, he was successful at fishing, but the reality is that he probably needed a better net.

How can we solve this? It's a hard problem, not least because YouTube is completely non-transparent. Right now, based on experiences like the opening anecdote, we really don't have much reason to trust anything they say. While demanding the algorithm be made public is a bit much, they could produce a weekly or monthly report showing how many videos the algorithm took down, and what percentage were appealed. If we had a history of reports like this, and we could see trends - such as a reduction in appeals - it would help build confidence in their system. If we were able to put this data alongside public anecdotes, and we found similar trends, that could be enough to create sufficient confidence, and YouTube would not have to worry about pretending to be a "safe" space.

What Do You Mean You Don't Have a Responsible Disclosure Program?

by Sp3nky

No product is perfect. You can have security involved from the beginning with the dev group, and something will be missed. This is still going to happen when you have a fully developed, mature DevSecOps group and program in place. While impressive, it doesn't matter. The group may have a checklist they work through as part of the procedure. While this is not optimal, there will still be people who want to check the box and not be creative with their solutions. Looking forward, we can't predict future technological advances. Soon, a present vulnerability which may not have been thought of may be detected and exploited. This has been experienced in the past, unfortunately. New technologies being implemented also provide for new attack methods, which are created frequently. These methods may be applicable to being applied against earlier products. Knowing all the advances that will be created in the next 10 to 15 years is not plausible.

With unknown future attacks that may be applicable to your product or services, the prudent move would be to attempt to plan for any future attacks. This may take many different paths for an organization. A CISO may want to put some process or procedure in place to meet the issue head-on. Any process in place well before an incident clearly would be beneficial. When there's an issue, it is always better to follow a plan. In the alternative, there's always the reactive model, which is never a good thing. The CISO would need to magically come up with a plan on the fly, which is critically needed, in an instant without having the opportunity of putting a couple of weeks of thought and vetting into it. Searching Google for a plan at the last minute isn't exactly the best situation.

This is where a responsible disclosure plan comes into play. When a researcher or third party finds one of these pesky vulnerabilities in your product, with a responsible disclosure process in place, the issue is manageable. This encourages the testing process to remove as many of these issues as possible up front. The company has their staff working on security, along with researchers throughout the nation and other countries also rooting these out. The researcher or lab finding the vulnerability has a road map to follow when disclosing this. There is a certainty with the process and the people involved have a method of showing the lack of malicious intent and clear focus of helping the industry and company with improving their product.

While this isn't the most glamorous topic, responsible disclosure programs are pertinent and a tool to give researchers some level of assurance that at least no legal action will be taken. What brings this about is the workplace recently completed a limited scope pentest of several consumer products (e.g. testing eight hammers from different manufacturers). Through the test, too many vulnerabilities were found. There was no data leakage between these. Each of the manufacturers was contacted individually (again, no cross contamination of test results), asking them what their responsible disclosure program was. Each email included the lab and possibly had information to communicate. This seems easy enough. Each manufacturer was emailed, letting them know that their product may have issues, and we wanted to communicate these to them in whatever format and method was best for them. Help me to help you. Very simple.

Well, not so much. It turns out manufacturers did not put an emphasis or much thought into this. There were two manufacturers who had something in place. One was mature, and the other not really, but they were moving in the right direction. The general response was in two forms. There was a lack of

response, which is bad. This lack of attention to a valid issue speaks volumes as to the weight and care placed with their products' cybersecurity.

The other general response received was more generic, not addressing there being an issue. These appeared to be more of a copy/paste from another document. This fit the circumstance like a square peg being forced into a round hole. The manufacturers were all contacted at least seven times, except for the two who had some form of a plan in place.

We all know the value of getting ahead of an issue. Handling a minor issue is so much easier than when it explodes through the network. We've seen what happens when the organization is not proactive. One issue with cybersecurity as a task and function is that it's difficult to quantify the benefits. These aren't tangible as this is with other disciplines (e.g. tax accounting saving the company six million dollars). The same problem occurs with the responsible disclosure programs. Management may view this as a money pit, with the labor, overhead, and any perks provided to the researchers.

There is a need for these programs. The researchers need to know they can do the research and testing for the product and provide real results for free, and there will be no legal repercussions. The alternative is to treat the non-malicious researchers as quasi-criminals. Naturally, the researchers would not want this and may move towards releasing their findings anonymously or in other venues with no notice.

The responsible disclosure program is a prudent avenue to follow. The company receives valid tests to help them with their product from researchers for free or with some bounty. In comparing the bounty amount with how much it would cost the company to be surprised with an exploit, the bounty and its benefits are clear.

The Coolest Hacker Multitool On the Market: The Flipper Zero

by Andrew "OGSkeltal" **ogskeltal@pm.me**

I am not affiliated with the Flipper Zero team, but have found substantial positives to using the product. I believe security professionals will benefit from owning one, so I wrote the below short piece advocating its uses. With wider adoption, there could be an increase in competing products, allowing users greater choice. The Flipper Zero opens a lot of possibilities for unique hardware devices targeted at, and made by, the hacker community.

Introduction

Imagine a device where you hack almost any wireless (IR, Sub-gHz, Bluetooth, RFID cards) and hardware device. It fits in your hands and it's fun to use. It seems almost science fiction, but it exists! It is the only type of device I have found that does this.

I recently purchased a Flipper Zero device and was fortunate enough to get it quickly, considering difficulties in shipments. I can say - without a doubt and for lack of a better word - this device is the coolest piece of technology I have seen in a decade. It is billed as a "hacker multitool" and lives up to its name. The Flipper Zero can work with various wireless technologies and has GPIO pins for hardware exploration.

Physical Device Features

The Flipper is slightly larger than a credit card and can easily fit into a pocket. It has GPIO pins for testing and expansion boards, a micro-SD card slot, and charges via USB type-C.

Modules

Sub-GHz transceiver - With the official firmware you cannot transmit, but the team behind the Flipper Zero allows custom firmware. Customization turns the flipper zero into a "baby Hack-RF." You can easily do rolling code attacks and signal analysis in the SubGHz range.

125kHz RFID Antenna - With this, you can access low frequency proximity cards, which are used in many access control systems.

Near Field Communication (NFC) - Read, write, and emulate high frequency tags. I have used it to read the chip in my credit cards - spooky! As more applications are developed, more functionality will be added.

Bluetooth - I have not used the Bluetooth functionality often, but the Flipper Zero website has the following to offer on the subject: "Flipper Zero has a built-in Bluetooth Low Energy module. As with other Flipper wireless features, we will be providing an open-source library for

adding Flipper support to community-made apps. Full BLE support allows Flipper Zero to act as both a host and a peripheral device, allowing you to connect your Flipper to 3rd-party devices and a smartphone simultaneously."

I have used the Bluetooth module to update my Flipper Zero, since the application on Android and IOS is already out.

Infrared Transceiver - Supports transmit and receive. If you remember the old days of the IR blaster prank device, this is similar. Large amounts of codes already exist that can be pre-programmed (more information is provided at the end of the article). Additionally, the Flipper can "learn" the codes and you can attempt to manipulate the device you are working on. I have used this to annoy my wife by turning off the TV!

Hardware Exploitation - Per the website: "Firmware flashing, debugging, and fuzzing. It can be connected to any piece of hardware using GPIO to control it with buttons, run your own code and print debug messages to the LCD display. It can also be used as a regular USB to UART/SPI/I2C/etc adapter."

One Wire Keys (ibutton) - 1-Wire connector to read iButton (aka DS1990A, Touch Memory or Dallas key) contact keys. This old technology is still widely used around the world. It uses the 1-Wire protocol that does not have any authentication. Flipper can easily read these keys, store IDs to the memory, write IDs to blank keys, and emulate the key itself.

BadUSB - The flipper Zero supports BadUSB and has a module for it. Many scripts have already been converted for use.

U2F - The Flipper can act as a universal second factor authentication key. It is currently only supported through USB, but Bluetooth is in the works.

Technical Specifications as per Website:

MCU (Microcontroller Unit)
Model: STM32WB55RG
ARM Cortex-M4 32-bit 64 MHz (application processor)
ARM Cortex-M0+ 32 MHz (network processor)
Flash: 1024 KB
SRAM: 256 KB
Display
LCD Monochrome
Resolution: 128x64 px
Controller: ST7565R
Interface: SPI
Diagonal Size: 1.4"
Battery
LiPo 2000 mAh
Seven days approximate working life (have tested this, it works as advertised)
Sub-1 GHz module
Chip: TI CC1101
TX Power: 0 dBm max
Frequency bands (depends on your region):
315 MHz
433 MHz
868 MHz
915 MHz
Note: Unlocked firmware exists, so if you flash the device you can RX/TX on all of these frequencies. If using official, you cannot transmit, and only receive on bands depending on region.
Near field communication (NFC)
Frequency: 13.56 MHz
Supported cards:
ISO-14443A/B
NXP Mifare Classic/Ultralight/DESFire/etc
FeliCa
NFC Forum protocols
RFID 125 kHZ
Frequency: 125 kHz
Modulation: AM, PSK, FSK
Supported cards:
EM400x, EM410x, EM420x
HIDProx, Indala
GPIO
3.3 CMOS Level
Input 5V tolerant
Up to 20 mA per digital pin
Bluetooth LE 5.0
TX Power: 0 dBm max
RX Sensitivity: -96 dBm
Data rate: 2 Mbps
Buzzer
Frequency: 100-2500 Hz
Sound Output: 87 dB
Type: Coin
Vibration Motor
Force value: 30 N
Speed: 13500 rpm
Infrared
TX/RX range: 800-950 nm
TX power: 300 mW
Ibutton 1-Wire
Operate modes: Reader/Writer/Emulator
Supported protocols:
Dallas DS1990A
CYFRAL
Physical
Size: 100 x 40 x 25 mm
Weight: 102 grams
Body materials: PC, ABS, PMMA
Operating temperature: 0 ~ 40 °C
GPIO pinout can be found here: `cdn.➥flipperzero.one/6xboq.png`
Official link: `flipperzero.one/`
Collection of official and unofficial software: `github.com/djsime1/awesome-➥flipperzero`
BadUSB Flipper Zero converted scripts: `github.com/I-Am-Jakoby/Flipper-➥Zero-BadUSB`

EFFecting Digital Freedom

by Jason Kelley

Killer Robots Are Coming, But We Can Stop Them

San Francisco is known worldwide as a progressive city, but those values were put to the test recently when the San Francisco Police Department tried to pass a new policy that would give them permission to use manually-controlled robots equipped with explosives. By the time most of the city heard about this, it seemed almost too late: the city's supervisors voted 8-3 to allow the policy on its first reading.

We scrambled into action, because the policy needed to pass its second reading as well. The "killer robots" were covered by news outlets around the globe, for good reason: militarization of police has been a longstanding problem, but something about attaching weapons to robots that were originally created for disarming bombs and sending them into a California city of 800,000 didn't sit right with most people who heard about it. The world was watching to see if a diverse and politically lively city would allow its police to kill with robots.

In just a week, activists and residents across the Bay Area worked together, made their voices heard, and even staged a rally early on a Monday morning. Thanks to their hard work, and the hard work of city leaders who never backed down on this issue (Supervisors Preston, Rosen, and Board President Walton), there was a stunning reversal on the policy's second reading: the San Francisco Board of Supervisors banned the SFPD from using deadly force with remote-controlled robots, by the same 8-3 vote that initially passed the policy.

The fight isn't over in San Francisco. The board sent the killer robot policy back to its Rules Committee for revisions and more public comment, and it could be taken up again in the future. But in one week, San Francisco and the greater Bay Area rallied, and that rallying cry was so loud and undeniable that it was impossible for the board, and the world, to ignore.

This battle is part of a history of militarization of law enforcement, and a sign of things to come. The weapons of the United States military - drones, mobile command centers, sound cannons, and more - have already been handed off to local law enforcement for years. The transfers have equipped police departments with the ability to redirect surveillance tools and the weapons of war designed for foreign adversaries toward often-faultless targets in U.S. cities.

More and more dangerous surveillance technology and military-style equipment is coming down the line - whether it's robots and drones manually controlled by law enforcement operators, or automated robots like the Knightscope variety of autonomous rolling machines. The slope is slippery, and we've been sliding down it for a long time. Knightscope robots are already patrolling our streets, parks, malls, and grocery stores. ShotSpotter's high-powered microphones that purport to detect and triangulate gunshots in order to alert police have been in use for years, despite their inaccuracy. Now, the company has said they are teaming up with a drone company to dispatch autonomous drones to fly automatically to the presumed site of gunfire.

But with the battle over killer robots, we have seen that there is a line that people do not want police to cross. Law enforcement agencies will want to cross that line, as they did in San Francisco, and we can stop them and, with work, even roll back some of the dangerous, ineffective, and overused surveillance technology and military weaponry that have been in place for years now. If you consider yourself part of the fight for digital rights, this is one of the next frontiers.

What can you do to help? For starters, push for transparency laws around police use of technology, and processes for community input and control. California is unique in having recently passed a law, A.B. 481, that requires democratic control of whether California state or local law enforcement agencies can obtain or use military-grade tools, whether they are received from the federal government, purchased, or utilized via some other channel. Through their elected officials, the public can say "no" to military surveillance and other technology, and it won't be allowed to come to town.

This is the sort of law that just makes sense - it's important for there to be more transparency into law enforcement practices, and for communities to have democratic control of surplus military transfers, particularly for high-tech surveillance equipment. The law was modeled on Community Control of Police Surveillance (CCOPS) laws adopted in over a dozen communities across the country. Most law enforcement agencies around the country don't have to go through a policy proposal process to obtain permission to use killer robots, but those laws can be implemented in any city around the country. And if you're in California, you have at least two agencies currently going through an A.B. 481 process - your local police and sheriff - that you can follow.

Second, continue to push back against surveillance tech in the hands of police by educating yourself and others about it. Our street-level surveillance website shines a light on the advanced surveillance technologies that law enforcement agencies routinely deploy in our communities. These resources are designed for members of the public, advocacy organizations, journalists, defense attorneys, and policymakers who often are not getting the straight story from police representatives or the vendors marketing this equipment.

Third - and this may be the easiest way to help - make sure you understand what's happening in your community. Usually, records are out there in the form of news stories, social media posts, press releases, or documents buried in government websites, about what equipment law enforcement and city officials are using in your area. Our atlas of surveillance project collects much of this information, but it's a big task and represents only what our team documented after a year and a half of research. You can always volunteer to help by sending a message to `info@eff.org`.

This moment is a turning point for pushing back on the use of dangerous technology by police. We hope you'll join us in making sure that killer robots never come to the town where you live - or anywhere.

Cyber Security Frameworks

by fsu_tkd90 AKA Bill

The last article I submitted to *2600* was printed in 27:3 (Autumn 2010). Back then I wrote about my biggest problem at work: spam. Now I am writing about a dizzying problem for all corporations: all of the cyber security frameworks a company could be subject to.

Let's start by defining what cyber security is. Cyber security is not to be confused with information security. Information security is intended to protect data from any form of threat regardless of being analog or digital. Cyber security is meant to protect attacks in cyberspace such as data, storage sources, or devices. Cyber security usually deals with cyber crimes, cyber frauds, and law enforcement. A cyber security framework is, essentially, a system of standards, guidelines, and best practices to manage risks that arise in the digital world. They typically match security objectives of corporations.

It's important to understand why the cyber security frameworks are so important. Cyber attacks are now coming from nation-states as a part of war. Iran nation-state attackers typically use remote exploitation, password spray, and phishing man-in-the-middle attacks. Russian state-sponsored advanced persistent threat (APT) actors have used tactics including spear-phishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security. Chinese state hackers are using open-source information and common exploits.

Some of the largest attacks in the USA were the Colonial Pipeline, Brenntag (a chemical distribution company), Acer, JBS Foods, Quanta (Apple's business partner), and the National Basketball Association (NBA). The two new top trends malicious actors employ are automating ransomware with a human on keyboard, and "ransomware as a service." Ransomware as a service is inexpensive and readily accessible. "Cyber crime as a service" companies now have human resource departments and operate from countries with limited extradition laws. An example of this is the ransomware gang Conti, which operates no differently than a legitimate corporate business. They maintain salaried employees who are provided bonuses, performance reviews, employee referral incentives, and the coveted spot of "Employee of the Month." The employee of the month receives a bonus equal to half their salary.

Any of the cyber security frameworks takes years to implement and this article is not meant to explain each in detail. Rather, it is meant to make you aware that they exist and to give you a basic understanding. The cybersecurity frameworks all promote good basic cyber hygiene. Some of the frameworks are listed below.

ISO 27001 is composed of 18 sections with 114 total controls. ISO 27001 is a framework that helps organizations "establish, implement, operate, monitor, review, maintain, and continually improve an Information Security Management System (ISMS)". It is a joint operation between the I.T. department and the human resources parts of the business. ISO 27001 certification demonstrates that organizations have invested in the people, processes, and technology (e.g. tools and systems) to protect an organization's data and provides an independent, expert assessment of whether your data is sufficiently protected. Reports and policies must be proven to be effective to the auditors.

Information Governance

HIPAA is composed of five main elements and the CFR Part 164, Parts C, D, and E. First, let's define information governance (IG). It is the process of aligning the management and the control of information with business objectives and regulatory compliance requirements. IG in healthcare sets corporate principles for addressing data-related challenges, such as ensuring the confidentiality and security of patients' data. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA improves efficiency in the healthcare industry, improves the portability of health insurance, protects the privacy of patients and health plan members, and ensures health information is kept secure and patients are notified of breaches of their health data. HIPAA was based off of The Health and Clinical Health (HITECH) Act. It encouraged health care providers to adopt electronic records and improve privacy and security protections for all of healthcare data. HITECH was enacted under Title XII of the American Recovery Act. It has five goals: to improve quality, to improve safety, engage patients in their care, increase coordination, and improve population health status. It was enforced by the Office of the National Coordinator (ONC).

CIS Security Controls

There are 20 sections (sometimes called the SANS Top 20) with 178 sub-sections. CIS 20 is a prescriptive, prioritized, and simplified set of cybersecurity best practices.

How are CIS Controls implemented?

Step 1: Take inventory of your assets.
Step 2: Measure asset controls.
Step 3: Perimeter defenses.
Step 4: Detect and respond to incidents.
Step 5: Evaluate the most critical gaps.

Step 6: Plan and implement your controls.
Step 7: Train and monitor users.
Step 8: Test your controls.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is composed of 12 sections with 288 controls. The PCI DSS is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The major credit card schemes are: American Express, Mastercard, Discover, Visa, and JCB. The PCI standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The Card Holder Data Environment (CDE) is comprised of people and techniques that store, process, or transmit cardholder data or sensitive authentication data.

Federal Financial Institutions Exam Council (FFIEC)

This is a framework (cyber assessment tool) for measuring cyber security risk and preparedness in the financial industry. The FFIEC provides a cyber security assessment tool to help organizations better understand and address their cyber security risk. It is a five member agency responsible for establishing consistent guidelines and uniform practices and principles for financial institutions. FFIEC guidelines provide financial institutions with expectations for compliance.

The below is not framework but recommended models:

FedRAMP - Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a framework that saves costs, time, and staff required to conduct redundant agency security assessments. FedRAMP Ready indicates that a third party assessment organization (3PAO) attests to a CSP's readiness for the authorization process, and that a readiness assessment report (RAR) has been reviewed and approved by the FedRAMP program management office (PMO). Because FedRAMP is mandatory for all cloud services used by federal agencies, you won't be able to do business without getting your FedRAMP authorization. Your organization is potentially missing out on a lot of revenue if you choose not to pursue compliance.

The below is a not a framework but a standard:

Federal Information Processing Standards (FIPS) was developed by the National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and is a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies. FIPS 140-2 has f levels of security:

- *FIPS 140-2 Level 1.* Level 1 has the simplest requirements. It requires production-grade equipment and at least one tested encryption algorithm. This must be a working encryption algorithm, not one that has not been authorized for use.
- *FIPS 140-2 Level 2.* Level 2 raises the bar slightly, requiring all of Level 1's requirements, along with role-based authentication and tamper-evident physical devices to be used. It should also be run on an operating system that has been approved by Common Criteria at EAL2.
- *FIPS 140-2 Level 3.* Level 3 is the level the majority of organizations comply with, as it is secure, but not made difficult to use because of that security. This level takes all of Level 2's requirements and adds tamper-resistant devices, a separation of the logical and physical interfaces that have "critical security parameters" enter or leave the system, and identity-based authentication. Private keys leaving or entering the system must also be encrypted before they can be moved to or from the system.
- *FIPS 140-2 Level 4.* The most secure level of FIPS 140-2 uses the same requirements of Level 3 and desires that the compliant device be able to be tamper-active and that the contents of the device be able to be erased if certain environmental attacks are detected. Another focus of FIPS 140-2 Level 4 is that the operating systems being used by the cryptographic module must be more secure than earlier levels. If multiple users are using a system, the OS is held to an even higher standard.

In conclusion, all of these frameworks are important because criminals want cash, things that can be turned into cash, and information someone else would find valuable. In 2021, REvil's domain was hacked by another gang, Emotet returned with Cobalt Strike, and BlackMatter used tools from Darkside, Revil, and LockBit. SquirrellWaffle was observed using office documents that infected systems with Cobalt Strike. To defend against future threat actors, Microsoft purchased Section 52, which is a world class team of defenders, IoT/OT security researchers, and data scientists.

I'll end with a couple of acronyms: The CIA Triad (Confidentiality, Integrity and Availability) is a common model that forms the basis for the development of security systems; The DIE Triad (Distributed, Immutable, Ephemeral) serves as an alternative to the CIA Triad that reduces our security burden, enables us to achieve true resiliency, and move towards anti-fragility.

Music in Ones and Zeroes: A Memory of Streaming Soundscapes

by Matt Johnson
ech0plex88@protonmail.com

It was an impulsive purchase in Orlando's Virgin Megastore that opened my ears to electronic music. I was 18 years old and a high school senior in the fall of 2000. Visiting from northern Minnesota for an academic conference, the music store was a chance to discover new tunes outside my three-year addiction to Nine Inch Nails. On that day, I ended up taking home DJ Krush's *Kakusei*, Chris Fortier's *Trance America* and Aphex Twin's *Selected Ambient Works Volume II*. The first album was enjoyable for a longtime drummer, the second was like a soundtrack for science fiction, and the third was an unsettling but captivating hallucination.

Soon, I was digging through CDs at Sam Goody, where I found Ministry of Sound's *Global Underground* series. Not only was this an expansive collection of trance music from a variety of artists, but each double-CD's liner notes gave enviable details on the location, attendees, and generally euphoric atmosphere of each event. Club nights for the young, rich, and famous; a far cry from the life experiences of a Midwestern teenager. Still, I could live vicariously through the music. Trance held my interest through college, where I collected hundreds of tracks and mixes by John Digweed, Paul Oakenfold, DJ Tiesto, Ferry Corsten, BT, Amoeba Assassin, and others.

Aside from enjoyable listening, I also found the music especially helpful with writing. Creative writing was a fun hobby I'd started during an English class at age 15. At first, I listened to whatever classical pieces were playing on public radio. Generally calming, sometimes thunderous, the music helped me focus and inspired me when describing a scene's atmosphere or character emotions.

Electronic music took this beyond simple short story background tracks. I'd already been interested in extracting music files from games like *StarCraft*, *Fallout*, and *Diablo*. Later, I'd do the same thing with *American McGee's Alice* and *Return to Castle Wolfenstein*. These new albums (particularly Aphex Twin) were perfect for driving, studying, chores, and even replacing the muted music of whatever game I was playing. Sometimes hyperactive and intense, sometimes softly flowing and moody. These experiences were not soundtracks, not popular songs referencing specific life events. They were soundscapes - as much a part of my environment as wind rustling trees and tall grass, or the dripping of melting snow; in some cases, directly sampling those sounds.

Then I started college in the fall of 2001, and two innovations expanded my exposure to free music of all genres. A modern campus interconnected with T1 lines, and file sharing sites. Napster, LimeWire, Audiogalaxy, even Live365 for streaming radio. I had all the music I could ever listen to, without ever needing to buy another CD. Out of all these options, one streaming music site stood out.

Site and trademark registration for `musicforhackers.com` (MFH) appears to have occurred on Thursday, September 7, 2000. In the registration, the site is described as providing "Entertainment services, namely, providing a radio program in the field of IT Security and Electronic music via a global computer network."[1] [2] The earliest versions of the site can be found via the Internet Archive. It appears under construction in the first snapshot dated February 29, 2000.[3] This is followed by a June update referencing an IRC connected to *2600 Magazine*, and a predicted debut of April 2001.[4] Through the remainder of 2000, the site progresses through beta versions. It offers 32kbps and 56kbps streams, broadcasting 2600 Magazine's *Off The Hook* radio program.[5]

The July 21, 2001 snapshot presents MFH in the form I first used, version 1.0. A nicely rendered graphic is centered, depicting the MFH server (hosted on Live365)[6] passing data through a firewall into the 32kbps dial-up and 56kbps cable/DSL streams. Along the bottom row are links to client applications used to play the streams. As a Windows user at the time, I listened with the wonderfully customizable Winamp (it really whips the llama's ass!). Linux users could access via the X Multimedia System (XMMS) while Mac users had iTunes (not even a year old at this point). Finally, there is a link for users of BeOS, a discontinued operating system which was developed in 1990 and sold to Palm Inc. in 2001. Stacked along the left side of the site are links to `/streams` (depicted center-site), `/playlist` (current and three previous tracks), `/home` (the main site) and `/null_news`.[7] This was MFH's form as I discovered it while searching for electronic music stations in the spring of 2002, the intriguing tagline "Soundscapes for Compromising a Remote

Host" drawing me in.

The news page provided links to such gems as:

"All your base are belong to us" - *The Register*[8]

"Microsoft Obsecurity"[9]

"Britney Spears' Guide to Semiconductor Physics"[10]

"Gary Coleman Talks About Priority Queuing"[11]

"Something Awful" - *BetaNews*[12]

"Hack1ng f0r D09z"[13]

How to describe being absorbed into a soundscape? I'm writing a scene in a personal creative writing project - genre: corny, paranormal romance. I'm chugging through calculus homework. I'm skimming news articles and looking for new games to try. Winamp ingests the 56kbps stream and deposits music. Maybe it's "The Shield" by Biosphere, or "UT1-Dot" by Polygon Window, or "Kalpol Introl" by Autechre.

Mentally, you enter an ocean current. Maybe a thought "slipstream." Your brain is taken along for a ride, swiftly and smoothly. Surroundings fade. There are only the *task* and the soundscape. It causes an incredible sense of focus, an out-of-body experience. Then there is the inevitable interruption. Roommate returns, or the stream disconnects.

Returning to the regular conscious world causes mental turbulence. It's a jarring effect, like suddenly slamming the brakes. The dizzy disorientation of standing up too quickly. Forcefully d-r-a-g-g-i-n-g your consciousness out of the soundscape like hauling a boot out of thick mud. There's a re-calibration period as you adjust to your surroundings and the room takes shape. That's true focus.

The final "first generation" screenshot comes from April 23, 2003. An addition along the left hand side is a link to Jinx Hacker Wear: "Swag for Hackers and Geeks."[14] After that, the site goes dark until 2011. It returns in an updated form, featuring a list of album art and a single "listen.m3u" streaming link. This form lasts for two years, disappearing in 2013.[15]

An mp3 horde replaced streaming music for me in the years between 2003 and 2015, when a hard drive crash cost me thousands of tracks (*back up your data!*). After that, it was YouTube and sites like Nightwave Plaza that satisfied my growing interest in synthwave and vaporwave. These days, I get my soundscape fix from Soma FM, an Internet radio site that, interestingly enough, first went online in 2000. Genres and sites come and go, but I'll never forget the life events that were enhanced by the strange sounds of Music For Hackers.

In retrospect, probably the strangest connective tissue from MFH began with a track called "Seven Day Galaxy" from the 1999 album *Oedipus Brain Foil* by Randy Greif, Robin Storey, and Nigel Ayers. Looking into other works by those artists, I discovered Robin Storey's (under the name Rapoon) album *What do You Suppose? (The Alien Question)*. A well-crafted example of ominous droning ambiance, it featured several samples of a man giving a lecture on Cold War-era alien and secret government conspiracies. Those words and music were perfectly complementary. After some research, I discovered the lecturer was 1990's shortwave radio host and conspiracy theorist extraordinaire William Cooper. The late Bill Cooper, whose program *The Hour of the Time* covered New World Order concepts in exhaustive detail, was perhaps most notable for writing the tome "Behold a Pale Horse." Strange journeys across wild lands, indeed.

[1] alter.com/trademarks/
➥musicforhackerscom-78024924

[2] trademarks.justia.com/780/24/
➥musicforhackers-com-78024924.html

[3] web.archive.org/web/20000229121447/
➥http://www.musicforhackers.com/

[4] web.archive.org/web/20000604080520/
➥http://www.musicforhackers.com/

[5] web.archive.org/web/20001206210300/
➥http://www.musicforhackers.com/

[6] web.archive.org/web/20010604040125/
➥http://www.live365.com/
➥stations/173099

[7] web.archive.org/web/20010721153755/
➥http://musicforhackers.com/

[8] www.theregister.com/2001/02/22/
➥all _ your _ base _ are _ belong/

[9] www.bbspot.com/Features/2001/02/
➥obsecurity _ server.html

[10] britneyspears.ac/lasers.htm

[11] web.archive.org/web/20001109102400/
➥http://www.routergod.com/
➥garycoleman/

[12] web.archive.org/web/20011205053504/
➥http://somethingawful.efront.com/
➥jeffk/

[13] web.archive.org/web/20010629010627/
➥http://www.meydabbs.com/hack4d0gz/
➥main.html

[14] web.archive.org/web/20030423203357/
➥http://www.musicforhackers.com/

[15] web.archive.org/web/20110207102117/
➥http://musicforhackers.com/

Cryptocurrency - Busted!

by lg0p89

When we hear of cryptocurrency, we think of bitcoin and making millions overnight - and then losing millions the next day. While this is the outward focus, there is still a backbone of technology. This houses the vulnerabilities that we exploit. Historically, the general attack has been the 51 percent among others. There have been variations of this and others. Recently a newer attack has become more prevalent in certain configurations. This ingenious attack deserves a greater level of attention and applause.

This attack by far is not the first and certainly won't be the last. In 2022, there was an attack where over two billion dollars were liberated from a company. Many of these attacks had been perpetrated by persons and groups in North Korea.

This time around, the target was the Binance coin. This wasn't their first rodeo. In 2019, the company was successfully attacked. This time the amount involved was approximately seven thousand bitcoins - or 40 million dollars. In this round of "We Pwned You," the compromise was initially valued at 100 to 110 million dollars. The updated estimates were changed to the attackers liberating two million BNB tokens, valued at around 568 to 570 million dollars.

With this attack, the focus was on the bridge between the blockchains. For this, they were targeting the BSC (Binance Smart Chain) token hub.

The bridge is pretty much like it sounds. There is a link between two blockchains. This acts like a bridge between the two to facilitate the communication. The communication across the bridge allows for the tokens to be transferred from one blockchain (platform) to another blockchain (platform). This attack point has been a focus for some time.

Pre-attack, the group would have reviewed a threat assessment. The blockchain attacks usually take time and resources, so the weak points would have been looked at more closely. The bridge process provided this with multiple points to attack.

Once this was compromised, the attackers were able to move the tokens off of the Binance network. This vulnerability leveraged an issue with the smart contract. This allowed the attacker to create fraudulent transactions and have the tokens sent to their crypto wallet. Since the smart contracts don't require human interaction to execute (by definition), this was done relatively quickly.

After the attack, they began to move the funds across different liquidity pools. This acted to move the BNB into other assets and quasi-clean it. Only an estimated 70 to 80 million dollars were taken off the blockchain. The remaining money stayed on the blockchain and is not accessible to the attacker(s).

After noticing the anomalous activity, Binance temporarily halted activity and new blocks on the BSC. After the heist, the co-founder of Binance announced the issue was contained. Of the stolen funds off of the blockchain (70 to 80 million dollars), approximately seven million dollars had been frozen.

The attack, while interesting on its own, does highlight the need for creative minds to test and re-test any company's processes and infrastructure. We have to stop only using a checklist and hoping we are good. Without a proper and robust pentest, companies will continue to have issues.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

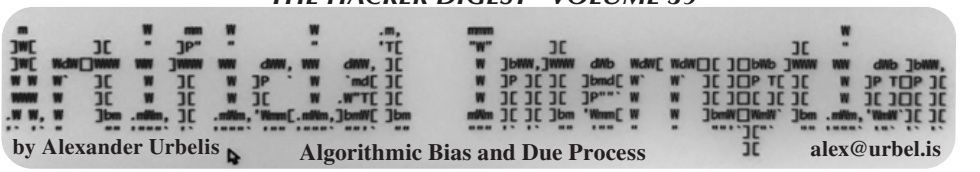
Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access, our editorial department can be snail mailed at:

2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.



by Alexander Urbelis

Algorithmic Bias and Due Process

alex@urbel.is

In December 2021, New York City passed a first-of-its-kind law regulating the use the artificial intelligence in the employment context. That law bans employers from using artificial intelligence or algorithm-based technologies for employment-related decisions - such as hiring, recruiting, retention, or promotion - if an independent third party has not audited those technologies for bias.

Ordinarily useless, banal, behind the times, and out of touch with the people it serves, it seemed like the New York City Council actually passed an ordinance that was worthwhile, on the right track, and protective of New Yorkers' rights against discrimination and bias, even if a machine was responsible for the prejudice. I applauded this legislation. And because it comes into effect in January 2023, I have been helping numerous companies navigate this audit requirement and prepare their disclosures about what, if any, bias results from their AI or algorithm-based employment screening decisions.

As a matter of fundamental fairness, it should be universally agreeable, and even self-evident, that we would want important decisions to be free from prejudice. And if there exists an AI-based system that produced questionable or biased results because of an identified defect, then we would certainly want to revisit and remake those decisions on the basis of a revised process that was free from bias.

As human beings, our decisions are complex and the result of our experiences, emotions, education, and a range of other nuanced factors and, unless someone is a bigot or racist, we all presumably strive to make our decisions in a manner that is free from bias or discrimination. But the complexity of our emotions does not lend itself to being audited. Bias may creep in despite our best efforts. Someone may not think they are inherently racist, but because of their upbringing or experiences, certain prejudices, however subtle, may affect a decision.

This raises the question: could a well-regulated AI make better decisions than humans? And, if the answer is anything resembling a "yes," then that raises a further question: could an AI that is free of bias or discrimination replace a jury in our legal system? And, again, if the answer is anything resembling a "yes," then that raises a further question, a heartbreaking query this time: could an AI have prevented a tragic injustice that occurred on November 29, 2022, at 7:40 pm, in Bonne Terre prison, when the State of Missouri executed Kevin Johnson?

Kevin Johnson was 37. He had been on death row since he was convicted of first-degree murder 17 years ago. On July 5, 2005, Johnson killed a police officer, Sergeant William McEntee. Johnson was 19 years old at the time.

The facts of what happened on July 5, 2005 are heartbreaking on many levels. They do, however, explain in part why Johnson committed a murder for which he later unconditionally repented and for which he paid with his own life.

Suspected of a probation violation, police showed up at Johnson's home on July 5 with a warrant for his arrest. According to multiple sources, Johnson saw the police arrive, woke up his 12-year-old little brother "Bam Bam," who then ran next door to their grandmother's house. Bam Bam had health issues: he was born addicted to crack-cocaine and had a congenital heart defect. When he arrived at his grandmother's house, Bam Bam's health began flagging. According to the *Missouri Independent,* police officers including McEntee entered the grandmother's residence, after which Bam Bam began to have a seizure.

The officers ignored Bam Bam's distress and seizure. According to various reports, the officers stepped over Bam Bam's limp body and never helped him or called for help. The police officers also prevented Bam Bam's mother from offering any comfort, aid, or to even enter the house despite the ongoing seizure. A short time later in a hospital, Bam Bam died.

Johnson was distraught, kicked his bedroom door off its hinges, and, according to the Associated Press, Johnson had then wandered around his neighborhood furious with McEntee for preventing his mother from helping Bam Bam even as his little brother convulsed. Enraged at McEntee, Johnson screamed "He killed my brother!" as he roamed the streets.

A few short hours after Bam Bam's death, Sergeant McEntee was again in Johnson's

neighborhood, called in this time to investigate someone setting off fireworks. Johnson saw McEntee, pulled a gun on him, and shot him. McEntee tried to flee, and Johnson shot him two more times, killing him.

The State tried Johnson for first-degree murder. A first-degree murder charge requires premeditation and could result in the death penalty. The jury, however, was hung. The jury was not quite convinced that the murder was premeditated as opposed to the result of Johnson's emotional and impulsive state.

In 2007, the State tried Johnson again and convicted Johnson of first-degree murder. That conviction resulted in a sentence of death.

The report of a special prosecutor that the Missouri judiciary appointed to investigate claims of racial bias in that second trial concluded that race played a "decisive factor" in the death sentence, and that the process by which Johnson was convicted was "infected" with racial bias. The government, for one thing, tried to remove all black persons from the jury.

The special prosecutor sought to vacate Johnson's death sentence. This was the first time in Missouri that a prosecutor sought to overturn a conviction tainted by discrimination.

Despite the apparent racism and these extraordinary circumstances, after oral argument, the Missouri Supreme Court refused to grant any relief. The Governor of Missouri, Mike Parson, refused any clemency and would not commute Johnson's sentence to life. The last stop was the U.S. Supreme Court. Though Justices Jackson and Sotomayor vigorously dissented, that institution failed to provide any relief as well, clearing the way to Johnson's lethal injection.

As technologists, we understand the axiom of "garbage in, garbage out" as applied to the input and output of a function or program. As technologists, we know that a flawed system will produce flawed results that cannot be trusted. As technologists, this is why we understand and applaud auditing of AI or algorithms for bias, discrimination, and any kind of flaw that could negatively impact our lives or the lives of others. Why, then, do we neither expect nor demand the same kind of common sense and rigor be applied to our justice system?

How much injustice can this system tolerate in the name of justice before it fails to an insecure state? When evidence that racial bias and discrimination permeated a capital case lies in front of you - and even a prosecutor is clamoring for the sentence to be vacated - how can we countenance those in power when they refuse to act? Those persons in positions of political power assumed an awesome responsibility when they took office, and we cannot allow them to shirk their obligations or to act as if they are somehow allowed to abdicate adherence to basic moral principles.

The irony, of course, is that it was because of politics that Governor Parson refused to intervene and stop an execution that was a well-documented result of a racially biased and discriminatory legal proceeding. It was self-interest. It was borne of his own political ambition. When this is the norm, are not dispassionate, unambitious machines better decision-makers?

I have no idea whether a detached, artificial intelligence would have prevented any of the horrible outcomes throughout the process that led to the State of Missouri taking the life of Kevin Johnson. What I think is crystal clear, however, is that we need to apply the same low fault tolerance levels of the technological systems we design to the justice system of which we are all a part. If we are right to be so cautious about bias seeping into the decision of whether a private company grants a job applicant an interview, then, *a fortiori,* shouldn't we be infinitely more concerned about bias seeping into the decision of whether the State should terminate the life of one of its own citizens?

Auditing AI systems for any hints of bias is not only about identifying and remediating prejudicial algorithms. It is also about accountability for discrimination and prejudice. We demand accountability of private parties, but it is also that which has been missing from our political processes and justice system. So many of our institutions that should have acted to prevent injustice - the prosecutor's ethical obligations, the jury system, the appointment of a special prosecutor, the trial courts, the appellate courts, and the U.S. Supreme Court - turned a blind eye.

No doubt there were many that tried to act, but it was aggressive apathy that prevailed in Johnson's case. With such ample evidence around us that we have created and are perpetuating an imperfect justice system that produces prejudice with no accountability, we owe it to ourselves to prioritize change, especially if we are to continue being the ones to audit AI systems, and not the other way around.

Tales for My Toddler

by macmaniac

Disclaimer: I do not encourage piracy. Remember that some artists are depending upon you paying for their music.

Some time ago, I purchased a music player for my toddler. I mention this because I like the producers' spirit (the producer of the player, not of the toddler - the latter is me). That player is built to last, energy saving by using wav instead of mp3, easy to deal with by toddlers and to maintain by their parents. Last but not least, their answer to "Well, I use Linux..." is not "We don't support Linux." but "Our Linux application is still being developed, but have a look at this script that some customers wrote. Maybe it's helpful."

For months everything was fine as the pre-installed music files were enough for my toddler. But some days it was enough for me. Another day of "Baah Baah Black Sheep" in endless loop - no way! So I decided to put some other stuff on it. If you have mp3 files, you can just convert them to wav and put them on the player's SD card. But getting the desired sound is not too easy, as I found out.

Now I have to mention that I'm from a small country with its own language. Albeit our laws concerning pirating are rather liberal, it's hard to find content in my language. And even harder to pirate kids' stuff. Toddlers and loving parents are not known for being pirates, arrr! So I was looking through my old stuff to find music or tales for my toddler. I found some tapes. But no player. For the blink of an eye, I was thinking of tearing the tape out and getting a pencil to roll it up again. Nah, these were the old days. I came across some compact discs (CDs) with nicely told tales. For DVD ripping purposes, I still own a CD drive. So I was able to rip the tale, convert it to wav, and put it on the player.

The next thing was a song we had watched on YouTube. This was the only source I could find. A video. The sound on its own was not available anywhere. Luckily, youtube-dl[1] still exists and hopefully will forever. It's a mighty tool to rip copyleft videos from YouTube and other platforms. But it also lets you solely extract the audio tracks. As YouTube is so big, you can get a lot of content from there.

Another big thing is Spotify. It doesn't stream videos, but songs. And even lets you save songs offline! But these files are still encrypted. So there's no chance to just copy your favorite songs to another device. I found some dubious browser add-ons and applications that claimed they could de-DRM Spotify. No thanks. There was nothing like youtube-dl for Spotify, reason why I looked for other ways to get the latest Peppa Pig tales on that player!

Audacity came into my mind. Another powerful tool I know from the days I wanted to be a rapper and needed some professional but cheap (that is - free) audio editing software. This tool is capable of recording directly from your soundcard - which means recording without any degradation[2]. The downside: it's like old-fashioned recording - it takes time. And if you record a playlist, you need to split and export the single tracks. It wouldn't be a mighty tool if a manual didn't exist on how to do this the easy way[3].

Wouldn't it be great if some script existed that would automate the whole Spotify/Audacity process? Or even some youtube-dl equivalence for Spotify? I'll leave these tasks to brains that are more skilled than mine.

P.S. The player is called Hoerbert. Have a look: `www.hoerbert.com`.

[1] `youtube-dl.org/`

[2] `manual.audacityteam.org/man/tutorial_recording_computer_playback_on_linux.html`

[3] `manual.audacityteam.org/man/splitting_a_recording_into_separate_tracks.html`

Raising Generation Orwell: A Guide to Teaching Kids the Human Rights of Privacy

by Worlds_Gr8test_DeFective

I was born at a time where I consider myself both lucky and unlucky to come of age during the analog to digital transformation. I can vividly remember when you could only get in touch with someone if they were home, when staying in touch with your friends was a question of "do you have Internet?" instead of "what's your Insta?", and when I could walk down city sidewalks without seeing CCTV or an Internet-connected camera in everyone's hands or beside their doorbell.

I consider myself lucky because I grew up with a slower pace of communication, with less expectations to have an "online presence," and when privacy in public was the norm. Where I am unlucky is that, as an adult, I have been coerced into an "always on" working culture, facial recognition technology paired with Internet-connected cameras and microphones every square meter that is enough to put your subconscious in a manic state of paranoia, and legislation such as the Patriot Act in the United States constantly expanding its capabilities to abuse the very technology that is meant to bring us closer.

So how does this tirade fit into the title of this article? I remember a time when this was not normal. When it was different. I am conscious of the subtle surrenders of privacy we have stumbled into. Children and teens today are growing up in an increasingly surveilled world which is the norm for them. They will never remember a time when returning to the United States from overseas travel meant you did not have to surrender your electronic devices to Homeland Security for inspection, or entering a country by air travel did not require you to provide your biometrics at a kiosk prior to crossing customs.

So what can we do about this? Legislation is not keeping up with the pace of Internet-connected technology from a security and privacy standpoint, so I believe our best strategy forward is to harden the coming of age generation with privacy awareness. Please consider the following suggestions in how to accomplish this:

- Before taking a photo or video of a child, ask them for permission. Kids now are conditioned to seeing Internet-connected cameras constantly at home and in public. Asking them permission gives them control over their digital footprint.
- Educate kids and teens who use Internet-connected devices on vendor telemetry collection and the monetization of data analytics. This will help them understand that the communication between their source device and the destination is usually more than a two-way connection and involves sometimes up to hundreds of third parties collecting personal and technical data. Do not do this as a sense of paranoia, but as an awareness piece on understanding what information is collected over the Internet as an end user. You can take this a step further by analyzing network logs or using services such as Electronic Frontier Foundation's (EFF) Privacy Badger to visualize data analytics collection.
- Show what surveillance technology your security forces and local law enforcement use in public areas or, in some cases, on private property. Explain how license plate readers can be abused for profiling patterns of life and how Amazon Ring has the capability to back up recorded footage and audio forever. This footage can also be integrated with Amazon's Rekognition or Clearview's facial recognition technology and indexed into a criminal database if an agency integrates these services. A good starting point for this information is the Atlas of Surveillance project by EFF or the work done by The Citizen Lab.
- The most important aspect of this is to not under any circumstances teach kids to be paranoid. It's very easy to fall into the abyss of paranoia when researching how emerging technology invades privacy. You will do them no favors by scaring them into thinking Big Brother is always watching. Empower them to have control over their digital footprint and to understand the privacy risks of attending a protest or sharing photos over social media. Arm them with knowledge and surveillance self defense, not fear.

```
#!/bin/sh

# Consider that perhaps nmap is unavailable to you, but netcat is.
# Netcat has scanning functionality, but it can be a little slow.
# This script will speed things up by running several instances of
# netcat in parallel.
#
#    - Justin Parrott

NUMTHREADS=10
TIMEOUT=3
STARTPORT=1
STOPPORT=1024

usage() {
        echo "usage: $0 [options] host"
        echo "  -s startport        Where to start the scanning (integer)"
        echo "  -S stopport         Where to stop the scanning (integer)"
        echo "  -t numthreads       Number of processes to execute in parallel"
        echo "  -w timeout          Timeout per connect (integer)"
        exit 1
}

while getopts s:S:t:w: opt
do
        case $opt in
        s)      STARTPORT="$OPTARG";;
        S)      STOPPORT="$OPTARG";;
        t)      NUMTHREADS="$OPTARG";;
        w)      TIMEOUT="$OPTARG";;
        \?)     usage;;
        esac
done
shift $((OPTIND - 1))

if [ $# -ne 1 ]
then
        usage
fi
HOST="$1"

tcping()
{
        nc -z -w "$to" "$host" "$port"
}

i="$STARTPORT"
running_threads=0
while [ "$i" -le "$STOPPORT" ]
do
        port="$i" host="$HOST" to="$TIMEOUT" tcping &
        running_threads=$((running_threads + 1))
        i=$((i+1))

        if [ $running_threads -eq "$NUMTHREADS" ]
        then
                wait
                running_threads=0
        fi
done

wait
```

The Search for Life at 300 Baud

by N1xis10t

N1xis10t@protonmail.ch

In *2600 Magazine* 38:3, a letter to the editor was featured in which a person named HC asked if anyone remembered a publication entitled "Life at 300 Baud." The editors said that they didn't find anything when searching for it online. My interest was piqued after reading this exchange, and I set off to conduct my own search for this elusive publication. It took several searches with several different search engines and variations in keywords, but I did end up finding two published items that may be what HC was remembering. One is a full fledged magazine bearing the name of *300 Baud*, and one is simply a magazine column, but it bears the full correct name of "Life at 300 Baud."

When I was looking for this publication, the first thing I did was run a simple search (Life at 300 Baud) though my go-to search engine (DuckDuckGo). Almost immediately, I found a web article that was discussing a magazine called *300 Baud*. I then checked the Internet Archive to see if this magazine was available, and much to my delight, I found the entire limited run. I continued the search by putting my first search term in quotes to look for an exact match in DuckDuckGo, and also ran a search with the meta-search-engine Dogpile. With these two searches, I found an obscure reference to an article in a column called "Life at 300 Baud," and also an interview with an investigative journalist who appeared to have written this article. Interesting. Next, I looked at Google Books, and found a couple more references to "Life at 300 Baud" articles. Armed with some of the information from the interview, I decided to look for the magazine containing this column. It looked like it was a magazine called *ProFiles* that was written for users of KayPro computers. I searched DuckDuckGo for "Kaypro users magazine profiles" (without the quotes), and found this magazine on the Internet Archive. Sure enough, the "Life at 300 Baud" column is featured in many of the issues. I did run more searches, but ultimately didn't find anything more. With all the searching out of the way, I could now study these magazines closer.

The first publication that I found, *300 Baud*, was a periodical about retro computing that ran for three issues, starting in January 2010. It had a good article selection about all sorts of cool stuff, from using the Internet with old computers to soldering without burning your fingers. All three issues are available for free at this location on the Internet Archive: `archive.org/➥details/300baudzine`

The second publication that I found is more likely to be the one we are looking for. "Life at 300 Baud" was a regular column in a 1980s computer journal called *ProFiles: A Magazine for Kaypro Users*. "Life at 300 Baud" was written by the investigative journalist Brock Meeks, and can be found in most issues of the magazine, beginning with Volume 2, Number 3. It makes for fun reading, with many of the articles exploring different facets of the old Internet, and providing interesting insights into different kinds of bulletin board systems. A nice digital archive of the *ProFiles* magazine is available at: `archive.➥org/details/kayproprofiles`.

I was intrigued by HC's missing publication, and when I dug a little deeper into the more musty corners of the Internet, I did manage to find a thing or two. I do hope that one of these publications turns out to be what HC was looking for. Even if this isn't the case, it sure was fun to conduct an in depth search like this, and I am happy to have found some interesting new reading material.

Useful Resources

- Article about *300 Baud* magazine: `www.➥apl2bits.net/2010/07/19/300-➥baud-magazine/`
- Interview with Brock Meeks: `www.➥digitalriptide.org/person/➥brock-meeks/`
- *300 Baud* magazine archive: `archive.➥org/details/300baudzine`
- *ProFiles* magazine archive: `archive.➥org/details/kayproprofiles`

Search tools that I used:

- DuckDuckGo: `duckduckgo.com`
- Dogpile: `www.dogpile.com`
- Google Books: `books.google.com`
- The Internet Archive: `archive.org`
- The WayBack Machine: `web.archive.org`
- WorldCat: `www.worldcat.org`

Hey, I Paid For This Cabin

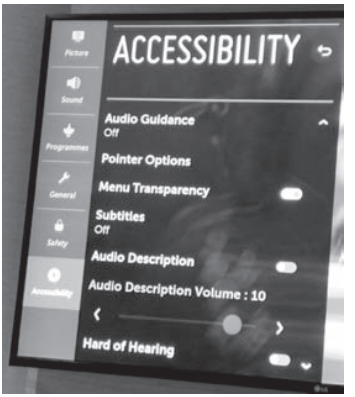
by the6thv3n0m

The information shared in this article isn't some sort of mind-blowing hack, but just serves as an example of what can be accomplished when you have a hacker mindset.

First off, the obligatory disclaimer. This information is for educational purposes only and I bear no responsibility should you use it in a malicious way.

So my wife and I just recently took a cruise. Anyone who has taken one before may notice that the TVs in the room typically have the sleep and/or auto power off timer set to turn off the TV at a set time (typically four hours). This may sound a bit petty, but both my wife and I are used to leaving our bedroom TV on all night at home and tend to get upset when during the cruise, if we happen to be in an inside cabin, we wake up to a completely dark room. While we both have gotten used to the sound, one of the main purposes at home is that it acts as a source of light should one of us need to get up in the middle of the night. Anyway, on most, if not all cruises, they will provide a very generic remote control like the one pictured below. If you've been on a cruise, you may immediately recognize it.

As you will notice, given that it's just a generic remote control, there are no buttons available to provide access to the TV settings. My goal now was to figure out how to access the settings for the TV to allow me to either change or disable the sleep timer and/or auto power off settings. After trying a few various button combinations, I stopped and really took a good look at the remote. I then thought that cruise lines, given the large number of passengers they have to manage week after week, would probably have this set to something that is relatively easy to remember and access, but would not seem as clear to the average passenger. Giving it a bit more thought, I asked myself "what would be the least-used button on the remote?" Given that there is typically an overlay system providing all the features (i.e., viewing account, ordering food, viewing ship activities, etc.) pretty much every button on the remote is used to maneuver except one, the mute button. So I pressed and held the mute button. A colorful circular graphic appeared on the center of the screen and behold, the settings for the TV appeared (pictured below).



I now had access to all of the settings, and therefore full control of the TV, including my primary goal: the ability to now change and/or disable the sleep timer and/or auto power off settings (pictured below). I immediately located these settings and disabled the option, which now left the TV on until either we manually turned it off, or the cabin stewards did.

Performing some additional exploration, I noticed some other interesting things such as the fact that although this was a smart TV, it was not configured with any network information. There was also the ability to disable the overlay mentioned above. On Carnival Cruise Lines, this overlay is called HubTV, for example. When the cruise was over, I restored any settings that I changed. Since they remained unchanged for the duration of the cruise, it wasn't clear if they would be prior to the next round of passengers boarding the ship.

Hope you found this interesting.

Hacking involves a different way of looking at problems that no one's thought of. - Walter O'Brien

An Atavistic Freak Out, Final Chapter

by Leon Manna

This story is a work of fiction.

When they arrested us, I had dyed half of my hair light brown.

"Your honor, I'd like to begin with the fact that a recent malfunction in the FBI offices of the witness we will be having sworn in, Segev Bezalel -"

"You pronounced his name wrong, it's Bitch." This came from the defendant's table, and then a fake cough. The witness snickered from across the room. The judge yelled at me to shut up or I would be held in contempt of court.

Lenny continued. "Segev Bezalel, whose evidence room caught on fire due to a malfunction in the thermostat, has been unable to produce any evidence so far tying my client or I to any of the charges that are currently levied against us."

Some guy from the district attorney's office shouted that he objected for the millionth time that day, and his motion was not sustained, although quite a few were. They ended up calling Moe to the stand to testify. The prosecutor asked him about the intrusion that corrupted all of the computers and servers in his office.

"Yes, somebody installed malware on all servers and computers in my office."

"And who do you think did it?"

"Leon Manna."

"How do you know?"

"A combination of the childish message and Leon's real capabilities to do such a thing. The planning was characteristic of Leon's previous plots, such as Sawtooth."

"Sawtooth, where he was seen doing fraud in person?"

Fuck.

"Yes, exactly."

Fuck, again.

He asked a few more questions. Soon after, Lenny went in on him. "Tell me, Mr. Bezalel, about the IP address that was associated with this attack?" He had a look on his face like he was planning something.

"It was some kind of uh... proxy." He stuttered! Sweet-mother-of-god, here it comes!

"And where, exactly, was this proxy located?"

After a brief pause, he said, "Turkey."

"Were you able to get jurisdiction in Turkey and subpoena this server?"

"No."

"Then how can you be so sure this was tied to me and my client?"

"It was timed with your planned escape."

"Did the exact same attack not happen in multiple other locations nationwide? How can you be so sure that this wasn't some act of planned terror by a greater force and not some vagrant who wanders across the country? My client isn't capable of something that meticulous, at least not in that timeframe." I made sure to do the same thing a bunch of times. Everywhere. A lot of places. As many as I could. I am god. I am not an American terrorist.

"Well... I mean... Technically... No."

"I heard Sawtooth was mentioned, how can you say for sure that it was my client? How do you know?"

"We have CCTV footage of your client in the bank, as well as witnesses." He did not sound confident.

"Have? Or had."

"Have."

"Where is it?"

Segev glared at Lenny. The judge told him to answer.

"We're working on that."

But Lenny continued. "Sawtooth was robbed by a man named Joseph Erickson. As far as we know, Joseph Erickson is dead. And as for your evidence, it was destroyed in an act of terrorism, *from an outside source,* combined with a malfunction in the evidence room. Was it not?"

Moe chuckled, and said, "It was."

"Is that the case? Then how come Sawtooth was unable to recover the footage

from their own system?"

"That information is classified. We don't have to tell you. We're not going to tell you. Leon knows, why don't you ask him?"

Lenny paused, and gave him a strange look. "You're aware perjury is a crime, right?"

Moe continued to give Lenny the death stare.

"I rest my case."

Then they brought in the bane of my fucking existence, Khir, who got on the stand for 15 minutes but was ultimately unable to say for certain that I was the man he saw in the bank. My disguise was so half-assed, but despite what I thought, worked. Thank you, uh... What was his fucking name... Joseph Erickson! Thank you!

Liz denied sitting next to me on the stand due to the fact that there was now no CCTV footage and nobody was present in the room when she uh... *didn't* do this and the prosecution was unable to get anything useful out of her.

They pulled the clerk from the car rental place up. She said she couldn't identify me (I'm a shapeshifter) even though she definitely could, did not feel like ratting me out, and was willing to lie under oath for me. I smiled at her. She smiled back. I didn't technically go in there. Somehow she seemed prettier than before. From across the courtroom, she looked like an angel.

They were unable to get in contact with Aryana. Probably for the best. Hope she's okay, though I heard she still hates me. I think she moved to Europe and found a nice French boy. John Capper refused to testify for obvious reasons. He was arrested on a failure to appear warrant, and was sentenced to 15 years for murder when they tied him to the crime. I think I disabled the script on their server while I was blacked out on bromazepam. I don't remember. May went missing and is presumed to be dead, which *totally* happened and is 100 percent true. She has them fooled though. I think she's a contract killer now, or some shit like that. Unconfirmed reports, but I know it was her. A woman matching her description was seen with several men who later died of cyanide poisoning. Goldstein also did not testify; he was busy testifying for a different case. I think they understood the nature of, well, Goldstein, and gave him a pass on that. Pierre moved to Ireland. Quite often I like to imagine he's still out there somewhere, riding out on the water. Right now he is a fugitive. Ireland did not extradite him, if they ever even found out that the fake identity I set up for him there was a fake identity.

The only charges we couldn't beat were the drug possession charges. A couple misdemeanors, one felony. I spent ten days in a state hospital for an evaluation before they released me on probation, under the conditions that I participate in an intensive outpatient program and if I fail drug tests or fuck up at the IOP, they will send me to jail or a mental hospital. Again. Mountain View State Forensic Hospital. There were people in there who hadn't seen the sun in years.

I got a call from Segev when I got out. "You tryna smoke?"

I said yeah. Even an FBI agent can break the rules.

And in the end, I learned nothing. There doesn't seem to be some kind of moral to the story here. I just couldn't figure it out. I was so close. By only a hair, they got me. But that hair was just in reach.... What if I had done it right? What if I had gotten away to Cuba? What if I hadn't mistreated my ex-girlfriend? Then it hit me like a bolt of lightning.

Hah hah hah.

What if I did it all again? I sat in my apartment for a moment, thinking. Then, in the blink of an eye, my new name is Lee Williams. Lee Williams was born into this earth through a Ring Zero rootkit I installed on an SSA machine a lifetime ago, just like Leon was all those years back, and he was a new man, born again, for a second trial. A fallen angel, if you will. Which you won't.

Then, I reached into my drawer, pulled out a check, and the outworn chase of money continued.

Enjoyed "An Atavistic Freak Out"? Buy Leon a coffee!

`BTC: 39L63B9qAiAnPbqqLZempJQG8xeXVRFvYT`

Land Mines

HOPEward Bound

Dear *2600*:

I will be submitting a talk soon for consideration, but still wanted to purchase a ticket while they're available. Thank you *so* much for organizing this! I was there in 2016 and it was a really special time. Hope to see you soon.

Halley

We thank you for your support. As of now, there is still time for people interested in submitting a talk or workshop to our upcoming conference. It's going to be an historic event. Full details can be found at www.hope.net. And your ticket is free if your talk is accepted!

Fixing Phones

Dear *2600*:

Recently, AT&T accidentally killed my dad's Samsung Galaxy S7 which is 4G and compatible with their network. They thought his phone was stolen since the original account holder (my mom) had passed away. His name is on the account. Anyway, it's been three days now and they cannot get his phone to work (as in call or receive calls). Is there any way on our end to somehow deprogram AT&T's kill code? Or are there only two options: asking them to replace the phone or buying a new one?

Barry

This should be possible, but it's likely all of the data was wiped from the phone. Between AT&T and Samsung, this seems solvable, but you need to convey that it was their mistake in the first place so they feel some obligation.

Dear *2600*:

My mother has dementia. She lives out in the desert with my tech savvy father. She walks daily up and down the road with a neighbor and by herself. She knows the area and feels safe (and we feel comfortable with her doing it, the community is constantly driving on the road and people always stop to say hi and chat, and don't hesitate to help if needed). We don't want to take that independence away from her, but at times it gets scary.

She recently lost her iPhone and it was dead, so the Find My iPhone app was useless and the problem was solved with just getting her another phone. Her phone is her lifeline and, as a retired realtor and social person, is a must for her. Texting, calling, emailing is second nature for her (even though now it gets confusing).

I had a coworker tell me about how her young teen just got her first phone and about the app she put on it that literally gave her access to GPS, microphone, video, texts, calls, and whatever else. I looked up the website and it was an app you downloaded, a monthly fee, and the app showed up as a calculator app and you put in a code to access it. This was like a decade ago.

What do you recommend? I want GPS, video, and microphone. I don't want to say money is not an issue - there are a bunch of free apps out there and I just want something reliable.

Max

Ironically enough, the app you're looking for is known as a "parental control" app, which is kind of the reverse of what you want to do, but the description still works. The features you're looking for are almost identical to what parents want to control on their teenagers' phones. Assuming having pornography sites blocked won't be an issue, we believe this could easily work for your needs.

We suggest searching for these "parental control apps" online and trying them out before committing. The average cost is around $50 a year, which is well worth it considering that support and updates are usually included.

Dear *2600*:

I was having new fiber service installed and got talking to the phone engineer. He was telling me how the U.K. is going to be turning off their analog public switched telephone network (PSTN) service in a few years and you would only be able to get data/VoIP services. Kinda made me a little sad, as I have great memories of me and my friends messing with the analog phone system, opening the BT box in our estate, connecting our homemade linesman set, etc. We even found a guide on a phreak message board on how to physically get into most local BT exchanges. That adventure is what set me off down the IT/technology path. Do you think that would be the end of phreaking or do you think it can live on in a VoIP world?

Michael

It's always going to be possible to mess around with phones, no matter what form they wind up taking. And there will always be new devices that we haven't even imagined yet where our imaginations can roam wild. That said, it certainly will be a great loss to not have analog phone service, a phenomenon we're slowly witnessing in the States. We think it's always best to mix new technology with old, as there will always be times when the newer systems will fail. For instance, during extended power failures, your local central office typically had enough battery power and generators to keep your phone connection working uninterrupted for weeks. Newer fiber systems only last a few hours without power. Cell phones have other issues. During catastrophic events when you need a phone the most, a cell tower can lose power or connectivity, making your phone useless. And if you lose power, it will be difficult to charge your phone. During last year's hurricane in New

Orleans, government officials were unable to call the local television station to share information for precisely this reason. Those with old-fashioned landlines had no trouble getting through.

In the end, it all comes down to profit, and the copper network just doesn't provide enough of that for phone companies to continue investing in it. We believe there needs to be a way to keep it running in order to provide enough of a backup in the event of a catastrophic event. They do tend to happen.

Observations

Dear *2600:*

BBC *finally* set up official Tor mirrors and introduced Tor to their viewers/readers. Links are below. Believe it or not, Facebook can be officially accessed using Tor too.

(facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mh ➥bshg7kx5tfyd.onion).

"The BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts. The Tor browser is privacy-focused software used to access the dark web. The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship. Countries including China, Iran, and Vietnam are among those who have tried to block access to the BBC News website or programmes.

"BBC News in Ukrainian:
https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion/ukrainian
"BBC News in Russian:
https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion/russian
"BBC News internationally:
https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion."

Ilgaz

This actually happened back in 2019, but its importance is being realized now. Of course, the hardest part can be getting the news about the existence of these links out to the affected people. We are learning a lot about control and blocking of the net, and clever ways of getting past these restrictions. The hacker community is key in making that happen.

Dear *2600*:

The information super dirt road! In America.... Get a "forbidden" message trying to access RT News from home through AT&T, but it pulls up fine on my phone. Nothing like good old fashioned thought control.

Robert

Thought control is closer to what is being blocked. You will always be able to find a way to access the lies and hatred of the Putin regime as you've demonstrated. But nobody is under any obligation to help them spread their message. Sites with illegal or terroristic content are generally shut down or blocked. Why should this state-sanctioned propaganda site be treated any differently?

The sad fact is that no matter how much evidence is presented from independent and reliable sources, it will never be accepted by those with a vested interest in continuing to spread lies. We can either continue the dance into perpetuity or take a stand for justice. It really shouldn't be a hard choice.

Dear *2600*:

I was just watching the movie *Hackers*. There was a part where Dade asked his buddies if they knew who Acid Burn was. They said no. But later they did know.

Rostislav

This is actually true. Our theory is they were simply lying. We know this never happens in the hacker world, but it's possible.

Dear *2600*:

The Russians tried stealing my wife's Microsoft account today. Do your worst.

Kaleb

It didn't take long for them to up their game, did it? This will surely be their undoing.

Dear *2600*:

The AWK keyspace iterator should have been written in portable C. I apologize for the inconvenience.

Justin Parrott

It happens. But AWK is nothing to be ashamed of.

Dear *2600*:

I opened an AOL account in 1993 and haven't touched it in 15 years. Holy shit, it's still there. I just logged in.

Chris

This is what digging up an old bone must feel like to a dog.

Dear *2600*:

The Ukrainian military has an "IT enthusiast group" within their ranks that travel around on quad bikes and use drones to drop bombs on Russian tanks. This is every IT desk jockey's dreams realized.

Alex

No reason they can't outsource to bored employees around the world.

Dear *2600*:

Weird first world problem: I use Keepass to store and generate long, complex passwords. If the website allows it, I use caps, lower case, numbers, and special characters and use 20 or more total characters. My problem is that when I'm typing these numbers into my phone, I have a hell of a time telling the difference between a 0 and an O or an I and a l. I end up having to copy my password into MS Word and then change the font to an easy to read font where the letters are unambiguous. That's all. I just find it a little funny. I would not have had the same challenges on a Commodore 64 or Apple][. The fonts on those early devices were pretty well designed for being so low res.

Charles

We're told you can indeed select a different password font. But we know this has been a problem

in many places. And a rather funny one, too.

Submissions

Dear *2600*:

I sent this to another website, so I am disqualified now.

submitting

While true, we still felt it was good enough to share with our readers. So we're including it as a letter below:

Dear *2600*:

I didn't know I could be called a hacker until recently. I have some computer skills, but that's not what would make me a hacker. When someone mentions "hacking," it usually presumes pentesting, programming, or cracking. Those are aspects of it, but what does it take to be a hacker? I think a hacker is someone who is driven to achieve their goals, almost obsessively. I think a hacker demands to live life on their terms, by their own compass, so to speak. Hackers not only want to live life the way they want, they also have the intelligence and ability to make it happen.

When I was young, I read everything that interested me. I wasn't very social, so for many years I had books as my company. I developed talents for writing, psychology, and computers, along with an interest in art and music. I was, maybe still am, a divergent thinker; I thought for myself and I felt good doing it. As a result, I wasn't interested in what the educational system had planned for me. I was not only placed in the "gifted" classes, but I was also held back a grade! My lack of interest had gotten me branded as a failure. My attitude towards the educational and economic system was completely soured. Today I live with my parents and am ineligible for employment. I recently thought that I should have known when to compromise. Still, some things are worth standing up for even when you know there is a cost.

I also learned about P2P systems. Finding and sharing files with people over the Internet brought in exciting new concepts that I wouldn't find anywhere else. They helped define my tastes and skillsets. I was really lucky to be a youth in the mid 90s. I don't think everyone realizes what they are giving up when they delegate their lives to companies like Facebook and Google. I have wanted to live free from interference for my whole life. For quite a long time, I thought that meant fighting the government and corporations.

After school came the insanity. I developed schizophrenia and lost everything. I was housed in a community assistance program. I think most people that I knew expected that my story was over. No! I was pretty messed up for a while. I later had a change in environment and I regained my ability to self- regulate. I learned the skills I needed to get back in control of my mind. I also did very well socially. I didn't give up on myself, I just needed time and a plan. I think it's important to always have a plan. Be willing to change them if you need to.

submitting

This is a great story and deserves to be shared. We think there's a lot more you can say which will enable it to qualify for our "Hacker Perspective" column in the future. As the above was already published online and now printed in the magazine, it would have to be rewritten. But the good part about that is that this version is relatively short, which means there's much left to tell. The column itself needs to be about 2500 words - significantly longer than the above - but we believe there is a great deal more insofar as experiences, philosophy, and, of course, the changing technology of the times described. Like growth itself, there are challenges, setbacks, and surprises when putting together a piece like this. We hope you take the time to tell the story; we believe many of our readers will be interested and inspired.

Dear *2600*:

I'm a network engineer with one of the *big* ISPs out there, and I've bumped into a few things having worked in data centers, backbone (yes, the Internet and P2P connectivity to everything inside my company), and most recently with my IP management operations team. I have a couple of ideas for things I've seen and worked on regarding securing the Internet, and massive hacks I've experienced (I'm talking about things that brought Cisco 9K routers to their knees). Was curious if you'd be interested in this kind of thing?

Chaz

You have us at the edge of our seats.

Requests

Dear *2600*:

I need a login seller
Like Bank logins...
CC logins
Local bank

Hills Mary

Tell us honestly - does this approach ever work? We strongly doubt you can say anything honestly, but it's worth asking.

Dear *2600*:

Hey, is it okay with *2600* if my friend who runs an online publication reprints the *2600* article I wrote? Thank you.

Michael

It's your article, so you can have it displayed anywhere you wish after it's printed in our pages. As a general rule, we ask that the author and magazine are attributed.

Dear *2600*:

I want a link to download fb account

Pramod

Just once we would love to pursue this sort of inquiry to see just what on earth is expected of us. No details of any sort are ever given; we're presumably expected to read people's minds and furnish them with the exact info they're in need of. We can only assume that what's being asked for here is a universal link that allows someone to download any Facebook account anywhere. Because that's what we're all about.

Dear *2600*:

Subject: Article for 2600
teach me how to become a hacker

Florianus

We're curious if other fields of study get people sending these one line requests constantly, expecting to be injected with wisdom and knowledge through the Internet. What was particularly ironic (and disappointing) here was that this email was entitled "Article for 2600" so we were expecting something truly awesome.

Inquiries

Dear *2600*:

Aside from *Sneakers*, what are some other 70s, 80s, and 90s era hacker/phreaker movies or shows?

Matt

We'll open this up to readers so we don't play favorites and/or leave out worthy candidates. But we suggest also including the decades prior to and after your date range. And while there are a bunch of films and television series that focus primarily on hackers, there are even more that touch upon them briefly, as a single episode or small part of a film. And, of course, don't limit yourself to only American material. There is a great deal from English-speaking countries like Canada, Australia, England, etc. Nor should you limit yourself to that either, as there is a ton of material in different languages from other countries that you can see dubbed or with captions. Among all of these, there are examples that are so terrible that they're really worth sharing. And there are also classics that are found in the most unexpected places. We will be happy to share reader opinions on these.

Dear *2600*:

We are two college students from the University of Paris majoring in a master of cybersecurity. We are requested to publish an article in a hacking magazine. We are currently working on an xml injection article and we would like to know if you could help us with publishing our article. If the answer is positive, we would need to know your deadlines and if we have to have a certain template for the article that we'll be doing,

Lylia & Moncef

This is rather unusual, as there aren't that many hacking magazines around, so this assignment seems designed with us in mind. Anyway, you're more than welcome to submit your article to us at articles@2600.com with as much detail as you can include. We prefer straight text, but any format will do. As for deadlines, we're always working on future issues, so that's not something you need to worry about. Just send it in and, if accepted, we'll have it printed in a future issue. Good luck!

Dear *2600*:

Sorry if this is a dumb question. I'm curious to get my hands on a red box to have for conversation and to potentially play with. Is that something I can buy somewhere or do I need to build one?

Matt

Definitely not a dumb question. Just don't expect to be able to use it to make free calls from payphones anymore. There are plenty of schematics available online if you actually want to build one. It's also incredibly easy to generate the tones with virtually any audio software. The tones are simply 1700 Hz and 2200 hertz combined. A nickel is represented by that tone played for 66 milliseconds while a dime is two instances of that tone separated by 33 milliseconds. A quarter is a little different: the frequency is only played for 33 milliseconds and each of the five instances is separated by 33 milliseconds. (They really should teach this in schools.) If you're looking for an actual physical red box that someone may have used in the past, that seems like a great thing to ask for in the "Wanted" section of our own Marketplace, which is free for subscribers.

Dear *2600*:

We are two students in cybersecurity Master's Degree at the University of Paris, and as part of one of our classes we have to publish an article about the way we could build undetectable ransomware in Python in 2022, avoiding Windows Defender.

Do you accept article submissions? If you do, what is the process to do so? We thank you in advance for your help.

Barrault & Fabi
University of Paris, Paris, France

So how many of these are we going to get? Are you all in the same class? We can't wait to start getting all of these French articles.

Dear *2600*:

Why the name *2600*?

Max

Every couple of years, we're obligated to answer this question. 2600 hertz was a frequency used by the phone company. If you sent it down a long distance connection, you basically seized control of a long distance trunk and gained the ability to route calls throughout the world using special multifrequency (MF) tones and completely bypassing billing. When naming our magazine, those numbers were the perfect symbol for what we stood for: exploration, technology, mischief, and occasional free phone calls.

Dear *2600*:

What email list server do you guys use?

Kris

As we tend not to trust outside companies for this sort of thing (they tend to disappear, impose policies we can't live with, or violate people's privacy), we've been relatively content with Mailman. Except for the things it does badly which drive us crazy.

Dear *2600*:

I've got a very good question! What does your passport say when you travel to another country where you owe a traffic fine or appear to be due in court? Will my crimes in France show up in America? Will my past traffic citations show up when I return to Australia or America or Europe or any of those countries?

William

Yet another France-related letter. To answer your question, it really depends on what your crimes are. If, say, Vladimir Putin were to go through passport control in virtually any country in the world, all sorts of alarms would go off. Your traffic tickets aren't going to interest anyone at a border unless they involve a stolen car that you're attempting to drive over that border. Your passport only contains info that is then cross-referenced in various databases. Your identity may be flagged if you're a wanted criminal or on a particular country's list of undesirables. Your traffic tickets could, however, pop up if you try to rent a car and present your driver's license. Good luck with whatever's going on here.

Dear *2600*:

One of the big discussions in the cybersecurity industry right now is whether or not destructive tools are covered by the Second Amendment. Cryptography will likely be contested at some point, and the likely scenario there is that the Fourth Amendment will cover your personal right to strong cryptography. But hacking tools, especially those designed to cause damage, are more like weapons. Owning malicious software has never been a crime, nor has writing malicious software. But as the ability to cause real world damage increases, there will probably be attempts made to limit access to them. A key difference between a software tool that can damage an enemy's computers and a weapon that can kill a person is that the software tool only has that one purpose. It isn't by design a defensive tool, nor do you need one for any purpose other than to harm someone else. But I'm curious what you think. Will hacking tools designed to cause damage be targeted by governments? What about those who use them, or who built them? And if so, should those be covered under existing laws?

Chilton

Amendments to the United States Constitution mean nothing in other countries, so that right there tells you how difficult it would be to eliminate such tools - or to guarantee their protection. And it wouldn't take much to define a malicious bit of software designed to damage specific hardware or software as a defensive tool, in much the same way this logic is used with physical weaponry. One thing is clear: most governments lack a clear understanding of technology, so they will attempt to control things they have no power over. It's certainly possible for penalties to be enhanced if a crime is found to have been enhanced by a specific tool. It happens all the time.

Dear *2600*:

I'd like to ask a question. I am looking for info about the *2600* meetings in Paris, France.

It used to be on the first floor of the Burger King at Republique, but now I cannot find any info any more.

I'd be grateful if you could help me because I'd love to join the meeting if it still exists.

Tatiana

So all of the hackers are in France now apparently. That's fine with us. Concerning the meetings, as of this writing we haven't heard from anyone in France interested in restarting them after the pandemic. Since there are clearly a lot of interested people over there, it's only a matter of time before someone writes in to meetings@2600.com or DMs us on Twitter (@2600Meetings) with location info. It could be you.

Dear *2600*:

Why does the mag not follow the season at the real time? Autumn was released in December and Winter in Spring.... When will you come back to the real seasons? Thanks for the info.

Discovery

This is a direct result of the craziness of 2020 when we were severely affected by COVID-19. Bookstores shut down, issues were thrown out, and we very nearly didn't survive. When the dust started to settle, we were behind by a bunch of months. We didn't want to skip a season or "catch up" by putting out a double issue. Since we're not really tied to seasons in the first place, we felt the best way was to cut time off of each issue's shelf life and get closer to a normal schedule with each passing issue. We had a decent plan in place that would have had us caught up by July 2023, but then our printer had a supply chain problem with paper and we had to push that back to the end of 2023. But we're making steady progress and the day will come when you see the season printed on our covers and at the bottom of our pages once again. We look forward to it.

Further Info

Dear *2600*:

In a recent issue of *2600* (38:3), you received a letter from a Roscoe Village alderman's intern requesting that you address the beat-up *The Hacker* newspaper box in their neighborhood. I have some un/fortunate news.

The box in question is actually owned by *The Heckler*, a relatively well-known (in the area) satirical sports publication. I find it amusing that this intern was not just unaware of *The Heckler*, but also went on what must have been a great trip down a hacker publications rabbit hole and ended up on you.

Enclosed is a nice shot of the box from Google Street View, with a very legible *The Heckler* logo.

J0hnnyXm4s and the Chicago *2600* crew

Thanks for helping to solve this mystery. It's proof that not only do we get blamed for the misdeeds of hackers everywhere, but hecklers as well. But we're thrilled that not only are there still newspapers, but sports newspapers, and also satirical sports

newspapers. We love surprises like this.

Dear *2600*:

I never knew this... saw it on Twitter. If you want all images from a .docx file, just rename it to .zip and extract the media folder.

Austin

And who says you can't learn something from Twitter?

Dear *2600*:

Hello fellow readers of this insanely amazing magazine! Fellow reader since the 90s here! I thought this little challenge might appeal to you all. We have been working on a way to safely transmit signals for our trading systems (and other systems) end-to-end by encapsulating the data into something like the following:

052827154109282846109285912054799621027263066004309903114730008026646308097948174114729050

But we'd like to make sure that no one can actually figure out what it says without us telling anything about how the string was created. Your job is to decipher it. If you figure it out, send your solution to tcarey1053@emailinterface.org. Good luck!

sky henrikssøn

Readers, please don't miss the summer trying to figure this out.

Dear *2600*:

I am writing a horror novel. It is called *Legacy Code*.

Arne

We hope it's more verbose than this proclamation.

Thwarting Security

Dear *2600*:

I found a hilarious way to get around select news website paywalls. In some cases, simply turning on reader view - in Firefox or Safari - washes away all signs of having to subscribe. So far, I know of three websites that this works on: *The New York Times*, *The Epoch Times*, and the *The Daily Wire*. Maybe these websites should consider patching this hole.

Snake in a Lawn Mower

We're sure they're considering that right now.

Dear *2600*:

Me: "I'd like to test your color laser printers please. I'm looking to purchase one for my home office. I brought a sample of what I would be printing often on my USB flash drive."

Staples Clerk: "No problem sir. Do you need my help? If you need extra paper, let me know."

Me: (on the way past the print center on the way out): "Hey, how much do color copies cost?"

A customer doing their own self-printing: "$.57 per page."

Me (pointing at the printers for sale section): "Wow, well I just got $74.10 worth of printing for free just over there."

Hacking skills require innovative solutions to common everyday problems and you don't always need a computer, yes?

Johnathan

We doubt you could get away with that more than once in the same place. While an overall sleazy move, you get extra points for rubbing it in with the poor guy who was following the rules. And for instantly calculating what your 130 pages would have cost.

Dear *2600*:

Would *never* do this, but on American Airlines, Sprint users get free Internet. When it asks for your phone number, I bet you can just keep upping your phone number by a digit until you are matched as a Sprint user.

Eric

It's not quite that simple. First off, these deals are always changing. And T-Mobile has taken over Sprint. Beyond all that, you generally need to have your phone with you, as you're using it to connect in airplane mode. But we're certain there are many tricks you can play while in the air, including sharing the connection you eventually get with others.

Dear *2600*:

This is something I discovered several years ago, brought to the attention of my employer and the software publisher... but no fix has ever come through. Figured it was time to suggest that other people fix their systems. If your employer uses SMAtechnologies.com's product called "OpCon," you need to look and clean up a serious security issue this application installed on your system (if you haven't already).

One of the secrets to how it does its thing is by installing a public key for access to the root account of the target UNIX system. The public and private keys for this account are included in the application distribution file. The public key is installed without notice or prompting, and it is the same key pair used on every single OpCon installation - it is *not* locally generated. So every administrator of a system with OpCon installed on it has root access to *every other OpCon server in the world* they can get SSH access to. I think that's kinda bad.

At my employer, we discovered we could remove the key without any impact on our operations. Apparently this was part of a magic "move files between machines" function we didn't use, in spite of using OpCon extensively.

After discovering this problem, we implemented stuff to make sure that the key didn't get reinstalled, as it did after every OpCon update. The key you want to remove looks like this: "ssh-rsa AAA**{...}**3wfcDE= root@redhat4as". Yes, it is a very old RedHat generated key. This was pulled out of an AIX system, but it appears to be the same key for every install.

Honestly, it scared the crap out of me when I found it on all our servers - a key with a completely undescriptive identifier field? I was quite afraid all our systems had been compromised. The key files exist in the distribution .tar file as bin/sma_id_rsa and bin/sma_id_rsa.pub.

SMA Technologies was not aware of this when I brought it to their attention, and it took several iterations of explanation before they set up a

conference call to discuss it with me. I had to explain to them how SSH worked, how key logins worked, and why a 15-plus-year-old common key for all OpCon installations was a really bad idea, and installing it on the root account was a potential disaster... at which point I heard a quiet "oh shit." And nothing more after that, other than repeated "we are working on it."

Nick

This was shared on one of our Facebook groups, so we certainly hope it's been fixed by now. This is the kind of alertness we all could use more of.

Ideas

Dear *2600*:

OK, crazy thought: electricity and water being so similar in their behaviors (always flowing to low ground; susceptible to resistance, capacitance, and other forms of flow control), it's possible to construct a water-based Turing machine. So in theory, a city's plumbing and sewage system could be designed to also perform computations. Obviously, it would be extremely inefficient, and probably inconvenient for the city's inhabitants, but theoretically....

Deva

Theory is what we live for. Remember, Charles Babbage is considered "the father of the computer" and he lived in the early 1800s, before the age of electricity. We doubt you'll get any grants for this kind of research, but it's sure fun to imagine.

Dear *2600*:

I am not a cryptographer. I am an amateur mathematician. I read Steven Levy's *Crypto* book where Whitfield Diffie traveled the U.S. inventing public key cryptography before it existed. I read about the RSA encryption scheme and thought I'll take the simplest explanation and see if a pattern existed in the multiplication where N=p*q, knowing only N. I believe there are patterns that can be seen in many different equations, three of which I list below - where N=p*q, p being the smaller factor and q being the larger.

Crypto is popular due to cryptocurrency. These equations are specific to the prime factorization problem where a large semi-prime number is factored into two prime numbers, but I hypothesize it could be expanded to logarithmic and modulus problems. I do not know how the prime factorization problem would affect cryptocurrency, but it will break the one way function of RSA.

The equations are complex, but only algebra. There are multiple variations. But I believe in these equations. I even advertised in *2600 Magazine*. I post in a letter and not an article because I have posted these equations on message boards. Also, on first inspection, no one knows if this is correct. So I wrote a letter hoping that some cryptographer will read it.

p^3 - (p^3*N^2) / (N^2 + p)
p^3 - (N^2 p^3)/(N^2 + p)
p^3 - \frac {N^2 p^3} {N^2 + p}

The above equation should be close to zero, but sometimes the error is closer to one.

(p^3 *N) / (N^2 + p) = fraction
fraction/ p = fraction / (N /p)
Sqrt[fraction / (N /x)] * N = p^2

The above equations are the second example.

q = Sqrt[(N*q^2 + q)/ N]
q^2 - (N*q^2 + q)/ N is approximately 0
In the case where N = 85 and q = 17,
q^2 - (N*q^2 + q)/ N is 1/x or 1/5 or 0.2
0.2 * 85 = q or 17 in this example

Bobby Joe Snyder

And if some cryptographer has a comment on this, we will print it.

Memories

Dear *2600*:

Anyone from the 80s remember running your computer overnight to collect 950 Sprint calling codes? Good times.

Paul

*That was one activity, although long distance dialing codes were so insecure at the time that they could even be guessed without the help of a computer. The real fun was in the exploration of phone numbers, where you would leave a smart modem running overnight, dialing phone numbers in succession and logging any that picked up with a carrier tone. Sure, hundreds of phones would ring in the middle of the night. But there was no such thing as Caller ID or *69. Seeing that list of phone numbers the next day that led to computers - BBSes, dialups to secret networks, and more - was part of the magic that drove the hacker scene.*

Opportunities

Dear *2600*:

The F.B.I. 's Silicon Valley counterintelligence field office is seeking qualified people who can help protect computers and computer networks. I think that many readers of *2400 Magazine* have the expertise to lend a hand defending America during this very challenging time that has left America very vulnerable to cyber attacks that can shut down mission critical communication and computers that control electricity, credit card payments, gasoline production, food warehouses, traffic lights, television, radio, cars (cars have 4G modems that allow hackers to send remote commands to engines, brakes, etc.), etc.

Jeff

We'll be sure to pass that along to that weirdly-named magazine.

Dear *2600*:

I can clone your partner's phone and link it to yours without him knowing and recover all deleted messages and chat on his phone so you can see them.

Michael

We wouldn't be surprised if Michael could also see them. Not our recommended route.

Dear *2600*:

Can I trust you? I have a business proposition regarding shipment of gold bars. Get back to me on mg.brewer@beco-techinc.co for more details and as well discuss the terms and condition for cooperation.

SSgt. Brewer Michael

You can trust us. We can't speak for the tens of thousands of people reading this, though. But you knew that when you emailed the letters department, didn't you?

Dear *2600*:

Hi Eliza,

My name is Todd Weiss. I'm a former VP of a Fortune 50 company, so I'm familiar with the corporate grind. I've also experienced the benefits of owning two franchise fitness concepts.

I noticed that you work with *2600 Magazine*. If you're happy in your position there, that's great. And I genuinely hope you are! But if you've ever thought about exiting corporate America, I can help.

Todd Weiss
Franchise Consultant

Well, great. Now we've lost Eliza. Game on, Todd.

Dear *2600*:

Please do as much social engineering on this account as possible! Doing a search of his email and social media presence indicates he is very open with his details of his workplace between Canada and the U.S. and flowery preamble to complain to a company that has wronged him - message headers usually don't provide any info on the targets ("Undisclosed Recipients") but I love the way he spearphishes!

J.

Yeah, we're not going to get involved in whatever this is all about. Suffice to say that using spearfishing techniques to track down a spearfisher can certainly be fun, but it's best to play the game on your own and share your final results. Otherwise it can quickly spiral out of control.

Responses

Dear *2600*:

In response to the letter by Shocked998 (38:3), I have been reading *2600* shortly after it began and had been reading other hacking philes and mags prior to that and after that, although my support of *2600* has waned in the last decade or so and I'll explain why throughout this letter. However, Shocked998 mentioned a letter by 6NdLXzc2 in which they described 6NdLXzc2 as whining. I have not read this letter, so I am not familiar with the content. But, describing a letter as whining about the political bias of the magazine was a tip-off of where Shocked998 was going. So, I'm guessing someone said a bunch of things that Shocked998 didn't agree with, thus it became whining. Typical.

Well, I'll have to agree with the political bias of the magazine taking a really strange turn at some point in history. I noticed it as well, and it appears to be accelerating. After a long departure from *2600*, precisely because of this weird "political bias," I decided to try again with your most recent issue (38:3) and quickly discovered two things: the political bias is still there and the content is rather lacking in substance. It certainly isn't the magazine it used be.

So, now Shocked998 can write back again and complain of another "whiner." Shocked998 then says, "The hacker spirit is not sophism and conspiracies. The hacker spirit is not hatred and apologism..." Well, hacking throughout the ages has certainly entertained a multitude of conspiracy theories, conjectures, hypotheses, and so forth. So, not sure where Shocked998 gets the idea that hackers or the hacking spirit never dove into that arena because it has a massive history of doing so. This is especially true of UFOs and trying to figure out what projects government has done and what they were for and how they were carried out, covered up, financed, etc. Anyone who ever used a BBS system through the 80s and 90s knows this as most BBSes worth a grain of salt had scads of philes and discussion on such subject and often had government documents on various topics. So, yes, indeed, conspiracies were and are still very much a part of the hacking spirit. Further, apologism is a vast part of the hacking spirit, as even *2600* has made a documentary defending a position/person. The hacking community and *2600* are dedicated to defending the position of exploiting technology for the gain of and dissemination of information that other entities and/or people would prefer not be shared. The very nature of hacking pits one against someone else who does not want you to be doing what it is you are doing and places you into a position of defending your position and activities and why you share information. That is the very definition of apologism. So this statement by Shocked998 is very wrong in my opinion.

Shocked998 continues with, "The hacker spirit is not false equivalencies and bad faith. Instead, it is progress. As is humanity. Pushing the envelope and improving." Ahhh, no. That might be what you want it to be, but that is a false point of view in my opinion. The hacking spirit and/or the hacking community is all these things and more. Like anything else, the reality is it is full of good, bad, and all things in between. There is no prequalification to be a perfect righteous person before becoming a hacker. And there is no authority which rules over the ethics of hacking protecting the spirit of it. It is what is, man. It is an all encompassing subculture comprised of people with a passion to exploit, understand, and use technology... and the passion and drive behind this is not uniform across these people whatsoever. What Shocked998 describes is like the unicorn and rainbows version of hacking.

I can tell you that at the height of phreaking, most phreaks were indeed apologists defending their trade, craft, and practices in light of the fact they were basically ripping off the phone companies of the world, rightly or wrongly. And most phreaks wanted to place free calls, either to talk or to connect modems. And the reasons for this varied from just wanting to say hello to a friend to wanting to connect to a government system to see what could be found (conspiracy research, perhaps).

Then Shocked998 carries on with some biased views and arrives at "these radical idealogues cannot be convinced of anything that goes against their zealous belief. Whether it's trying to convince them that the vaccine does not have alien DNA,

microchips, or demon reproductive material; or trying to explain to them that rational and science-based public health messaging will change as new information is presented; or insisting that an attack on the nation's Capitol was not simply equivalent to a tour group, nothing seems to be enough," which is a lot to unpack, but points to an obvious and deep bias.

I've not heard of anyone talking about alien DNA in vaccines and I suspect that might have been said in jest in an attempt to make a particular group of people look ridiculous. However, even if I had heard of such things, I would listen. See, I don't really have too much of a problem listening, as it tends to offer opportunities to pick up new information and ideas that can lead to places and thoughts. I have, however, heard of people who are deeply concerned about the safety of these vaccines and who have very valid points and I have witnessed a concerted effort to silence these voices.

I don't know anything about demon reproductive material, but that does in fact sound very interesting. In fact, I would very much like to hear more on that subject and those ideas. As far as microchips, I personally do not believe there to be microchips, or nanochips, in the vaccines, however, the technology does in fact exist if it were to be used.

One thing Shocked998 has failed to acknowledge is that all forms of technology can be exploited for various reasons. All systems, especially control systems, can be geared toward good or bad purposes. Now, getting back to what I said about the hacking community and spirit, the biotech and pharmaceutical industries are hacking industries. Do they in fact subscribe to the hacking spirit as described by Shocked998? I think it would be naive and dangerous to believe that. It would be very naïve to assume that a control system, such as a government, or a health service, or a vaccine for that matter, is immune to being used as a vector to carry out evil or bad acts/plans. But from what Shocked998 wrote, I would read out of those words that that conversation wouldn't even be allowed by Shocked998. Hmm... now we get to censorship. Is that in the hacking spirit?

You see, Shocked998, you are not the gatekeeper or decider. If there were anything ever true about the hacking spirit or community, it was that dissemination of information was the priority and that each individual was his or her own decider of truth or fiction. And you should be damned, as in really damned, careful what you think is misinformation and what is not. Misinformation is typically a misnomer used by those who rather you know only what they prefer you to know and nothing else.

The hacking spirit and community I grew up with (late 70s to early 90s) consisted mostly of people who held their own personal beliefs but were willing to listen and allow people to have their say and we didn't freak out all the time on what people had to say.

ViSiOn/Strang'r

We'll keep this brief as you've already used a lot of ink. Believe it or not, we agree with much of what you say. The hacker community has always been open to a wide variety of views and has always considered all kinds of wild ideas as possibilities. That's what hacking is all about. But there's another part of hacking that's being left out of your analysis, one that is just as essential. We reach conclusions based on evidence, experimentation, and dialogue. Our minds can be changed when all of that is processed.

The resistance we're seeing is that of people who don't like the conclusions that are being reached. They seem to want a different conclusion and, if the facts don't support that, then the facts are deemed to be false. This is where our paths diverge. Then we then get accused of not listening or weighing the evidence when we've already done precisely that. And those making the accusations justify their conclusions with insufficient or faulty evidence. We are able to easily disprove them, but, as the original writer stated, we can never convince them of this. And that is what's not a part of the hacker spirit.

Sure, we've seen a lot of what you describe in the hacker world: being open to conspiracies, ripping off phone companies, etc. These are basically points in our development where a choice is made as to which path to go down. We consider all sides of an argument, but we generally conclude that it's the one with logic and facts that's correct. We may be tempted to use our interests and skills for illegal activities, but we usually utilize those skills productively and avoid a life of crime. There are those who make other choices, but we believe they distance themselves from the true hacker ethic by continuing down those roads.

A common complaint we hear in many circles is that people aren't allowed to make their own choices or to have a certain opinion. Nothing could be further from the truth. But, as the pandemic has taught us, certain decisions can carry certain consequences. Whether those are consequences doled out by nature or by society, we can't just make them go away.

The hacker spirit is most certainly about pushing the envelope and improving. That doesn't mean there aren't roadblocks and negative elements that must be overcome. But it's that spirit that moves us forward. Otherwise, what's the point?

Dear *2600*:

In 38:4, J accused *2600* of belligerence attacking the "majority" of your readers. J also questioned your trust in science and data using the fact that there were *some* (as in an extremely small percentage) front-line workers who chose to lose their job rather than get vaccinated. J even tried to use this: "It certainly must mean they have quite specific reasons - such as knowledge of likely damages caused by the COVID-19 vaccinations..." as logical support of their rationale that *2600* and most of the world is wrong.

Besides my assumption that J does not speak for

the "majority" of *2600* readers (and definitely not for me), the hacker mentality tends to look at things with an open mind, allowing for us to explore both traditional and especially nontraditional thoughts for any given situation, event, or problem rather than from a shut-off political view. The point J tries to make is not logical, nor has any scientific weight. The number of those who refused to get vaccinated and lost their job is low (and heavily weighted in "red" political areas), and that argument can be the same as saying "I always see nurses and doctors smoking outside hospitals, including cancer research centers. Therefore, smoking must be good for me."

Anyway, keep up the great work, *2600* team! This is one longtime subscriber who is not going anywhere.

Brad

We never thought speaking our minds and following science would be met with such resistance. We used to be amazed at how those who embraced logic and science in the distant past used to be treated. Not anymore.

Dear *2600*:

I enjoyed Gregory Porter's article in 38:4 about scripting downloads of .ts files to save online video. I also do this because my rural DSL line is too low-end to stream video, so I download videos to watch from my local disk.

Here are more tips. There is usually a .m3u file hidden in the HTML source; sometimes it's in a .json file that the HTML links to. Use the browser dev tools to search all requests for .m3u to find it. Download this file and you will see it lists all .ts segments to download.

Here's a bash script that takes a .m3u URL and output file name, downloads the .ts segments in the .m3u, and merges them into the output file. It assumes relative paths in the .m3u file.

```
#!/bin/bash
PLAYLIST_FILE=`mktemp`
TEMP_FILE=`mktemp`
curl -s -L --compressed --retry 3
➥"${1}" -o "${PLAYLIST_FILE}"
BASE_PATH=`echo "$1" | sed 's|\
➥(.*\)/.*|\1|'`/
while IFS= read -r INPUT_LINE
do
 if [ "${INPUT_LINE:0:1}" != "#" ]
 then
curl -s -L --compressed --retry 3
➥"${BASE_PATH}${INPUT_LINE}" -o
"${TEMP_FILE}"
  cat "${TEMP_FILE}" >> "${2}"
  rm "${TEMP_FILE}"
 fi
done < "${PLAYLIST_FILE}"
rm "${PLAYLIST_FILE}"
```

Some more advanced videos separate audio from video so blind viewers can select an audio track with narration over silent moments, or to offer different video resolutions without having to store copies of the same audio with each separate video version. In this case, the .m3u file will list the tracks with additional .m3u files for each track. You'll need to write a script to parse which tracks you want, then go after those second layer .m3u files with the above. Lastly, there may also be a .srt file in the HTML source, which is the subtitles. You can merge all three using: "ffmpeg -y -i subs.srt -i audio.ts -i video.ts -c:s copy -c:a copy -c:v copy output.mkv". If you found a .json file describing the video, you might also find metadata that ffmpeg can add using the -metadata parameter.

David Mooter

Thanks for what undoubtedly will prove to be useful code for many of our readers.

Dear *2600*:

Responding to David M's letter in 38:4: The effectiveness of the easy fix David M suggests is, as he notes, intimately tied to the assumption that there are no inputs that would trick models trained on different data sets. Results from experiments in other (non-cat) problem domains suggest that such inputs do indeed exist, and, furthermore, that the likelihood of finding such inputs increases with the accuracy of the models.

This might seem counterintuitive at first glance, until we remember that the accuracy of a neural network depends on its ability to generalize and detect learned features when they appear in novel data. An accurate model has presumably extracted the most relevant features associated with what we're trying to detect, e.g. "catness," and those features would quite likely look nothing like a cat to the human eye. Our working hypothesis for the explanation of the phenomenon described in the previous paragraph is that two reasonably accurate models have likely extracted and learned many of the same high-quality features during training, and therefore might be tricked by the same inputs where those features appear. In other words, there are a limited number of ways to skin a cat successfully! David M's easy fix works better for models with lesser accuracy and really well for models with close to coin-flip accuracy. Such low-quality models are often useless in practical applications, since they will produce excessive amounts of false positives and negatives.

Finally, I want to stress that these observations are based on early experimental results using image and time-series data, and that more stringent investigation might invalidate them.

Thor M

Dear *2600*:

On the back cover of the latest issue (38:4) is shown Herbert`s, which repairs typewriters and calculators. I think it would be just as interesting to see pictures of places like this as it is to see the payphones for the reason that these are probably soon to be extinct relics. Calculators can be an enormously fun place to start exploring hacks. Case in point: I have built an entire backtesting/trading simulator (for futures, stocks, et cetera) into a TI-89 Titanium calculator (among other cool things),

and if it were to malfunction, I would need such a place (probably). And, in federal prisons inmates are forced to still use typewriters (Swintec) for all their legal paper typings with printwheels costing a whopping $23 and print ribbons going for $7, because G-d forbid they put some kind of Word-like program onto the computers that we, ur uh, *they* use for emailing. Figuring out how to make it print from memory into the same format as a legal motion is quite a challenge. In short, these "primitive" devices are still full of Easter eggs. Perhaps a link somewhere at 2600.com for photos such as these repair shops (not that they can be seen in prisons - wink)? And I agree that we should de everything to preserve this increasingly rare repair knowledge. Cheers!

metaknight

We're glad to see this picture has evoked such appreciation. We know there are many more out there yet to be sent to us.

Spreading the Word

Dear *2600*:

NotTheFed.com is a pentesting company built from several decades of history in the hacker scene.

We were hoping to advertise in *2600 Magazine* and we were wondering if you had any details.

Marcus

Well, here's a mention in the letters section, which isn't nothing. But you can also have a free classified ad in our Marketplace section if you're a subscriber. Email marketplace@2600.com with your text and subscription info.

Dear *2600*:

I run a community hackerspace in Fresno called Root Access. Before the pandemic hit, we hosted our local Defcon group, DC559. Attendance was alright, we'd have maybe five or six people show up each month. (Tech isn't huge in Fresno, but it *is* growing.) Root Access has started hosting meetings again, and we're looking at bringing DC559 back online (or back from online, as it were).

I'm looking for ways to reach out to local sec folks and encourage them to come, and I think that listing in *2600* might be a good option. I know there are some *2600* readers around here because our local Barnes and Noble always seems to run out.

For a meeting to be listed in *2600*, does it have to be strictly *2600*, or do you welcome Defcon groups?

Thanks for all you do; I'm a big fan of y'alls work.

Derek

Hopefully this will help get those meetings going again. We only list our affiliated meetings on the meetings page (www.2600.com/meetings and page 66 of every issue) and those meet on the first Friday of each month. But other groups who meet at other times can get a free listing in our Marketplace section if the person submitting the ad is a subscriber.

Dear *2600*:

Despite the current demonization attempts of all Russian hackers and Russia (including Russian civilians) in general, *shout out* to the subset of Russian hackers who developed the website Library Genesis, a repository of the largest book, comic book, and scientific papers on the interwebz, and therefore by default the number one website in the world and in the history of humanity.

Janet

Sure, that's a good thing. But there are so many others who are risking their freedom and even their lives to fight the horrors being unleashed by their government. We need to figure out how best to support them, contribute to their efforts, and inspire many more to get involved. We agree that blanket demonization is not the way to go.

More on Meetings

Dear *2600*:

I don't see Cincinnati, Ohio listed as having a meeting. There used to be one. Not sure how long ago and if it's still active. Have you had any inquiries for Cincinnati? If not, what do I need to do to start up a meeting?

Donald

The short version is to simply find a decent public space and start getting the word out to people in the area while updating meetings@2600.com with the info. The longer version can be obtained the first time you email that address or in the meetings section of the www.2600.com website.

Dear *2600*:

Hi, My name is Jackson. I am 12 years old. I have an interest in radio spectrum, software, and computer science in general. I am just getting started. My uncle works in cryptography. He suggested I meet with *2600* to meet other great people in this space. When is your next meeting?

Jackson

Our meetings take place on the first Friday of every month, starting at around 5 pm. Check www.2600.com/meetings for the closest one, as well as any variations in the starting time. Our meetings take place in publicly accessible areas with no age restrictions. We hope you find a welcoming environment as well as other people who share your interests. This is the magic of our meetings and of the community.

Dear *2600*:

I've recently moved from Odessa, Texas to Destin, Florida. There were never any meetings in my west Texas area and now that I'm looking, I don't seem to see any in this northwest Florida area either.

I'd love to get some help getting something started in Destin, Florida. What do I need to do?

DISLEX

This is a common problem. But when you consider that people who have started meetings in the past were basically in the same position as you, it becomes much less of a challenge to go ahead and start a meeting in your area. Assuming there aren't already meetings nearby (an hour's travel distance once a month is generally considered nearby) and that you're starting meetings in a place where a good number of people can easily get to them, then

we see no reason why you can't just pick a place and see what happens.

Social Media Woes

Dear *2600*:

I am hoping to wean myself off of Facebook, but would like an alternative. I have played around with a lot of them, but wasn't impressed enough with them to use daily. What alternative to Facebook do you recommend?

D

We know a great one called The Front Door. Just open it and anything's possible. There are others known as Reading, Writing, and Telephone. There's also Sarcasm, which is guaranteed to help you feel better about most anything.

The other answer we can offer is that social media is no substitute for being genuinely social. There is an unhealthy dependency on being liked, popular, or visible. While there are certainly good things that come out of these outlets, there are so many bad things and many of today's major problems can be traced directly to them. False news items, rewriting of history, dangerous health advice, mass hatred, bullying... the list goes on and on. And that's not even taking into account the massive privacy issues involved in broadcasting your entire life to the world.

As with any form of technology, there is good and bad contained within. It all depends on how we use it. And the human race is not using social media very well right now. So for those who want less Facebook in their lives, we suggest identifying all of the negative elements you're trying to get away from and then coming up with how you would prefer such a service to work. But if that proves to be impossible, perhaps we're all better off without these services, or at least not being as dependent on them as we are now.

Dear *2600*:

Please excuse using this email address for complaints, but I am or might be banned by now on the Facebook group for *2600*. A guy posted on there asking for email lists. It sounded dodgy, so I said "yeah i got email list contact in private message" so then I could question and confirm his intentions that it was not going to be used for spamming. He would not have publicly admitted this on the group. I have an email list part of database dumps that are publicly available online. I said to the admin that he can't go round making baseless accusations and suggested for him to find out first. Imagine what would happen if police started arresting people cos they seemed like a criminal. I personally never assume anything. He should have checked with the guy first and based his decision on facts. He then started to accuse me of spamming. As I said, I had an email list - another assumption. All this time, I am trying to explain that you can't go making baseless accusations just cos it seems like it based on no facts. People where I live are spreading lies about me, so I know all too well with dealing with the police on the issue what damage a baseless accusation could cause to him. Sounds dodgy what he asked for, granted, but until you know you shouldn't act. He may have very well had a valid reason why he wanted them and, without asking, you just don't know. He then started to threaten me, including a link to my local police station as if to accuse me of breaking laws - which I do not. He does seem to understand that judging a book by its cover is bad. I am an example of this, due to lies spread about me being a bloody pedo cos i disciplined a drug dealer's child for bullying. All went to court and he was found guilty, not me. But when the accusation has been made publicly, that can still cause issues if someone is innocent. He just cannot go around assuming things just because it looks a certain way. This has caused me three years of hell. He's probably banned me out of spite. I have not been back on Facebook yet to see.

i am white hat - he knows that as he checked my profile and posted links on it to me.

He needs to be told. How would he like it if people started calling him a rapist in the street due to a baseless accusation. He said he doesn't care what people think. Well, he would when he got beaten up for someone else's lies.

Please look into this. I'd be surprised if he didn't ban me out of spite. He needs to learn to get along and not accuse somebody of anything without facts, which is why i wanted to ask his intentions in a private message where he is most likely to get loose lipped and I can check.

Please look into this guy. Don't know why he is admin if he goes round assuming things.

Steve

Whenever anyone asks why we don't spend more time in the social media world, we point to letters like this one. We have no idea what the issue actually is, at least partially due to the pronoun issues which makes this read like a confusing movie (is the admin the same "he" as the person who posted?), but mostly due to an overwhelming and passionate desire to not care one bit about these sorts of interactions.

We don't dislike Facebook or other social media, but we don't have the time, energy, or addictions required to devote a whole lot of time to these issues. Our admins have a tough job dealing with managing things as it is. We expect people to not make their jobs any harder, but if they are truly misbehaving, let us know in a non-rambling way and, if at all possible, without supplying more evidence to make it look like you're in a non-ending war against the rest of the world.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

Prognoses

Findings

Dear *2600*:

Anyone else have an email address that's too popular to use? I managed to get in on the early days of Gmail with a very common email address. I get so many emails for *other people* that I can't even use it. Today I got someone's Kenny Chesney tickets straight from Ticketmaster, no spam/scam.

Carl

This is yet another problem Gmail has. Way too many people assume they have email addresses that they don't actually have and the scenario you describe repeats itself over and over. We've been experimenting with this for quite some time and often get all sorts of personal information, as well as inside corporate and government details that we really shouldn't be seeing. With Gmail, it comes to you without your even asking because everyone somehow assumes they have the address they want. We never noticed this issue with Yahoo, Hotmail, or any of the other email services of the past.

Dear *2600*:

My wife's email address is very similar to someone else's, and she's frequently on email chains involving the same cluster of people (a random community in Alaska). She has tried politely several times to get removed from these chains, but the folks using them are seemingly very un-tech-savvy and misunderstand, re-include her later, and the cycle continues. My wife has taken to just ignoring it and amusing herself by passively reading the communication. So my question is, if it were you, what would you do to mess with them? It's a group of five to ten people who do things like plan lunch outings. The main person who misuses my wife's address is the intended correspondent's wife. She often forwards things like utility bills and "honey do" sort of reminders.

J

As these people seem mostly harmless, we don't advise anything that would really mess with them. This kind of cluelessness is extremely common. To have some fun, we suggest becoming part of the conversation until they realize that they actually don't know who it is they're talking to. Actually showing up to one of their lunch outings would sure be fun, but the trip to Alaska might be a bit much. If you really didn't like them, including them in a different mail chain would probably get them running off the net in a hurry. The possibilities are really quite endless. We'd like to hear more ideas.

Dear *2600*:

Ever since the war in Ukraine started, Russia Today's website rt.com is offline every now and then. They've even installed a DDoS checker.

Peter

It's been rather interesting to see the evolution of this. RT was a channel seen on many cable and satellite systems through Europe and North America. As Russia's unfortunate actions progressed, the channel began to be taken off of these outlets. Then it became only available via YouTube. Then they were kicked off that platform and were only reachable through their own website. Then that site was attacked and taken offline, as well as blocked by various providers. We're currently able to reach it fairly easily, but that can change at any moment. Creative types can almost always find a way around the blocks, as people have been doing inside Russia when trying to reach many Western sites that are blocked there. We believe all of these sites should be accessible to everyone, but there's absolutely no obligation on the part of any cable, satellite, or Internet service to amplify their messages. We believe individuals are usually smart enough to be able to distinguish truth from fiction on their own. In groups, not so much.

Dear *2600*:

I've had Verizon Fios for 14 years now and it has *never* gone down!

Jesse

We're not sure what prompted this proclamation, but we just know you're going to regret saying that.

Dear *2600*:

So yesterday I experienced my first automated fast food order at a McDonald's drive thru. In true form, it totally f'd up my order and I had to repeat myself several times. Eventually a human came on and asked if I needed help. Is this the future? Ordering with Alexa?

Brad

It probably is. But if this dystopian hell has to exist anywhere, it may as well be at McDonald's. And we can always count on people to do what it takes to clog up the works.

Dear *2600*:

So evidently Irish cellphone provider Eir has screwed up its clock, and is resetting cell phones to a very wrong time. I don't know how they can screw something like this up so badly. It takes real talent.

Robert

We prefer to think of it as a test to see if people are paying attention. And maybe a reminder to never believe anything you see on your phone without question.

Dear *2600*:

I have been reading *2600* since the early 1990s

and have been involved in hacktivism my entire life. I don't know if you all have noticed it yet, but there is something "wrong" with the world right now. They are taking over the planet. I don't know if they are aliens, fallen angels, cyborgs, etc., but I know this. In 2019 I stood face to face with some sort of 14-foot-tall, white skin giant that spoke directly into my mind and said, "this is the only time we will see each other face to face." I don't know what the literal fuck it was, but I have a few theories. Since this happened, I started looking heavily into freemasonry, Nazism, and both of their connections to the Ashkenazi Jewish people - who aren't even "Jews" but some steppe people from the Caucasus Mountain region. The Nazis never "lost" World War Two. They just changed strategies. They are trying to enslave all of us right now. The 5G system and the vaccine are *not* what they are telling people. The vax contains nano particles of graphene oxide. GO will vibrate rapidly when 26ghz microwave radiation is applied to it. The 5G system can produce 26ghz radiation. It is a fucking remote control killswitch. There are literally *billions* of people with some fucking nanocyte death system inside of their body right now. I began talking about this on my YouTube channel that had close to 30,000 subs and my account was *banned* within 20 minutes of uploading the video after having had it for ten years. I don't know if you all are infiltrated like Anonymous has been (they are a CIA psy op at this point), but unless you want to be fucking enslaved, I need help. I have a plan to stop this, but I cannot do it on my own.

Jason

There are plenty of letters that we don't print, but occasionally we feel compelled to share one so readers can see the type of content that pours into our offices. There's a lot going on here, none of which we're going to touch, not because we're part of the conspiracy (which, of course, we are), but because there simply isn't enough time in any of our lives. Much of this is being spoon fed to people everywhere and accepted as gospel by those who lack the ability to question things that don't make any sense. The people who are the real problem are those who take advantage of this for their own selfish purposes. That's a conspiracy that's quite real.

Dear *2600*:

Hey real quick, Computerphile has great videos on Unix and the history of Bell Labs.

Zach

Too quick. We were able to figure out that you were referring to a channel on YouTube, but others might not have. There's no need to rush. That said, yes, there are all kinds of cool videos there.

Dear *2600*:

I never thought of myself as a hacker. Maybe if I had acquired hacker credentials from *2600,* I would have. But there have been times....

Like the time I received a list from an organization including names, addresses, zip codes, and another identifier (that I can't go into). Several million records in a PDF file. No other format such as text, CSV, or Excel. I only wanted the cross reference between the zip code and the other identifier that the organization obviously must have. So I contacted them and asked, but was rebuffed, told that their contract with the post office in this country didn't allow the cross-reference information to be released. But I had it already in a giant haystack; I just needed to find the needles. There were millions of records over thousands of pages, based on this cross reference. But how to obtain just the tiny fraction that I needed? Any manual process would obviously take too long.

Luckily I remembered that Adobe Acrobat contains an implementation of JavaScript. With this I was able to go to each page and sequentially ask for each line. This, unfortunately, returned header and footer lines and other junk, but the lines I wanted had a very consistent format, so I could throw away every line that didn't match the data format. For each data line, the script would extract the ZIP and other identifier, look it up in the smaller list I was generating and, if it was a new pair, add it to my list.

So, after several hours of crunching PDF pages, I had exactly what the organization refused to give me.

I wish I could give more details, but I'm sure you don't want me serving time....

D1vr0c

It doesn't really sound like you'd be in any trouble for revealing what this list was all about if you were able to contact an organization that had a contract with the post office concerning this same data. But lists of millions is hardly enough these days to even make it onto the news. Remember, Equifax let data for over 100 million people get out. Yahoo lost private info for over three billion! You know we're in bad shape when leaks can't keep up with what the companies lose on their own.

Recommendations

Dear *2600*:

My daughter is going to her first concert with a friend and she is 15. I will be dropping her off and picking her up. With her consent, is there some sort of tracking device we can install on her iPhone so I can know her location from my Android phone? I realize it sounds creepy, and I may be over protective. But I assure you it would just be for this concert and maybe others.

Max

You really don't need our approval to do this. It's quite common, actually, although the potential for abuse is huge. "Find My iPhone" is just one of

these apps - there are many. But we can't mention such an app without also telling people how to detect them on their phones (which shouldn't be a problem in your case if you did in fact get consent). In most cases, the tracker would need to have physical access to your phone at some point and would also need to know your Apple ID and password. Changing the latter can help to stop tracking from continuing. If you're using a feature known as "family sharing," you can be tracked by other members even without knowledge of your password. Checking what apps are installed and running is usually the best way to find something like this. There are numerous other methods for compromising your phone, such as iCloud or admin access to local routers. We hope to see a detailed article on the various abuses out there.

Dear *2600*:

I'm a big fan of the magazine for a long time, and a subscriber since 2008. Congrats for the fantastic work you have been doing for the hacker community.

Although I've never written any letters, I wanted to share the way I'm storing my physical magazines, as it was suggested by *2600* in one of the past editions (don't recall which one).

I'm using "photograph" sleeves (8"x9") from BCW, and storing them on small boxes (same as those used to store standard comic books). I'm also fastening the back of the sleeves with standard Scotch tape so as to maintain them perfectly closed.

It's a perfect fit for me as the "digest" sleeve format also from BCW is larger than the *2600* mag and the "comic book" sleeves are too small.

Hope this helps hackers/collectors to store the mags throughout the ages!

Keep up the great work.

sl33p

Thanks for that helpful suggestion. We'd love to see pictures of this and other methods people have devised.

Dear *2600*:

I am writing to see if you can help me. I am looking for two things. I am looking for a secure private chat service and a secure private payment service to pay people with. Venmo is just too open for me.

Sean

There are tons of so-called private chat services, but there's always someone who will tell you they're not as private as they claim or that they're run by some evil entity. You need to simply use a service that employs encryption and connects you to the people you want to communicate with. Then take the usual precautions since there isn't a system anywhere that can't be compromised in one form or another. As for private payments, paying by cash remains at the top of the list. Disposable credit cards and gift cards are probably the most anonymous methods of payment, but they require a bit of coordination. Otherwise, there are plenty of semi-anonymous options, each of which has its own unique weaknesses.

Dear *2600*:

We all know that Mastodon and the fediverse exist and should be using that instead of Twitter anyway, right?

Chris

While such decentralized outlets are far preferable and don't run the risks of abuse that the mainstream social media companies do, let's not kid ourselves that there won't also be negativity and abuse on these platforms. As long as we don't believe this will solve everything, any disappointment won't be crippling. (We're also looking for a good comprehensive article on this.)

Memory Lane

Dear *2600*:

I was wondering if anyone might be able to fill in some gaps in my memory. I recall using a chat system of sorts at the University of Alaska Fairbanks in 1989-90. I recall I was able to talk to users at the other two campuses pretty easily (one on one, it wasn't a chat room). I was also able to get out and talk to other people at other universities - several U.S. schools and some of the European ones, some cool guys at the University of Helsinki (I think?). I just remember one of the admins for that system went by the user purplehaze and was a super nice guy. Does anyone know what program(s) they probably were? I want to say the university system at the time was IBM A/S 400 if that helps at all.

Bill

While we can't steer you to any of the specific systems or people, we can confirm that it was indeed once possible and common for users of one university system to be able to chat with users of other systems using programs with names like "talk" or "ytalk." Some of this software can still be found on many Unix-based systems, but we don't believe it's still in use between systems anywhere as the security holes this opens up are just too great. Most of this predated instant messaging, the web, and even SMS.

Dear *2600*:

How many people still get on Usenet? The alt.2600 thread made me think back to what was once a thriving community on the Internet. Agent Newsreader was my go-to choice to get on... that and my WWIV BBS.

Miles

We would love to know how many people still are on Usenet and what they are reading. We have fond memories of alt.2600, but like much else on Usenet, it turned into a real shitshow of spam and abuse.

Dear *2600*:

Hello, I'm clearing out a magnetic media HD here, and found something I wrote that I never

sent you. I think it's pretty amusing! Had forgotten about this. Do what you want.

"How to Steal Things Part 2 (25 or so years later) by J.J. Styles aka 0ptiKal i1usioN aka Zot the Avenger

"Okay, this article is completely despicable, it completely undermines the capitalist system that holds our society together. But, this is a *2600* article and I've been reading this magazine ever since the How to Steal Things article. So here it goes. Go to any store, buy two items, return later, and say that you got double charged and that you didn't realize it. They will refund you for one of the two items. Then return later with the same receipt and return the first item. You will have the second item completely free. Getting double charged is a simple mistake. It could happen to anyone at any store. You know they're scanning the barcode and it beeps but they don't hear it, so then they scan it again and they hear the beep and they're like okay everything's good but it's not, cuz you got double-charged! If this technique works for you, I don't want to hear about it. This right here is a reason to use the self-checkout because I never get double charged when I use the self-checkout because I pay attention and I only scan the barcode once. Don't be a criminal! Fix the system! Goodbye."

JJ

Yes, this is outright theft as you correctly conclude. The original article you refer to was indeed printed back in our Winter 1996-1997 issue and wound up pissing off a lot of people, which was our intent, as too much of the hacker world seemed to be veering into common criminal behavior at that point in time. We're all about the theory and the technical explanations, but stealing has always been stealing.

Dear *2600*:

Back in the 1970s and 1980s, you could call a number - xxx-xxx-0046 - and hear a strangle tone that just went up and maybe down. Was told by a phone tech that it was a special number for testing something or another. Anywho, told our female friends and for years they'd give out that number at clubs. We called it the acid line. Sadly, since analog has left the scene, so has the acid line. Can anyone confirm this?

S

It sounds like you're referring to a sweep tone that used to be operated by the phone company. In New York, they could be found on numbers ending in 9979 and were used to test frequencies on a phone line, but for some reason only in analog switch areas. It was definitely a good number to give out to people you wanted to annoy, as was the always-busy extension of 9970. Believe it or not, some of these test numbers are still in operation, but it's a real challenge to find them. Our recent series on phone switches shared a few of these numbers. We will certainly print more when we find out about them.

Dear *2600*:

A couple of my earliest "hacking" experiences: In middle school (1994 or 1995), we had a "computers" class that was really just a typing class. For some reason, the word processor we used had an option buried in a menu that dropped you to a DOS prompt. I couldn't (or didn't) do much, but I could explore the network drives and see some cool stuff. That got me yelled at by the teacher. Another one: In that same class, our usernames were algorithmic (it's been nearly 30 years so I don't remember the exact formula but think something like "smithj" for "John Smith") and our passwords were our student ID numbers. Pretty secure for a bunch of 14-year-olds who didn't even know their own student IDs before this class. This teacher also posted our grades on the wall. To anonymize them, she posted them by student ID instead of name. So it wasn't hard to match them up to usernames, and soon I had all my friends' usernames and passwords. We used to get into their accounts and mess with their assignments and stuff.

Eddie

In many places, this would be enough to get you labeled as both a computer genius and a massive threat to the entire school. While the technology has changed over the years, the attitudes haven't. And, in many cases, neither has the security.

Dear *2600*:

Many decades ago, I taught "Introduction to Teleproceasing" at a college in New York City. The first time I created an exam, it was an accident.

The first day of class, I told the kids that I would call my final exam "20 Questions" as my personal rebellion to the Education System. After I printed out the two page exam, I noticed a mistake. At the bottom of Page 1 was Question 19, and at the top of Page 2 was another Question 19.

I then recalled a friend lecturing me on Exam Panic Syndrome, and made a decision. I explained about the two Question 19s as I placed the exams face down before each student at every desk, and said that as a consequence of my mistake (and having promised them 20 questions and not 21), they would be granted one free wrong answer. The collective sigh of relief in the room was palpable. I kept the two Question 19s in the exam in subsequent semesters. Only those who got all 21 questions correct got an A+ on the exam.

Cheshire Catalyst

What we really want to know is what kind of material was taught in "teleprocessing" back then.

Offerings

Dear *2600*:

We would like to place the article on your site.

Do you allow the guest posts with do-follow links on your website? If yes, can you tell the price for that? Thanks a lot!

Daniel

This shit again. What if we just say it costs a million dollars? Would that make it stop? Or would it make us rich?

Dear *2600*:

Hi there. At this point, you may be thinking "Wow, this person has been bothering me for weeks, what a tremendous heart! Is this person going to summit Mt. Kilimanjaro next?"

All jokes aside, the reason for my persistence is I believe our Shopify agency can help you deliver a seamlessly interactive, innovative, and scalable e-commerce solution so you can attract more customers, untap bigger ROI, and grow your business into the future.

Are you the right person to be having this conversation with? I'd appreciate any reference.

Lisa Hudson
Business Development, PureLogics

No, Lisa, we are not the right person. We are the letters department and what we were thinking had nothing to do with Mt. Kilimanjaro, but now that we've thought about it, we would like to suggest that you relocate there and be sure not to bring a computer or communications device.

Spam has gotten so conversational in recent years. Soon we will be having spirited debates and fights with AIs and, once they interface with robots, actual battles will commence. We are already planning ways of sabotaging this dark and dangerous future.

Dear *2600*:

I am the Project Manager working with Middle Island Country Club in Middle Island, NY. We are creating the brand new scorecards to be used by the golfers that will be highlighting a few local businesses around the scoring grid. The course has invited your business to be featured for 12 months in front of all golfers as the industry exclusive.

Jude

This goes on for quite a bit about what a great opportunity this is. It makes us ponder what kind of message we might have for local golfers and how simply having a post office box in a particular community is enough to get pulled into this world. Had they done even the tiniest bit of research, they would have quickly realized that giving us a mouthpiece to their clientele would end badly in every possible scenario. It almost makes us want to try.

Dear *2600*:

Hello concentrationcamps.us

Hope you are doing well.

I was examining your website and saw you have a good design and it looks great. But it was not ranking on any search engines for most of the keywords.

[...]

Note: We are not spammers and are against spamming of any kind. If forwarding this email has made an offense to you or to your company, then we apologize for the same. In order to stop receiving such emails from us, simple type "NO" in the subject line.

Warm Regards,
Maveric Miller
Digital Marketing Executive

NO.

You wrote to concentrationcamps.us with this unsolicited cheery message and a pitch to do some kind of search engine business. How could we possibly be offended? You are the very definition of what spam is, from the cluelessness of your initial contact to telling us that the only way to stop hearing from you is to respond to you. Does this approach ever actually work?

Dear *2600*:

Hey there *2600* - people sure do want some new swag. I couldn't sleep last night, so here's my contribution for a possible new design. Are there potential copyright issues? Possibly. But it's your design now. Do with it what you will. Love ya.

Moose

Well, we sure don't want any trouble with the Quaker Oats people. But this was too good a design not to share. Thanks for thinking of us.

Thoughts on Meetings

Dear *2600*:

I live in Miami and have always wondered why there was never a meeting here in the biggest (and most well known) city of Florida. And it's not just because of COVID-19; there hasn't been as long as I can remember (which means decades).

I find it impossible to believe I'm the only person in Miami with the *2600* "hacker" mindset. In fact, I know several people/friends that would be joining if one was created (assuming I had your blessing, of course).

What is required to start a *2600* meeting (if you don't mind my asking)? I'd like it to be an official *2600* meeting and have it published in your future editions (only to draw in the most amount of people). And yes, I fully agree with everyone having to be vaccinated and will do everything in my power to state that requirement. What are the requirements as for where it's held?

Also, is there a certain part of the city where it would have to be held? I only ask because Miami is quite a large (and spread out) city with a lot of traffic and essentially no real (practical at least)

public transportation. Especially Friday at 5 pm (which is peak rush hour) - that could easily take three or four hours to go from one end of the city to another. Again, assuming it's OK with you guys, I'd much prefer making it slightly later in the day (only because of what I said above). I'd say 8 pm would be the best time if being totally honest, but even 7 pm or 7:30 pm would make it much better than 5 pm (in my humble opinion).

Not that I'd think I was some kind of "leader" of that meeting by the way. I have zero such ambitions, I promise. I just want to link like-minded people together (for everyone's sake, including my own as well).

Anyways, thank you for your time. I appreciate it as always. And I'm almost done with my next article submission for you guys, by the way (actually I have several I'm working on).

Thanks again! Much love!

Doorman

We appreciate the support and we look forward to seeing more articles. To address your questions, it does indeed sound like starting at a later time might be best for your particular location. But you also want to make sure it remains open for those who can't stay out too late. It's a great question as to why there hasn't been a meeting in Miami in recent years, but usually the reason winds up being simply that nobody took it on. All it takes is one person to start the process. We prefer that meetings be held in easily accessible public spaces. That's something a native of the area is best off deciding. And, yes, you have it exactly right that setting up a meeting doesn't make you the "leader" of those who attend. We take great pride in nobody being in charge of our meetings. We wish you luck and hope to see something come out of your city soon.

Dear *2600*:

I was looking for *2600* meetings in Wisconsin and didn't see any on the list. Are there any groups (active or otherwise) in Wisconsin?

Nathaniel S

We're certain there are lots of people in Wisconsin who would be interested in meetings. The challenge is in reaching them and in getting one person to come up with a public place in which to start them. It's actually not that much of a challenge, but you'd be amazed at how we often convince ourselves that somebody else will step up. Every meeting we've ever had has started with the initiative of a single person which led to the flourishing of an entire group. There were meetings in Wisconsin before the pandemic, so we see no reason why there can't be meetings now.

Dear *2600*:

Hope all is well. I was curious what the startup plan is for the Toronto meeting?

Jeff

All it will take is someone from that meeting sending us an email (meetings@2600.com) or a DM on Twitter (@2600Meetings), letting us know where and when the meetings are. We will then help them spread the word. It really doesn't take much. We just suggest people choose a meeting location carefully so that it's easy to get to and in a public place.

Dear *2600*:

When is the next U.K. meeting?

Samir

Same as everywhere - the first Friday of the month. Check www.2600.com/meetings for specific locations or contact us to start a new one.

Dear *2600*:

Hi! I've read *2600* since I was a preteen. Now I'm in my 30s and, well, a "cloud engineer." I stay between Bali, Indonesia and Seattle, Washington, USA. I would love to host meetings for either or. I think there is an active Seattle *2600*, but I've never seen one for Bali. Could I get a listing in for May and future months?

Steven

Yes, but you have to tell us where you want those meetings to take place! Please send us the details. We also presume you'll be in Bali enough times to help the meetings take off.

Dear *2600*:

Was Petrozavodsk removed from the list because of the events in Ukraine?

***2600* Petrozavodsk**

Technically, yes, and we must apologize for that. We were contacted by a representative from another Russian meeting who requested that both meetings be delisted because of those events. We assumed they were speaking on your behalf, but clearly that wasn't the case. We've since restored your meetings to our listings. And we hope to see the other gatherings resume.

Dear *2600*:

Could you please give me the email address of the coordinators of LA2600? Thanks.

Queuemark

We don't give out personal info for anyone. What we can suggest is that you send a Direct Message on Twitter to @la2600 or visit www.2600.la, although it doesn't look like either of these outlets has been recently updated. Hopefully, we'll get an update in the near future. Failing that, anyone is free to restart them at a convenient location.

Random Bits

Dear *2600*:

If your computer is going slow, it might need more memory: DownloadMoreRam.com.

Alex

Who knew you could download RAM? We're sold.

Dear *2600*:

To find exposed FTP servers, use the following Google Dork: *intitle: "index of" inurl:ftp.*

Jim

There is an incredible amount of exposed content out there that's really easy to find and

that we often forget about. Thanks for this handy tip. (Although we should warn people that despite this being a simple command to access publicly available content, there are clueless people out there with a lot of power who will say you're committing a crime by doing this. You are not.)

Dear *2600*:

Seems very strange that the far left are losing their minds because an African American bought a social media platform in order to promote an open and inclusive dialogue. What gives?

Lee

You think you're pretty clever, don't you?

Hello *2600*:

Please do not change the greeting line of this letter to read, "Dear *2600*". Thank you.

N1xis10t

That's the power of "please."

Security Issues

Dear *2600*:

So I brought up a problem with security in a group for Rove R2-4K dash cams. Why do they not allow you to change the default password? The password is 12345678. The responses I got from idiots in the group is amazing.

D

We don't doubt it (but please always share idiotic responses). Perhaps now that it's getting more attention, this "feature" might be added?

Dear *2600*:

Right now in America, a certain group of people are losing their mind over the idea that an app that tracks their period could be used against them if certain laws in states they do *not* live in are passed. And that "they" will know what is happening in their bodies. So what is stopping "them" from tracking you as you sit on the chair at a gynecologist, or any other doctor's office or service provider for two hours? Think of all the RFID tags ESN, IMEI, SIM, MSN (SN), and PIN identifiers that will connect to the apps on your cell phone that will tell "them" everyone around you, and which doctors and nurses are helping you. Not to mention the Wi-Fi networks your phone automatically handshakes and connects to, every minute of every day. If "they" really want to track you, "they" already are. One app is not the only thing holding "them" back or allowing "them" to do it. Ask Google to show where you have been in the last month. And if you really want to get scared, send Apple a legal demand letter for their location data of your Apple device for the last 120 days. What you get will be less surprising than how fast you get the data back.

Tim

You raise many good points, but you do so in an incredibly imbecilic manner. Do you think this is some sort of paranoid delusion? This shit is happening right now. The Supreme Court has taken away women's rights and there are backwards states in our country that have every intention of tracking pregnant women to make sure they don't try and get abortions, even by traveling to other states. There is currently a very real push to make this a nationwide restriction, which could become reality if people don't turn out en masse to the polls. It's a hell you'll likely never be able to imagine, but let us assure you that this is very, very real. Now the question becomes: how do we fight back and defeat this blatant intrusion into our privacy? We hope you become more supportive of this very real fight looming ahead as you seem to already be aware of the privacy implications.

Dear *2600*:

With the latest iOS, it's possible to locate your iPhone even if it's powered off. That's because even when the iPhone is turned off, certain wireless chips remain on, allowing the phone to still send signals that can help locate it. Now a group of researchers from the Technical University of Darmstadt in Germany has found that one of those chips, the one that enables Bluetooth, can be exploited and hacked to install malware on the phone even when it's turned off.

Ed

It's always nice to have something new to lose sleep over.

Questions

Dear *2600*:

Is *2600* a server attached to your magazine?

Brian

No, that's the name of the magazine that's attached to our server.

Dear *2600*:

Is there a proper hacker name registry? Just wanna make sure there are no well known hackers using MaxResDefault.

Dave

A hacker name registry... now there's an idea. Because we all just love to register our identities.

Dear *2600*:

Have you ever considered doing a "behind the scenes" article or video documentary about how the magazine is made? Or does one already exist? It would be really interesting, and potentially inspiring to anyone trying to start their own publication.

aestetix

It could also have the exact opposite effect. Plus, most of the action takes place on screens these days so it wouldn't exactly be a riveting documentary. Perhaps tuning up the 2600 *van might make for more compelling viewing.*

Dear *2600*:

I am sorry to ask. I have your digital subscription and I was searching for an email address to send the picture of a payphone I found here in Ohio but I just cannot find it and a web search is of no help. Is it payphones@2600.com?

Roland

You guessed right! We will work on improving

our visibility. It's harder than it seems.

Dear *2600*:

What is *2600*'s opinion of copyleft sites like free2600pdfs.com?

John Hardy

What do we think of a site that takes our work and gives it away for free? Not much. If you support the magazine, then support it by helping it to stay alive. Ripping us off doesn't accomplish that. Is this really something we need to explain?

Dear *2600*:

Can you do a job with me?

J Wu

When will we develop the courage to just dive into one of these schemes?

Dear *2600*:

My friend had her car stolen. Toyota will not give her the GPS information and will only give it to law enforcement who are on holiday. Is there a way she can track down the GPS information on her car?

Josh

Law enforcement is on holiday? Look, we like to answer questions, but we don't like getting bullshitted. Clearly, there is something else going on here. Had you been up front about it, you might have been reading an answer in these lines instead of an admonition to try harder next time.

OK, we can't resist answering the question anyway. The system is called Toyota Safety Connect and it costs $80 a year. The "vehicle finder" feature will tell you exactly where your car is. If your car is stolen, then the cops get involved and use this technology to track it down as soon as the police report is filed, regardless of whether or not you subscribe to this service.

Dear *2600*:

I thought *2600* was not political - what is up with USA.WTF?

T G

Perhaps you should be running USA.WTF. WTF. But seriously, have you ever known us to not express an opinion on an almost constant basis? And if so, when exactly was that?

Dear *2600*:

I keep getting IG messages from hacked accounts, asking me to help them by "sending a code." How do I fuck with them?

Philip

Don't send them a code? Or... send them the wrong code. Or, finally, ask them for a code instead. This almost writes itself.

Dear *2600*:

how's the day going?

Hugoland

Is it wrong for us to assume this is some sort of scam? Maybe somebody genuinely wanted to know. Why can't we be more trusting?

Outrage

Dear *2600*:

Adobe is seizing control of my computer Again and Again and Again to insist that I delete my Adobe Flash Player! Isn't this harassment!? Where can I go to report this unethical and possibly illegal behavior!?! It is *mine*, not Adobe's. I bought and paid for the damned thing. I *don't want* to delete it - though that is more sentimentality than anything else. But I am damned tired of Adobe's "won't take 'no' for an answer" attitude. One of my pet peeves in life is people who will not take "no" for an answer. Whenever *anyone* obliges me to repeat "no" a second time, it is extraordinarily rude and orkish. *Another* pet peeve of mine is folks who will let people obtain their nefarious purposes by means of not taking "no" for an answer. And when you try to persuade someone who has already plainly told you "no," you have lowered yourself to the moral level of a pimp.

Robert

Clearly, Adobe knows how to push your buttons. And, we agree those reminders to uninstall their now-unsupported software can be super annoying and intrusive. Despite the fact that it's a security hazard that will only become less functional with time, it's still your right and your decision as to when or whether to disable it. We understand there's an option within Flash called EOLUninstallDisable which will disable these alerts. Good luck.

Dear *2600*:

I really don't understand why search engine companies insist on feeding me results that aren't even close to my search criteria. For example, I want to know how much aluminum cladding was used on the original World Trade Center buildings, especially the Towers. I would think this would be a simple request, an ideal question for the modern computer age to answer. *No!* You cannot find this answer within three pages of results by using any of the big name search engines! In fact, my random selections of the results did not contain any of the search terms that I said must be included in the results! Back 20 years ago, I would have gotten what I asked for. Today, AI and whatever algorithm hack exists has ruined search engines. Here's my search criteria: World Trade Center "aluminum cladding."

Richard

We have the answer but we're sworn to secrecy.

Dear *2600*:

Canceled subscription. Your Facebook page went political and the administrator was disrespectful. Twenty-five plus years of support gone.

Bobby

You do realize (which you can't since you canceled) that our Facebook page or group or whatever has nothing to do with what appears in the magazine? The various forums run in our name are done as public services for members of the community by other members of the community. They are all different. If they start

doing really evil things, we will disassociate, but disagreeing politically or someone being rude are things that simply don't rise to that level. We hope you don't judge everything like this or you'll be cutting yourself off from an awful lot of people.

Dear *2600*:

What does it say about a security company who sends unsolicited marketing emails with no way to opt out? There's no subscription information in the body of the message or email headers. I had to contact them directly through chat to get them to unsubscribe me, and only after providing all my personal details and a confirmation code in my email to verify my identity. I then had to authorize them to unsubscribe me. This is completely unacceptable behavior for any security company, let alone one who says they're "protecting my privacy." I signed up for their service as part of a research effort, but their service is almost as invasive as the spam it is meant to block. How does anyone tolerate a constant onslaught of marketing and sales emails from this company? The application itself continually uses FUD (fear, uncertainty and doubt) to raise concern to strong-arm consumers into a hard sell of their other products. This isn't new for Norton - they have a reputation for the hard sell, even for products the consumer already has - constant pop-ups, email alerts, and alerts forcing people to renew.

Dave

For a moment, we were afraid you weren't going to mention the name of the company. But since you did, we can say that we've heard these complaints many times, not only about Norton, but a number of other anti-virus companies. It seems when fear is your main motivation in getting sales, it turns you into a bit of a jerk.

Dear *2600*:

I protest against moderators declining my posts as soon as "big brother" or "ministry of truth" is mentioned, while in the description of this group it is clearly mentioned that this group is also a place to speak out against increased digital surveillance and the limiting of free speech. That's what it says or doesn't it? If the moderators think that hacking is only about Cap'n Crunch whistles and script-kiddies, then they are wrong and acting against their own group policy. If moderators don't understand that politics (I hate it) can be left out of it, then they are wrong also. Yes, it shouldn't become a politics group, but censoring a member who posts a little about what currently is going on with the "ministries of truth" that they are trying to install everywhere is not OK.

Ronald

We really have no say in the particulars of any of our Facebook groups, but that's the precise reason why we have more than one. Moderators do an important job, but they're also human and will occasionally do things that you don't agree with. For most, the benefits seem to far outweigh the occasional conflicts.

Dear *2600*:

Attached is a copy of your classified advertisement from [redacted], a convicted child molester. He voluntarily entered into a nolo contendere plea and was convicted.

I do not appreciate a convicted child molester classified ad in *2600*.

I hope this magazine does not condone and support an imprisoned child molester. Please do not renew his ad. In my opinion, the ad is surveying for another victim.

From a paid in full subscriber

We understand your concerns and they are valid ones. But we are not going to do a background check on everyone who places an ad and we're not going to be the morality police and decide who is worthy and who isn't. What we will do is continue to advise people to be careful when contacting anyone they don't know. What we will also do is not run ads that appear to be encouraging illegal activity or looking for people to take advantage of. The ad in question didn't meet either of those conditions.

With people who are in prison, it's really simple to look them up and see what they're in for. They can't use handles. The knowledge that you get from finding out this information will then guide you into making a decision as to whether or not you want to contact them. And, despite what people may think, everyone still has the right to talk to other people, regardless of the crime they may have committed.

Keep in mind that the people who aren't incarcerated could be even more dangerous and able to hide their identities. That's why we always encourage vigilance. If we gave the impression that we were making things safer by weeding out certain people, that would only create a false sense of security. And, of course, it would also serve to dehumanize those individuals, something which we are not at all comfortable doing.

Dear *2600*:

See this man. [redacted], very politically connected, extremely wealthy. What if I told you this company was trying to buy my silence?

I'm not nearly as skilled like you guys. But I do know 1000 percent these fucks don't want it to be known child exploitation happened on their network, their servers, their dime, by their employees... or should I say taxpayer dime also (historic vehicle association)?

Anonymous

We're willing to investigate and reveal any such conspiracies, cover-ups, and/or misdeeds. But we need actual evidence in order to do this. We see a near-constant barrage of accusations but very little to back them up. Give us the data and we'll look into it. (We don't have time for long

conversations about any of this before getting to the point of actually having something of interest. We would still be stuck in 1986 if we returned all calls and answered all messages concerning these alleged injustices.)

Feedback

Dear *2600*:

Your cover page supporting Ukraine just brought me to tears and took my breath away. Thank you *2600* team for everything you do!

Mike
Lifetime Member

We're glad it resonated. It was the least we could do.

Dear *2600*:

This letter is in response to duykham's article in 39:1, "How to Use Gmail to Send Emails From an SMTP Server That You Do Not Own." The article is correct. However, while the spoofed message could get sent and might get delivered, the chance of it making its way into someone's inbox is slim. There are three big anti-spam standards that should stop a spoofed message in its tracks:

SPF (Sender Policy Framework) is a DNS TXT record listing sender IP addresses, so if a domain doesn't list Google there, it would fail SPF.

DKIM (DomainKeys Identified Mail) puts a cryptographic hash on an outgoing email, like putting a stamp on a letter. Google would put their "stamp" on the message, and while it'd be a proper DKIM signature, it'd be for gmail.com rather than spoofeddomain.com, so a DKIM check would still fail. (Those guys at the IETF thought of everything!)

Finally, DMARC (Domain-based Message Authentication, Reporting and Conformance) would see that the From and Return-Path addresses on the email don't match, see that SPF and DKIM failed, and do whatever the spoofed domain's postmaster wants: deliver normally, deliver to quarantine, or flat-out reject it.

Assuming the message got this far, its last task is to get past spam filters such as SpamAssassin or Exchange Online Protection, who might give it more scrutiny.

The astute hackers out there might see one flaw in this plan: what if the other domain uses Google for email? On paper, that would pass SPF/DKIM/DMARC despite being a spoof. Did duykham discover a way to spoof Google Workspace users' emails? It's possible, but I'd bet some Google engineer put up a thin paper wall to prevent Gmail users from impersonating Google Workspace customers - you know, as opposed to fixing the actual problem.

PSA: SPF, DKIM, and DMARC are free and open standards that can stop phishers and spoofers in their tracks. Like flossing, setting these up is something you should do without being told, whether you outsource your email or you self-host (like Byeman espoused in another of 39:1's great articles). A how-to article would be out of scope for a hacker magazine, but there are plenty of resources online. This audience can figure it out.

Colin Cogle
Exchange Server Administrator

We have no doubt they can. Thanks for your feedback.

Dear *2600*:

Thank you for publishing my article and thank you for publishing Kevin Coombes' letter about it!

Discussion can only make the world a better place. Maybe one day the Internets will be secure! (Only *2600* readers can make it so!)

I say to all *2600* readers: Keep your thoughts not to yourself but to everyone! Write to *2600*! Letters are as good as articles. Write as if your life depends on it, because it does.

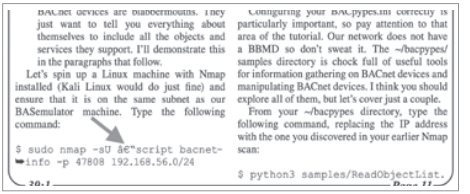
G.A.Jennings

That might be going a bit far. But we do value and encourage every last letter and article. Payphone pictures and back cover photos, too! The more the merrier.

Dear *2600*:

There was a typo in the Spring 2022 issue as shown.

Roman


BACnet devices are bladdermouths. They just want to tell you everything about themselves to include all the objects and services they support. I'll demonstrate this in the paragraphs that follow.

Let's spin up a Linux machine with Nmap installed (Kali Linux would do just fine) and ensure that it is on the same subnet as our BASemulator machine. Type the following command:

```
$ sudo nmap -sU â€"script bacnet-
➥info -p 47808 192.168.56.0/24
```

Configuring your BACpypes.ini correctly is particularly important, so pay attention to that area of the tutorial. Our network does not have a BBMD so don't sweat it. The ~/bacpypes/samples directory is chock full of useful tools for information gathering on BACnet devices and manipulating BACnet devices. I think you should explore all of them, but let's cover just a couple.

From your ~/bacpypes directory, type the following command, replacing the IP address with the one you discovered in your earlier Nmap scan:

```
$ python3 samples/ReadObjectList.
```

We are ashamed and embarrassed. What happened was a bad translation of a file format that resulted in extraneous characters slipping by. We're very sorry and have come up with a better way of avoiding this.

Incidentally, the line should read:

```
$ sudo nmap -sU -script bacnet-
➥info -p 47808 192.168.56.0/24
```

Dear *2600*:

In the letters section of 39:1, you asked for suggestions of other hacker/phreaker movies from the 70s, 80s, 90s, and more. I have one that might be forgotten or overlooked. Not a hacker in the computer sense, but Gene Hackman really showed off his skill set in the 1974 movie *The Conversation*. The pacing is slow and deliberate. The ending is perfect. I think it's one of the best in this genre!

mheyes

We're inclined to agree. That was one of the most authentic films on the subject ever made. It is indeed slow, but that's what made it work. It's also aged quite well.

Dear *2600*:

The letters section in 38:4 contained a pleasant surprise for me with a reader's generally favorable

comments on two articles I'd written about my Bitcoin experiences (35:1, 36:2). I really appreciate Ron's interest in a follow-up story and, in fact, I had been thinking the same thing!

A lot has been going on in the world of money, markets, and crypto. Bitcoin has been banned in several countries, enshrined in another, seen various scandals, has not reached the high prices that some predicted, yet it has not disappeared either. Inflation has returned at levels not seen in many decades.

I still think the evidence shows that Bitcoin is a decentralized hybrid of a pyramid scheme and a Ponzi scam. It is a con job wrapped in the appearance and language of investments. I believe it is not viable in the long term for many reasons, such as the extreme energy consumption of each transaction, which has real-world costs which must be paid. (Cash has no such fees, and credit card fees are low enough to usually be absorbed as a cost of doing business.) Bitcoin's system tends to give equal protection to good and bad actors, and provides little recourse for victims. (Credit cards skew towards protecting the good at the expense of the bad.) And some people see evidence of large crypto holders - "whales" - regularly influencing markets to their financial advantage. Certainly these kinds of problems also afflict other financial systems. There will always be those who seek ways to "get rich quick," others who will gamble at casinos believing they can beat the house, and some who will try to steal value rather than create it.

I have come to view cryptos as a legal (at present in the USA) scam in which nearly anyone can participate. When I saw prices continuing to go up, I bought into several different cryptos, sold some for profit, and continue to hold some in hope that "greater fools" will someday buy them for more than I paid. But I have not risked more than I can comfortably afford to lose.

All of this has led me to think a lot about the nature of money, wealth, and how they can serve as tools for those of us interested in using our abilities to create change for ourselves, and the world.

I'm writing more now, and plan to submit an article soon.

XtendedWhere

We look forward to this conversation continuing into all sorts of unexpected areas.

Gratitude

Dear *2600*:

I am already a lifetime print subscriber, so please do not initiate a second subscription for me! The purpose of this payment is simply to say "thank you" for the pleasure and enlightenment I receive from my current *2600* lifetime subscription. No doubt your costs of production and distribution are increasing, so please accept this contribution in the spirit in which it is offered.

Mark

We do appreciate your generosity, but always prefer to give something back when people make such donations. People tell us "just existing" is enough, but we think there should be something more. Thanks for the acknowledgment.

Dear *2600*:

For a while there, I was worried the final issue of my subscription (Winter 21-22) was lost forever, but it finally arrived mid-March at my state correctional facility! Whew! Close call.

After a brief consideration, I decided it is finally time to pull the trigger on a *2600* lifetime subscription. I've been an avid, dedicated reader for over 20 years now, but was always too frugal to splurge for anything beyond a one-year subscription.

Both my parents passed away in the past 15 months and my father specifically got me interested in hacking and computers at an early age. I remember being around 13 years old and him bringing me a boxed copy of Redhat Linux 5.2 to play around with. My father was a big fan of esoteric operating systems like OS/2 Warp, BeOS, QNX, and others. He spent most of his career working in IT and networking jobs. I miss him and my mother every day.

Their passing, however, has enabled me to be able to finally afford a *2600* lifetime subscription, and I know my father would find it a solid investment. I'm down to less than 20 months left on my sentence and look forward to getting back out in the world and learning about the latest exploits, technologies, etc.

It also seems like your magazine has really focused on hacking instead of politics over the past few issues and that too is refreshing to see. As a loyal and faithful reader, all I ask is that you continue to put out a quality product that questions the mainstream ideas in the world. People need to explore more, argue less, and not take their time in this world for granted.

I'll be having a third party subscribe for me on the street so future address changes aren't an issue. Thank you for this magazine - hack the planet and the universe!

Vincent

It was definitely a smart move to have that sent to a different address so your future issues won't wind up going to the wrong place. For people in a similar situation, we really appreciate the support, but please be sure you've taken care of yourself first. Most people reentering society will have their hands full finding places to live, employment, etc. Once all of those items are taken care of, subscribing to your favorite magazines can move higher up in the priority list. Thanks for your support!

Dear *2600*:

Readers:

Nice work on #OpRussia.

Respectfully
Anonomisiss

We're certain at least some of our readers were involved.

Dear *2600*:

Thank you for all the time and effort that goes into putting together and disseminating your publication.

I've just recently discovered *2600 Magazine*. I've read through the most recent issue and I thought it was really great. I learned about *2600* from reading Snowden's biography - a heroic and unfortunate story, I think.

I am a first-year graduate student at Illinois Institute of Technology studying software development. I never much studied anything related to computers or technology before this. In fact, sometime in my 20s, I convinced myself that I was "too dumb" to learn about computers or programming. A few years ago, I decided to give it a shot and see if I did have the mental capacity to learn. I started with studying for the CompTIA ITF+ cert and moved on to studying for the A+ exam. I did some cursory Python learning on the DataCamp website and read books, watched videos, etc. I took an Intro Java class at my school and then decided that these subjects can become complex and difficult quite quickly, but with time, effort, and sacrifice I was able to learn and understand the various concepts and how they come together. Now I've just completed my first semester of grad school. It was tough and I still have a lot of material to revisit from my Intermediate Java class, but I made it through and know more than I did before I started.

I am writing not to brag about these achievements, but to hopefully get some advice on how to proceed with growing into a competent and valuable developer, and also how I can get the most out of the upcoming HOPE conference. My particular interests are in learning about developing embedded systems/software and maybe even more specifically for hardware like cameras and sensors, etc. (machine vison types of things).

This will be my first participation in any conference/gathering/happening having anything to do with technology and I want to learn as much as I can, while not seeming uncool or unaware enough about this or that technology, social code, etc.

Any advice for a student that wants to show up, hang out, and be enlightened by the wisdom of those that come with lifetimes of experience?

All the best,
The PizzaOverlord

The best advice we can give you is to continue doing what you're doing. Setting challenges and meeting them is always the way to get on a good path forward. It's impossible to tell you which path is the best one to go down as the variables are always changing and everyone is different. The important thing is to be happy with your achievements on their own. You seem quite open to learning and, being in grad school, you should be able to surround yourself with a good deal of learning content, as well as people to share ideas and learn with. You tend to get more out of school by exploring subjects you weren't even aware of before. Too many people go into academic settings with very specific ideas of where they want to land in life. That's a wasted opportunity, as school is where you can discover whole new fields of interest that you never dreamed of pursuing. It doesn't always work out, but realizing that is a part of the process. Even failure is a learning experience and we know plenty of people who did badly in school, but learned much more than those who got straight As.

As for HOPE, it will have already happened by the time you read this. It's a similar scenario, all the more so this time, being set on a college campus. For people attending any conference that has a wide variety of subject matter, we suggest a similar agenda of exploration and learning about things you didn't know about before. And, as with any social setting, you will find many others doing the same thing. Just never assume that you or anyone else is "too dumb" to get something out of the vast array of knowledge that surrounds us every day. Good luck with the journey.

Dear *2600*:

Thank you all for being an outlet. The whole absence of solitude is fantastic. Seeing so much content from staff and subscribers and readers really enriches a niche that probably had other titles over the years. Labors of love are the most rewarding. Sure, you can solely commit to income and hoarding experiences as a revenue stream, but the transfer and enrichment of sharing is what I would dare say is a tenet of humanity over the ages. Maybe someday instead of thinking others know better than some, we can be more humane to more people?

Pic0o

We'll get there. It may be a bumpy ride.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

Articulations

Playing With Systems

Dear *2600*:

I had to make an installation appointment to have some blinds put up in my house, so I called up the company. There was a 15 minute wait, so I chose to leave a message and have them return my call. Their virtual assistant called me back. I answered and, after the first few syllables, I could tell immediately that it wasn't a human. Way too bubbly for a human that answers the phone dealing with customers all day. So I got through scheduling the appointment and when the call came to an end, it asked me if there was anything else "she" could help me with. So I asked if she was human. It said no, she was not, and asked if that mattered to me. I said no and it said "Well I'm glad I could help you!" in such a bubbly voice that I found myself smiling. Now I want to talk to her again.

RS

We're surprised she said no. But when you get to that point with a virtual assistant, we believe that's a green light to mess with them as much as possible. We're open to suggestion on the best ways to do this, but we imagine there are some secret commands that could result in all sorts of fun or perhaps some questions that yield surprising answers. In your case, we suggest ordering more blinds at the company's busiest time so you can avoid humans and have another conversation with her. Let us know how it goes.

Dear *2600*:

My wife received an email from PayPal saying she needed to call before $600 was taken from her account. She doesn't use PayPal at all, and checked all of the links to be sure they were legit. She did make the mistake of calling the number on the email, and the person was remote and was trying to force her to basically go through the two factor authentication process on her phone. He said that the URL version would not work. She immediately hung up and logged directly into PayPal to see that nothing was being charged (duh). So this is where it gets strange. I had her get the source of the email and send it over. The *only* thing that was off was the subject line "Billing Department of PayPal updated your invoice." Every link, image, etc. all went back to paypal.com. The *only* thing off was the phone number. Googling the 888 number returned no results. That number was *not* listed on their website anywhere. Went through the headers and *everything* checks out. They all came from an IP that is at paypal.com. Icing on the cake: my wife called the real customer service number (from the website). The customer service representative confirmed no charges *and* said they were "aware of many of those types of emails going out." Obviously suspecting breach and using the internal mail relays somehow, but thought I had to have missed something.

JS

We doubt the rep was inferring that these emails were coming from PayPal, but rather that lots of these scam emails were going out from somewhere and that they were aware of them. The 888 number was obviously the scammers' method of getting information from people. It's likely they were able to capture your phone number even if Caller ID was blocked, as toll-free numbers use ANI (Automatic Number Identification), which is much harder to suppress on the caller's end. But it sounds like the two of you are well prepared for any scams that come your way.

As for the lack of smoking guns in the headers, we suspect there are more headers you didn't see. Make sure you expand them on the system you're using so you can read all of them. Often, we find a weird IP or a strange domain name after looking several times because it can be easy to hide these in plain sight. If scammers have figured out a way around this, it would be really big news.

Dear *2600*:

Growing up in Queens, New York, we didn't consider ourselves poor. But we certainly had rules to follow when it came to buying things and spending money. One of my dad's pet peeves was putting dimes and then quarters into a payphone. It just wasn't tolerated. So to combat Big Bell, my parents taught us to call collect and ask for Joe Smith. The operator would simply make the call, ask for Joe Smith, explaining that there was a collect call for him. The receiver - me, my dad, whoever was home - would always just answer, "Sorry, Joe is out, can I take a number to return this call?" Of course, the NYNEX operator would give out the phone number from the payphone as a courtesy . A half a minute later and a call back. Anyway, I'm sure others have done this. I guess, after all, it was a hack.

LG

And a hack that virtually nobody had a problem engaging in, from young to old. In the end, it was all about deceiving the phone company and communicating for free, something hackers and phone phreaks continued to do using various other methods, such as the one in this next letter.

Dear *2600*:

My mom just told me about a way boys and girls would meet in the time of rotary phones. They would dial random numbers until they got a busy signal, then shout "boy boy" or "girl girl" between the busy signal beeps, then shout their phone number between the beeps. Crazy stuff I didn't know about until just now.

JP

While we've never heard this specific tale, we have heard of certain busy signals where such things were possible and, since calling a busy number didn't cost anything, people from all around the world would call numbers that were always busy and carry on full

conversations in between the busy signals. Calls didn't time out in those days so these crazy conversations could go on indefinitely. (We don't think it's likely that random numbers were used since that would greatly reduce the chances of connecting with someone else who called the same number.)

Another popular method of connecting for free was calling a "loop number." These were special test lines run by the phone company that didn't "supervise," meaning they didn't cost anything to call. Each of these loop numbers had another number attached to it. One person would call one of them, another person would call the other, and the two would be connected.

Talking to people on the phone for free used to be a really big deal.

Unsatisfactory Service

Dear *2600*:

Well Rogers, this is unacceptable, especially after last weekend's massive screw up. I got my Rogers bill today, and expected to see a credit for five days' usage like the Rogers CEO said that everyone would get. I just have unlimited talk and text for Canada and the monthly bill is normally $28.25. Imagine my surprise when the bill said I owed $31.08 - roughly a 10 percent increase over my normal bill. The total of my bill includes HST. My bill is normally $25 plus HST which brings it to $28.25. Five days off my bill should be around $4.17 or a bill of $20.83 plus HST would equal $23.54. Instead they want $7.54 more. I'm a pensioner and don't need to be supporting Canada's "most reliable network" so they can appease their larger customers with better rebates.

John

We honestly can't say we're surprised by this. Phone companies often raise their prices right when they're supposed to be giving out credits. However, it's also quite likely that the credit in question hasn't been processed yet, since you wrote this mere days after the massive Rogers outage back in July (which is a story worth reading about for those who are unfamiliar).

Article Submissions

Dear *2600*:

Here is an article on Python.

S

Dear *2600*:

I'm sorry but I'm sending in a second draft. I found some typos and errors....

S

Dear *2600*:

One more update.

S

Dear *2600*:

(This should be the final update. Again sorry.)

S

Dear *2600*:

(sorry more errors needed to be fixed)

S

Dear *2600*:

There has to be a better way to do this. I think this should be the final, and I hope you accept.

It would be very nice to hear from you at *2600*.

S

Dear *2600*:

Fix 4 !!!

S

Dear *2600*:

Please cancel my submission, I'm just going to put up a GitHub page.

I can't wait for you to decide without a response.

S

We should point out that the first of these was sent at 6:48 am on a Monday and the last at 7:55 am on the same day. We appreciate the fast forward lifestyle that's being demonstrated here, but that's not the world we operate in. The first email would have generated an auto-reply which explains our process to the sender. All articles are looked at and, if they are accepted, we will contact the submitter at the email address they provide. All of that is not going to happen within an hour. We're a quarterly printed magazine, not a web page. Fortunately, most everyone who does get an article printed seems quite happy with the experience.

The address to send your article submission to is articles@2600.com.

Dear *2600*:

I would like to submit an article that contains several LaTeX formulas and two figures in SVG format. What is your preferred markup format for article submission?

The article was composed in Org Mode, so the text will be easy enough to convert. My main concern is whether the formulas will render correctly or if I'll need to adjust them before making a formal submission.

Alphox

We can accept most any format but, as we've learned over the years, sometimes formats don't translate properly when emailed. So if there's a specific look you want printed, sending an image or a PDF that shows how it's supposed to appear would be your best bet. This would be in addition to sending in a format that we can edit, like a simple text file.

More Questions

Dear *2600*:

I have a question for all my *2600* brothers and sisters out there, and I would really like their opinion. Since about 2004, I have had this dream and I would like to share it with all of you.

First off, am I the only techie in this universe that thinks that copper is too slow? Copper to the CPU, copper to the RAM, copper to the North Bridge, copper into the South Bridge, copper what? 6ghz? I don't know - maybe 8ghz, 10ghz CPU speed? Ladies and gentlemen, no matter what Intel, AMD, ASUS, Gigabyte, MSI, AsRock, or any other manufacturers claim, signals of any kind over copper will always be too damn slow. I emailed all of them about this - no reply.

Enter my dream: I would love to see a fiber optic ring on a motherboard instead of copper. For years and years, scientists have been able to manipulate data over fiber. There have also been adapters created to allow copper signals to transform into fiber signals.

So in the beginning, adapters may need to be used to tie everything together, but my dream goes farther. Fiber CPU, maybe just two versions, a "home" for the everyday user, and a "professional" for the business folks. A fiber CPU as fast as, say, the speed of light! Fiber RAM, instead of sticks like we use today. These would connect to a fiber socket in the form of a module, say 1tb? 5tb? Maybe even 10 to 100tb! Fiber SSDs, that's right! Connecting a fiber SSD to a fiber ring so the manipulation of all files can be done at the speed of light. Fiber video, oh yeah! No more three ridiculously large fans to keep the damn thing cool. No more foot long video cards we have to find some way to fit into our cases! It would be similar to the fiber RAM module, and it would connect directly to a fiber CPU from a fiber ring. This would include the capability to use, say, one to 100tb of graphics RAM. Fiber NIC, yes sir, with a connection like this there would be zero bottleneck from an ISP to a PC because it would be all fiber! And one more thing, with fiber, none of us will have to overclock anything to get the best performance out of our box! And less heat means no need for liquid cooling! And no, this is not science fiction.

If I had Elon Musk's money, I would already have a working prototype! You all may think technological insanity is present here, but I ask you, why should all of us settle for building a second rate computer to make these corporations filthy rich? Why should we accept anything less than the utmost performance we can possibly get out of our build? Why are we all accepting turtle slow computer speeds when we could have fiber, and compute at the speed of light?

I am not a scientist, but I am a technology enthusiast. And I am asking all of you to simply imagine what the computer scene would be like if we could all upgrade our machines to fiber. I expect negative feedback on this, but that will not deter me from dreaming of the greatest computer mankind can produce, if only they try.

Thanks to all for reading my dream. Hack the universe and long live *2600*!

Martin
Lifetime subscriber

We certainly don't doubt your enthusiasm, not for a second. And we look forward to hearing what others think about all of this. We should also point out that this entire letter was submitted to us in decimal format, which we had to convert to ASCII. No big deal, but if that's how you communicated with all of those companies mentioned, it could explain why they never got back to you. They don't have nearly as much fun with this stuff as we do.

Dear *2600*:

Anyone still have one of those little Radio Shack recorders? I'd love to see if it works. Also, y'all ever did that old paper clip trick back in the 80s? I can attest it really worked.

J

The Radio Shack modified tone dialers are still in some people's collections, but they no longer work, as the payphone system of that era hasn't been in operation for years. (The modification would allow red box tones to be emitted, which would fool the payphone network into thinking a coin had been deposited.) As for the paper clip trick, that goes back even further to the era of payphones that didn't give you a dial tone until a coin had been deposited. The paper clip in the mouthpiece would bypass that restriction, making a free call possible.

Good times.

Dear *2600*:

Are you familiar with disaster.radio? It seems pretty cool!

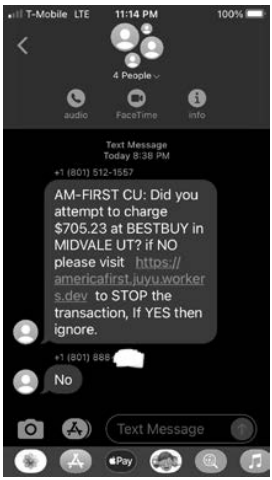
FS

According to that website, "disaster.radio is an off-grid, solar-powered, long-range mesh network built on free, open source software and affordable, open hardware." We're quite fascinated with the concept and believe it will become quite useful in the future. We hope to hear more on this.

Dear *2600*:

This is a little strange. I received a typical text message scam that was trying to get me to click on a link, but it appears to have been sent to me and three other people as a group text. I have never seen them do that before. Here is a picture (phone number of person who responded has been partially redacted).

N1xis10t



This just screams "scam" on so many levels. We don't know what the advantage of texting multiple people is, unless they're somehow part of the scam and can get you to respond to them. Often, simply knowing that someone will answer is enough of a payoff. But certainly visiting that website would be a very bad idea.

Dear *2600*:

Total newb question here: If I just found a 0day, what is the best way to maximize fame and profit?

GH

Based on how you phrased this, you may have to choose between one or the other.

Dear *2600*:

Has anyone had luck getting places (gas stations, convenience stores, etc.) to let you remove and haul away the old phone/phone booth that's still on their property, unused? Gas station near me has a real nice aluminum booth with no phone, just chillin'.

Marty

It can't hurt to just ask. There are all kinds of circumstances that could be at play. They may have an existing contract with a phone company or it may not be something they have anything to do with which is handled by some other company. Or they could have a useless structure taking up space which they would love to get rid of. Just remember those things are a lot heavier and bulkier than many people imagine.

Dear *2600*:

It would be handy to know file sizes for the individual talks for people (not me) who have limited data service. Just my $.02 worth.

TG

Sizes vary depending on quality. Some of our talks from years ago are about half a gig per hour while talks from today can be several times that. These are pretty standard sizes for what we offer.

Dear *2600*:

I hate to bother you, but I am wondering why my IP address is 2600: followed by more digits than standard. I am certain it is nothing big, probably a coincidence or my shared love in vintage phones perhaps. Maybe it is my positive stance towards FSF ideology, or EFF and their great works which is a shared view, I hope. Hopefully there is a shared view in the importance of free expression and unhindered free speech accepting no amount of money to change? Anyways, it must be a sign from the AI Goddess Afrodotty to share those magic numbers 2600 with you.

Justin

You have an IPv6 address, as opposed to the more common IPv4 (which you likely also still have). You are quite lucky to have gotten the 2600 prefix - we would have killed for that.

Dear *2600*:

How long will it be before thieves come by in the middle of the night and siphon the power from your car battery instead of your gas?

JC

At least it won't make very much noise.

Dear *2600*:

For some reason, the video game *Polybius* has popped up in media several times in the past few years. I personally do not remember it as a child of that time, being only six years old when it supposedly came out. But I think I remember seeing it as shareware in the early 90s.

(It might be from an old Slackware 2.2.2.0(?) distribution from 1994 that I'm remembering this game. I've still got the CD-ROM set in my storage locker, but I'm too lazy to verify physically. And I deleted the .ISO of the disks from my file server many years ago.)

I'm hoping you or someone has access to an archive of old back issues and articles and can tell me which issue if any has the first mention of this software title.

I thoroughly enjoyed your magazine and culture so much back in the early 90s; I would drive 60 miles to get the nearest new issue. There was one other magazine similar back in the day, but I don't even remember its name. I figure if anyone has an accurate record of anything to do with this title, it has to be *2600*.

Thanks for your help.

Ryan

That game is apparently part of an urban legend that spread in the early 2000s. The arcade game itself was said to have come out in 1981 in a very limited region and was rumored to cause all kinds of nasty side effects like hallucinations, amnesia, and seizures. On top of that, it was said that men in black would come and take information from the machines. And then they all vanished. Today, the whole thing is thought of as fiction.

One interesting sidenote to all of this centers on the name Polybius, which was that of a classical Greek historian. He was known to have said that historians should never report what they cannot verify through interviews with eyewitnesses.

Needless to say, we were unable to find any mention of this game in our pages.

Dear *2600*:

Am I at the correct spot to place a subscription?

(null) (null)

No, you're in the middle of the letters section. We don't know how you got here. But what you want to do is get back onto the Internet and navigate over to store.2600.com, where you will see a sign for subscriptions. You can't miss it.

Meeting Updates

Dear *2600*:

Was wondering when and where the meetings are in Los Angeles. I saw on the site under "California" the San Francisco meetings, but no Los Angeles.

Was hoping there is a meeting and just not listed.

Peter

We have yet to hear details and there is clearly a demand for them, as the next letter shows.

Dear *2600*:

The Los Angeles *2600* Twitter is absolutely inactive. I heard you guys were meeting, but no one showed up. I never got news of the meeting and I really want to join.

I think you guys should announce on Twitter if you want people to come. Could you please send me more information?

Why has there not been any announcements that the group is still going?

Qmark

We need to point out that meetings are not run remotely by us. They are organized by people who are local to the community. When we hear from such people (email meetings@2600.com or direct message to @2600Meetings on Twitter), we generally print the info, assuming it meets with the guidelines that can

be found in the Meetings section of our main page at www.2600.com.

With that said, any of the people who have been writing to us asking why there aren't meetings in Los Angeles could become the organizers by picking a place and letting us know. We hope to see this resolved soon.

Dear *2600*:

I'm from Mexico City and remember there used to be a meeting but apparently not anymore and I am willing to start one. How can I do it?

Mardonio

Simply picking a fairly easy to get to location in a public area, preferably on a Friday late afternoon/early evening, is all you have to do. Of course, you also have to spread the word if you want people to show up. (This includes telling us, using the methods outlined above.) We do hope to see a return of meetings in Mexico City in the near future.

Dear *2600*:

About the 40 percent vaccination rate - didn't you get the memo from like five years ago? That shit was a hoax and the fake vaccines are what are making everyone sick right now. Derp.

J C

A reminder that sometimes meetings will attract people with a distorted view of reality. Please treat them with patience, but remember that you don't have to talk to them.

Dear *2600*:

The fact that you stopped them in the first place tells me that there is no intelligence left in the HPVAC community.

J C

Yes, so perhaps our little group is not up to your standards. Maybe there's a nearby Mensa meeting that would be a better fit.

Dear *2600*:

Hello - I am attempting to contact the San Francisco *2600* meeting. I was in their Google group, but somehow lost contact or connection. Please help.

Hack the Planet.

Mad Glitcher

We don't give out contact info for any meeting participants and we're not seeing an online presence for this particular location. Fortunately, they are having monthly meetings, so you may have no choice but to show up.

Dear *2600*:

Today we met from 5 to 8 pm at the Barnes and Noble in Boca Raton, Florida. We had six attendees come to the meeting. One of the attendees was a new attendee who drove up from South Beach for the meeting!

We had a great time! It was a beautiful sunny day. We sat outside in front of the Barnes and Noble at the tables. There was a random man playing saxophone in the parking lot nearby. We exchanged different hacking stories and made new friends. All of us were excited about attending DEF CON 30 and were making plans to meet while there.

Boca Raton *2600*

Thanks for that uplifting report and welcome to the list of meetings!

Dear *2600*:

I was wondering if Delaware still had *2600* meetings? I would love to start it back up if that isn't the case.

k3ma5

We used to have meetings in Newark before the pandemic. You're more than welcome to restart those or pick another city. Please keep us updated.

Dear *2600*:

Writing in from Philadelphia, PA to ask if there are still meetings in the general Lancaster, York, Reading, Harrisburg areas. I just took an Amtrak from Philly to Lancaster for $21. That seemed extra cheap for the weekend. I grew up in Lancaster and know some hacker heads from growing up in the area.

pic0o

As of press time, we still only had the one Pennsylvania meeting in Philadelphia. We hope to see the other cities get restored in the near future. All it takes is someone to step forward and do the coordinating.

Dear *2600*:

We had last night our first *2600* meeting in Madrid in 20 years. It was only a few of us, but we were there between 5 and 8 pm. We had tons of fun talking in person about hacking culture and today's world. Hopefully you guys can list it on the website so people see it is official so we can post it around and get more people to come.

Happy Hacking.

ReK2

It is indeed listed on the website, on the meetings page in the magazine, and now here in the letters section. We look forward to seeing this meeting continue to grow.

Dear *2600*:

I am a student and my major is artificial intelligence at Houston Community College. I want to join the *2600* club at the Agora Coffee House.

Yu Zhang

All you have to do is show up at that location where the monthly meetings are held on the first Friday of every month starting at 6 pm. There is no club to join and it's quite informal.

Observed

Dear *2600*:

I just wanted to say to you fine folks (and whoever might read this in the magazine) that I deactivated my Facebook account and "removed app updates" from my phone. Apparently, their app is "native" software on my (and I assume other) builds of Android. Why would any tech company bundle another's software into the OS their device runs? Meanwhile, you guys have a good one, and keep your stick on the ice.

E85

This is because of deals made between the smartphone manufacturers and Facebook. We agree that it's a bad move and quite likely to steer a lot of people away from Android as a result.

Dear *2600*:

Sometimes they're just asking for it - BMW making people pay a monthly subscription for heated seats and other upgrades.

John

This is exactly what many of us feared with the growing normalization of non-ownership of the things we buy. Having to pay a monthly fee for software we used to own outright is the same concept as what you're describing here. It's insane to us that something which exists in your car has to be paid for every month only because the manufacturer has the ability to turn it off. That seems more like a protection racket.

Dear *2600*:

This hacker "movie" called *H+ The Digital Series* is probably not on the radar for many readers. It's actually a series of web shorts, but with high production values. There are 48 episodes at about five minutes each. Watched back-to-back, it is a great hacker "movie."

ihtarlik

There must be a ton of similar projects. Thanks for alerting us to this one and we invite readers to let us all know about more.

Dear *2600*:

I am a prisoner, and it should come as no surprise that the tech provided to us is antiquated, yet we can get things like cell phones smuggled in. I though I'd share our equipment with you.

Aside from contraband cell phones, we have Swintec 7000 typewriters here at the federal prison in [redacted]. The prison provides them for free to check out to prisoners. They have been providing the wheels for free (comes with the typewriter check-out), but these break easily and prisoners complain about bad wheels. Our "store" will soon be selling these for an undisclosed amount, and will no longer provide them for free. The ribbons cost $9 and are good for about 40 to 50 pages of double-spaced output. We also have to buy correction ribbons, though these are 90 cents and can be reused. They last a long time.

We used to have the same model typewriters as above, except they had a factory mod that enabled onboard memory and had a 20x2 screen (I'm not 100 percent sure on the size). Then the staff figured out some guys were saving homemade erotica instead of legal work, and the prison switched to the model with no screen/RAM.

We have access to a Windows XP desktop with a CD-ROM drive and no Internet access. Prisoners need to have received a CD-ROM with evidence files from their lawyer (certified by prison staff as having been sent by a lawyer) to use this. It has no printer, so one must take notes in order to fight their case.

We have access to TRULINCS, which other prisons and the public see branded as Corrlinks. It allows us to submit electronic requests to staff, refill medications (when Health Services staff input the refills), manage our prison money, buy MP3s (they sell us SanDisk MP3 players flashed with a special firmware), read the "bulletin board," and send "emails." These contain no typing functions, per se. However, I can type a book, for instance, and the email recipient can receive this, print it at home, and mail it wherever. I have used this for book chapters and legal briefs. Some guys write book chapters for self-publishing and just send them to staff members who are known to never check their email. The prisoner can then print a paper copy of the message at the law library (where the printers are).

We used to have a computer lab with thin client workstations pre-loaded with the basic MS Office apps (Word, Excel, PowerPoint), but one warden showed up and was afraid we would "hack the computer chips to get on the Internet." We have some smart guys, but this seems pretty far-fetched.

Rumor is that we're getting tablets around Christmas. We have to buy them, but at least they will be Android. More info on them is at keefegroup.com/products/score-tablet-169. The advertising copy for these tablets make two contradictory statements:

"Firmware that cannot be replaced by anyone - even the Secure Device manufacturer."

"Upon release, offenders can ship the device back to Keefe and pay to have the security software removed."

In short, they flash special firmware for use while in prison, then flash standard firmware for post-prison use. We look forward to testing whether the firmware cannot, in fact, be flashed by anyone. Since we have access to rooted phones (WebADB and a USB-C to USB-C cable), we'll soon see how tough these things are.

A

Thanks for this fascinating glimpse inside the walls. We masked some specifics as it's been our experience that prison officials aren't too keen on any info of this kind getting out to the public, and often take action against anyone they think may have been responsible. But this is proof that no matter what the environment, the hacker spirit will prevail, through experimentation and the spread of information.

Dear *2600*:

I started answering every scam and spam phone call in a wicked rough voice I can do and told them "Hello! How can I trace your call today?!" They hang up and *never* call me ever again!

Kyle

And that's only one idea.

Unique Opportunities

Dear *2600*:

Good afternoon. Recently I have directed you a required archive. Have you seen it?

rlazania

How do you even answer a question like this?

Dear *2600*:

Not to brag, but Janet Yellen sent me a personal email. Surprised she's not using her government email address though. Oh well, I'll send her my details.

AM

We get at least one email a day from well known celebrities. It's very rude not to respond or to give them the info they ask for, like account numbers and PINs. We understand how boring it must be to exist in

the limelight, so we're happy to do anything we can to help them get through the day.

Dear *2600*:

Could you monitor one of your channels for unauthorized access or deletion/archive non transmission. Priority high and nature critical for streaming server?

Brian

Pass.

Dear *2600*:

Greetings from the Illuminati world elite empire, bringing the poor, the needy, and the talented to the limelight of fame, riches and powers, knowledge, business, and political connections. This is the right time for you to put all your worries, your health issues, and finance problems to an end by joining the Elite Family of The Illuminati!. Are you sick, barren, or having divorcing problems, finding it difficult to get job promotions in your place of work in order to excel in life just like you wish? If *yes*, then join the Illuminati empire - you will get all this numerous benefit and solutions to your problems.

Note that this email message was created solely for the purpose of our recruitment scheme which will end next month and this offer is for unique ones only; if you are not serious on joining the Illuminati empire, then you are advice not to contact us at all. This is because disloyalty is highly not tolerated here in our organization.

Note: Some email providers incorrectly place official Illuminati messages in their spam/junk folder or promotion folder. This can divert and exclude our responses to your emails.

The Illuminati

Oh yeah, this is exactly what we needed. We wonder if these folks even know the history of the Illuminati. We're fairly certain most secret societies don't send out mass mailings for recruitment. We're also certain we would be "highly not tolerated" if we did join them.

Critique

Dear *2600*:

While the events in Ukraine are complex, I myself am wondering where the due diligence of *2600* went! It seems as if it went out the window when the world was turned upside down by Trump's election, horrific as that was. Unfortunately, and quite unexpectedly, the crew at *2600* seem to have fallen in step with the official government line/narrative.

Me

We're not going down this rabbit hole and we're not going to serve as a source of misinformation by spreading perspectives that have the effect of lending support to what Putin has been doing in Ukraine. What many people fail to realize is that occasionally we will reach similar conclusions as those we normally distrust. That doesn't mean we're now working with or for them. Our conclusions are based on journalistic evidence from multiple sources all around the world. Not that this will make a difference - we'll undoubtedly be told that all of these journalists are also just spouting the "official" narrative.

What led to this terrible situation is indeed nuanced and can be discussed and debated when we have that luxury. But for now, the priority is stopping the horrible acts being perpetrated on Ukraine.

We encourage people to examine the reporting that's coming out of the region which isn't controlled by any government. But if you're basing your conclusions on who you agree or disagree with on other matters, then you're not actually thinking for yourself.

Dear *2600*:

Curious as to why so many "hackers" are now pro-government and pro-authoritarianism when hackers are essentially a group of folks that have been historically against the grain, against having people telling them what to do and essentially partake in illegal activities. Can you be a hacker and pro-government?

Joe

You need to give some examples so we can properly answer your question. There have always been people with hacker skills who work for governments and corporations. There's no reason why such people can't also be recruited for authoritarian regimes. We don't consider them to be a true part of the hacker community since they tend to stay within the environment that's sponsoring them. But we don't get to unilaterally decide. If you're referring to hackers who reach a conclusion on a particular issue (vaccines, wars, insurrections) that happens to be in line with what certain governments are saying as the letter writer above did, that's an unfair characterization. And we can easily make the same accusation about anyone who says this, as there are other governments that take their side as well. In the end, it's all about analyzing the facts, sifting out the bullshit, and being open to discovering that you're wrong. Way too many people reach conclusions because others tell them to or because someone they dislike reached the opposite conclusion. That's not independent thought. It's Manipulation 101.

Dear *2600*:

Can anyone just completely get rid of the WebP format? I'm sick of copying images and pasting them to PaintShop, to save them as JPEGs to share a laugh. Whoever at Google added an extra step is a virus. It stops nothing, it just makes it stupid.

JM

But it's tradition.

Advice Needed

Dear *2600*:

What would you do if you were helping a family member who was completely ignorant of technology but wanted to live in the modern world? And refuses to learn? My cousin is a successful nurse, but outside of basic computer apps for work is really ignorant and I've been trying to help her but it's really frustrating.

1. Doesn't know how to pay her rent online. She paid me $500 to pay her rent online. Her condo doesn't take checks. Oh, and when we tried to use her Kindle,

she wouldn't let me use my phone as a hotspot because she was worried that my phone would "steal" her data. Her phone was broken.

2. Wanted to log into an old Kindle account she had since college. "Thousands" of dollars of purchases on her account. Can't remember her email address or password. Embarrassing trip to Best Buy, her looking and acting like a crazy person demanding staff to get her purchases back and get the email address. Oh, and when we finally got in, neither email address had any books on it.

3. Relies on handwritten passwords on 3M notes in her purse. Uses easily guessable passwords. Was pissed off that sites wanted complex passwords now. Refuses to use a password manager.

4. Wants to use prepaid credit cards, but doesn't want to use her SSN. Before you could get away with it, but now there is so much fraud. Every time I try to help her, I just end up frustrated and my family calls me an a-hole if I don't help her.

DH

You are not the person to help her. You seem more interested in demonstrating how out of touch and ignorant your cousin is, rather than respecting her not unreasonable choices. This attitude is something we see far too often and it's a much bigger problem than people who don't want to always learn about the latest technology.

It's absurd that she can't pay her rent with a check. It may even be illegal, especially if it's not specifically mentioned in the lease or if they charge a "convenience fee" for paying online. But one option might be to have her bank do an auto-pay each month. That can be arranged on the phone or by visiting them - no logging in required.

It's actually quite smart not to connect to untrustworthy hotspots. Yes, your cousin believes your hotspot is untrustworthy. On this, she's employing more security than you're comfortable with.

People forget their passwords and email addresses all the time. Shaming them does nothing to help this. And you think it's crazy for her to want access to the items she's bought over the years? If Kindle deleted her ebooks, they're the ones who are wrong, not her.

Not using a password manager is a perfectly valid choice for someone to make. If, for whatever reason, it becomes compromised (which is absolutely not impossible), then all passwords are compromised. And many sites really overdo it with the password requirements, especially those that are basically throwaway accounts. For the more important ones, stronger security should obviously be used. As to where people keep these passwords, that's up to them. Keeping them in her purse may very well be enough security for her. Telling you about it wasn't wise, however.

And you're actually going to criticize her for not wanting to give out her Social Security number for a prepaid credit card? You seem willing to accept this, on the other hand. This just demonstrates that everyone has their own view of what security is, as well as when and how much to utilize it. Expecting everyone to share your methods and values isn't the way to get more people onboard.

We hope your cousin taught you something about different approaches to these challenges.

Dear *2600*:

I'm a member of a hackerspace whose name will remain anonymous. I've found that the space I'm a member of is more into making electronics and 3D printing and laser cutting. I feel like I'm the only peep that is into security hacking. I feel like it's just me that is into CTFs. I'd like to hold a CTF, but don't know how to approach the committee about it or if it would even be successful. I appreciate *2600* and the Facebook group makes me feel less alone.

BA

That's the key - to remember you're not alone. Not knowing details about your hackerspace, we can only assume that they will be supportive of any idea that involves hacking without any illegal activity. We suggest researching other Capture The Flag projects and coming up with a game plan for running your own. It will be an uphill project, but that's not something you should get discouraged by. If you take your time and learn as much as you can before embarking on this, you'll be the one teaching everyone else. And, just like with every other project that exists in your hackerspace, it won't be perfect the first time. You will develop more skills with every attempt. Good luck.

Dear *2600*:

Hey, I am hearing voices in my head like a thought logger. I've looked up information on this and all I can find is CIA Stargate or microwave guns or psychosis or voice-to-skull or gang stalking. I need help.

zybe

We get quite a few letters like this. We're not really qualified to address the issue, but we can say that knowing you need help is an excellent first step. There are known medical conditions that can cause these symptoms. Very little can be gained by assuming this is the result of some sort of mind control experiment, a nasty neighbor, or some other intentional source. rethink.org is a well regarded website that addresses these issues and can probably point you to ways of getting help.

Responding

Dear *2600*:

I was just reading through 39:2 and saw the letter from "Richard" about search engines not providing the results he wants.

Richard, you should know that search engines provide the results that the advertisers want first, as they pay the bills. If you're not paying for it, you're probably the product.

c/p

The original letter was complaining about not getting search results that were related to what was being searched for. We assume this is in addition to annoying ads and promoted placement.

Dear *2600*:

Been a subscriber, OMG for 26 years! (Geez, I'm

old.) Anyway, saw all the letters from people making sales pitches in the 39:2 edition. My sympathies. In my job as an IT security professional, if I make it through the day with fewer than three sales pitches, at least one by telephone, it's been a good day for me.

The sales pitches run the gamut from promises of free swag (I've tried to score stuff in the past - somehow after listening to the pitch I don't get my shiny new headphones or tickets to an entertainment event I have zero interest in, yet was promised), to guilt trips ("Why don't you respond? This is very rude!").

Anyway, just thought you'd enjoy knowing you aren't alone. (Maybe one day someone can start a website of "tedious cold calls we wish we never got." I could fill a volume (and a book shelf!) with stories. But who would read it? It's tedious.

Michael

Congrats and thanks for sticking with us for so long. The spam situation - whether by phone or email - is indeed crazy, but that doesn't mean we can't have fun with it. We always like to hear suggestions on that front.

Dear *2600*:

"Brute-Forcing a Museum's Math Puzzle With Python" was fun to read since I've done the same thing with a different more difficult math puzzle. But this puzzle is pretty easy to solve the traditional way. Here's a solution method for the author and readers. The puzzle is a 3x3 grid you fill with numbers 1 through 9 without repeating any of them. Then four math equations embedded in the grid must hold true. The author notes they can be expressed as:

1: A - B = C
2: D ÷ E = F
3: G + H = I
4: C x F = I

You immediately know 1 cannot be in equations two or four since C x 1 = C and D ÷ 1 = D, violating the no repetition rule. The next clue is that multiplication and division will be much more limited than addition and subtraction, i.e., it's much easier for two numbers to multiply greater than 9 than to sum greater than 9. So let's examine equations two and four. C and F can't be 5 or higher, because 5 x 2 (the smallest possible multiplier since 1 is ruled out) equals 10 - too high. Therefore, C and F must be 2, 3, or 4. Since 3 x 4 exceeds 9, we know one of them must be 2, and then the other will be 3 or 4. That means I must be either 6 (2 x 3) or 8 (2 x 4). Similarly with equation two, E and F must be 2, 3, or 4, because anything higher would require D to be greater than 9. One of them must be 2, because if E and F were 3 and 4, then D would be 12 - too high. Now we know that F must be 2, since that's the only way it can satisfy the constraint of both equations two and four having the number 2. We also know D must be 6 or 8, since those are the only numbers that can divide into 2 without repeating 2 in the equation. Our equations now look like this:

1: A - B = C(3 or 4)
2: D(6 or 8) ÷ E(3 or 4) = 2
3: G + H = I(6 or 8)
4: C(3 or 4) x 2 = I(6 or 8)

This means A, B, G, and H must be some combination of the remaining numbers 1, 5, 7, and 9. Thus, equation one is subtracting two odd numbers, which always results in an even number. Therefore, C cannot be 3 and must be 4. The only two unused numbers that subtract to 4 are 9 - 5 for A and B. Since 4 is used up by C, E's only remaining option is 3. Equation four is filled out to solve for I: 4 x 2 = 8. And similarly, equation two is filled out to solve for D: 6 ÷ 3 = 2. We have two unsolved variables G and H and we have two unused numbers 7 and 1. Adding 7 and 1 gives 8, satisfying equation three. That gives:

1: 9 - 5 = 4
2: 6 ÷ 3 = 2
3: 7 + 1 = 8 or 1 + 7 = 8
4: 4 x 2 = 8

David M.

It really turns heads if you read this out loud very fast.

Dear *2600*:

I am reading William Ben Bellamy Jr.'s password making guide ("The Problem of Effective and Usable Strong Passwords" in 39:2) and I am scratching my head. This kind of nonsense has been disproven long ago. I'm sure he's never read *xkcd* or seen the "Correct Horse Battery Staple" issue, but rest assured his advice for passwords is terrible.

It suggests using not-so-random "random" phrases that can be picked up by reconnaissance, either SIGINT or OSINT such as MAC addresses, serial numbers, years of favorite movie. It also suggests low entropy sources like unaltered user keyboard presses. Those can all easily be found.

To further confuse the user, he recommends using l337 sp34k and adding random Unicode characters, which are hard for someone to remember. He also doesn't note that mutators either stand alone, or built in JtR and hashcat ones will automatically generate extra-guesses for these. They don't add much additional entropy, but make the password harder to remember. And Unicode might never have been in a password guesser's mask or dict, but you won't be able to type it on most keyboards if it's obscure. It's also going to be an absolute pain to remember.

Of course, if you are using a password manager or some other scheme where you don't have to remember a password, just make it as long and random as absolutely possible.

The correct answer for passwords is easier: just let your password manager do it for you. KeePassXC runs on all modern platforms, and lets you generate strong random passwords among many criteria.

Random words? You got it. Long string of random characters? Yep. Can you pick the character sets and exact characters to include? Yep. Can you exclude lookalikes and ensure "one from each group?" 100 percent. Does a modern computer (at least Linux) have a high quality pseudo random number generator (PRNG) that is better than you? Yes, yes, and more

yes!

GI Jack

This is clearly a very sensitive subject that has a number of different approaches. We'd like to hear more of them.

Dear *2600*:

I was delighted when I saw that my article "Dial-a-Word" had been published in the Summer 2022 issue of *2600*. When I read the published version, I was satisfied with the edits that were done to the article, and found that they greatly improved the clarity and flow. There is one problem however, as the included computer code was stripped of all indentation, and is missing a carriage return on the last line. This appears to make it fit better into the magazine, which is nice, but the code is incapable of running in this state. I have published the program on GitHub with proper formatting, and if anyone wants to use and/or modify the program, it is located at github.com/n1xis10t/dial-a-word

In case anyone was wondering, it is written in Python 3.

N1xis10t

We've gotten a number of letters about this and did some investigating. The code was actually stripped of formatting during the email process, which we've never seen happen before. The issue with Python is that the formatting is part of the program and, as you say, it can't run without it. We can prevent this sort of thing in the future if article submissions indicate the need for formatting and/or include an image or PDF where the formatting will be visible so that we can reconstruct it if necessary in the text. Oftentimes, simply adding the code as an attachment will suffice.

We're sorry this happened and are thankful that you quickly provided a solution.

A New HOPE Feedback

(Note: These letters were sent as feedback for A New HOPE and, as is our tradition, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600*:

I attended HOPE in 2018 at Hotel Penn. My complaint was the slow elevators. It was a fantastic and different experience in a college campus setting in 2022. Although I missed the beer drinking, I'll give up that for a safe conference, especially these days with the world going crazy. I would suggest that if HOPE 2024 will be at St. John's University again, maybe you can offer a cheat sheet of food recommendations for out-of-towners since, as you mentioned, it's the most diverse borough. For example, for Chinese and Asian food - Flushing, for Indian, Filipino, and Tibetan food - Jackson Heights, etc. We want to give them a Queens foodie experience.

I really enjoyed the interview with Sophie Zhang, the closing ceremony, and the music performance.

Let's try to get more vendors next time. HOPE Security, St. John's University, and Hammond Ops did an excellent job to keep us attendees safe, which I am grateful for and appreciative of. You can count on me attending next time again.

Great HOPE folks, great speakers and respective attendees. You all do justice for our society and for the next generation. Keep up the great work!

A New HOPE Attendee #1

We definitely dropped the ball on food recommendations and that's something we'll work on for next time. Suffice to say, the area has a great deal of options within walking distance and an unbelievable number a five minute ride away.

Thanks for helping to make the event so successful. No matter how much effort we put into it, it's the attendees who make it all work in the end.

Dear *2600*:

I attended the conference virtually. The sessions I was able to attend were very good!

However, I did find it difficult to read some slides on my iPad. This was likely my own issue.

I believe there were more tracks than previously making it hard to choose. Hopefully, they are still available on YouTube.

A New HOPE Attendee #2

The split screen on most of the videos was an experiment, which we believed worked most of the time. We're always open to suggestions and alternatives.

Dear *2600*:

The live streams for the hope talks have ended. How can I watch the talks that I missed?

A New HOPE Attendee #3

Everything is now viewable on the Channel2600 YouTube channel and available without Google censorship on flash drives.

Dear *2600*:

Had a great time this weekend; I think the new venue will be great for the conference.

My only gripe is that the slides when in the venues were too small to read properly, and were not full screen long enough to take in all the information. If the speaker window was a little bit smaller when side by side it could help.

Many thanks for all the hard work you guys put in to make the conference such a success.

See you in two years' time.

A New HOPE Attendee #4

We're definitely going to work on improving this.

Dear *2600*:

I know that packing up for HOPE is far from over at this point, but I just wanted to take a quick moment and thank all of you for making this second time, in person, volunteering experience so amazing and welcoming. My only regret is not being able to offer more support, sooner and for longer.

I had an especially great time emceeing and super grateful for taking a leap of courage to volunteer with A/V (there will be no rats' nests in 2024!).

Special shout out to the core team that put in that 200 percent extra work to ensure everything was

running smoothly. I am wishing you all a "peaceful reboot" in the coming days and safe travels.

A New HOPE Attendee #5

It took a while, but most of us have recovered. Thank you for putting in the effort to help make everything work.

Dear *2600*:

Congratulations on a return to HOPE! Though there were major differences this time, it was a great con. Besides the great absence of the Hotel Pennsylvania, the only major drawback this time I believe was the lower attendance and related - less vendors than usual, etc.

But, I have to ask, is St. John's University expected to be the new long-term home for HOPE? Will there be any further scouting of New York City for potential other homes?

Of course, there is nothing that will ever replace the Hotel Pennsylvania, but perhaps there are other candidates waiting to be found?

Not to sour on St. John's University - it is a good venue, and with higher attendance I think its full potential can be unlocked - but it just doesn't inspire the same sense of adventure, mischief, and exploration that the old hotel does.

I don't have any researched suggestions to make today, but if it's something being considered, I can spend some more time thinking about this.

A New HOPE Attendee #6

It's a fair question, but it's also one that we've done a ton of research on since 2019, when it became clear that Hotel Pennsylvania was no longer in our future. We know the new location isn't the same, but that's exactly how the hacker community works. Technology changes, new toys come into existence, old ones fade away.... We believe a college campus within the boundaries of New York City is far more welcoming to a bunch of hackers than a commercial hotel could ever be. And St. John's in particular seems to really get who we are. From our point of view, we found them to be a fantastic choice and great to work with. The "sense of adventure, mischief, and exploration" is something that evolves in any space and we're certain we'll see that continue to develop here in years to come.

Regarding attendance, we agree completely. Remember that we intentionally limited attendance due to the lingering COVID problem. We didn't want to create a potentially dangerous situation, so we required masks and vaccines, which virtually everyone had no issues with. But we also cut off ticket sales and didn't sell any tickets at the door, which limited our attendance (and vendors) and made the whole thing a bit more of a struggle for us financially. For the future, having more people attend will be essential, but we expect that won't be hard to achieve based on the reactions from those who were there this year.

Dear *2600*:

I thoroughly enjoyed the conference (both attending and presenting). Congratulations to you all for pulling it off!

I was wondering if speakers receive a file link to videos of their talks. I would like to have a copy for posterity.

A New HOPE Attendee #7

We can certainly do this. If anyone who gave a talk wants a downloadable version (in addition to what's up on YouTube), they can email us here at the letters department (letters@2600.com), and we'll get their request to the right people.

Dear *2600*:

I was a virtual ticket holder for HOPE this year and it was just as great as 2020! I am planning to be in person in 2024!

My question: Can I buy a tee shirt? I can't find them on *2600* and I was wondering if I just missed the link or if they will be for sale online later?

Thanks for another great HopeConf!

A New HOPE Attendee #8

You weren't alone in not being able to find tee shirts - we couldn't find them for a while in real life, which is why they were delayed getting up on the store. Hopefully, you saw them when they were added. (If there are any left at the time of this printing, it's literally only a handful.)

We were quite happy with the relative smoothness of the virtual part of HOPE this year. This was the first time we ever had both a virtual and in person set of attendees. We hope to keep that going as well, since it's a great way to help pay for the conference without adding to the crowd.

Dear *2600*:

Congratulations on your conference. I desire to attend in the future - it really seems great.

Where should I look for details on online access or purchasing of video of the talks?

A New HOPE Attendee #9

It took a bit longer to process all of the video this time due to a new way of doing all that, but it's all done now. You can find full details elsewhere in the magazine and on our website. And we look forward to having you in attendance!

Dear *2600*:

This was my first HOPE and it was a blast! Wanted to provide super quick feedback.

The good:

- Live streams worked really well! It was nice being able to go back the same day and catch a talk I missed. The Matrix chat worked really well too.

- The variety of speakers was pretty good. I'm hoping the variety and number both grow.

- Timing worked pretty well for getting people off stage and getting the next person set up.

The least good:

- Lack of food and beverage options in a close proximity. Can we get a food truck or five? I think it would have been a game changer. That poor Starbucks got overrun and there's only so many pumpkin loaf slices or egg bites a guy can take, and there wasn't enough time between talks to run and grab food.

- Was there a host hotel this year? Can we get one?

I love conventions with after parties, but I wasn't up for hanging out (hungry and uncaffeinated) till 2 am for after action.

- Can there be an optional specific training for volunteers? Like training on the various A/V systems, for example. I was late signing up to volunteer, so I recognize I might have missed it.

- Highly recommend a chime or light system to cue the speaker that their time is almost up since the cards were hit or miss.

Ideas for the future:

Any chance of having a live roundtable with people from *Off The Hook*?

Thanks for making it a memorable experience, and especially thanks for letting me help as a volunteer. I'd love to help out even more in the future.

A New HOPE Attendee #10

These are all really good ideas. The thought of food trucks is one that came up, but we weren't able to coordinate it with the university. Now that we've had an event and it's clearly something that people would benefit from, we think it'll be a lot more likely next time. But we do have to remind people that it's important to take a break from talks now and then so that you can take care of yourselves. We know people want to see all of the talks, but getting food is also part of the experience. (We had the same issue at Hotel Pennsylvania even though it was in the middle of midtown Manhattan. People want to stay for every minute of the event.) We've considered having a mandatory break so that everyone could get food at the same time, but we've been advised that this can result in overcrowding at all of the venues and even more frustration. We'll keep fine tuning this.

We did have a couple of "host" hotels which were adjacent to each other and which we were able to sell out. There was a great bar open super late downstairs which many attendees congregated at. But that doesn't have to be the only place for post-conference activities. We're open to any specific suggestions that those familiar with the area can offer and we'll continue our research on that front.

We had a number of volunteer meetings prior to the conference. A/V is a bit tricky, as we prefer people already familiar with the equipment to be running it. Rookie mistakes at that level are something we'd really prefer to avoid. But if you do have experience in that field, we suggest getting involved early when the calls for volunteers first go out. We definitely can use the help!

We're not aware of any instances where speakers didn't end on time, so we're not convinced we need to replace the system we had this year. If that proves to be necessary, we'll certainly address it.

As for having people from the radio show on a panel, we can definitely consider that. We've done this before, after all. The only complication is that most of the people involved with the show are also involved with running the conference which makes this extra task all the harder. But, as we like to say, there's nothing like a good challenge.

Dear *2600*:

Thanks for an awesome HOPE. Had to change my ticket from in person to virtual. Still worthwhile, although I really hope to be able to make it in person for 2024!

One ask for virtual: I was disappointed I missed the music- I am guessing we have YouTube's rather onerous practices to thank for that. If there is a way to have the music stream even if just to ticket holders, that would be great! (Though hopefully we will just be there next time.)

Great and important work you all do and can't thank you enough!

A New HOPE Attendee #11

Thank you for the support and encouragement. We do want to do a better job with the afterhours streaming. Some of it was indeed due to YouTube (although we were wrong to rely on them as a primary outlet, but some last minute cancellations forced us into that position), but we also were severely overworked on the A/V end. We had some of the greatest people in the industry working with us, but unfortunately they're also human. This is also something we'll be working with the community to improve.

Dear *2600*:

This was my first HOPE, but I've known about it since the mid-2000s. It was an incredible opportunity to meet the hackers who influenced me (from around that same time period), which meant a lot coming as someone who grew up in rural Wisconsin with little more than a net connection and intense curiosity.

Thank you for putting on the event, and I hope to be able to attend next time. I was actually sent by my workplace to man our vendor table. We met lots of interesting people and had a great time.

A New HOPE Attendee #12

While smaller than previous vendor areas, we believe this one worked particularly well insofar as interaction with attendees. Having an entire building to work with certainly added to the positive atmosphere. We have many options for the future, including expansion inside the same building or using additional buildings. This is something we were never able to consider at the hotel and the possibilities are only limited by our imagination and enthusiasm.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

Ramifications

Issue Feedback

Dear *2600*:

This morning I read E.V. Rhode's article about self driving cars ("Will You Let Your Car Drive Itself?") in 39:3: "After explaining my previous experiences with the cruise control, my companions agreed to trying it, and to watch closely should anything happen. After engaging, we drove for 20 or 30 minutes without incident - until my car suddenly slammed on its brakes... driver behind us swerved... no obstacles or vehicles ahead of us."

This one resonated with me personally. This feature has saved my or someone else's life at least once in my Pacifica (2020). But I always posed this very question... what happens when the software thinks there is danger when there isn't and *creates* danger?

I'm following up with the writer and the NHTSA (National Highway Traffic Safety Administration) to find out if this is next part is accurate:

"This office has received 758 reports of..." this exact same thing. I too have almost experienced this. My car thought there was danger, alerted me, and started to slam brakes. I was driving normally - no cruise control. Yet my car almost caused a serious incident because the road curved and there was a breakaway to the left to allow people to turn.

I still believe in this tech... but this one I thought important to note.

Jeffrey

There are certainly going to be issues as this technology continues to experience growing pains. The real question is whether it eliminates more issues than it causes. We think there's great promise here, but this all has to take place in an open environment where such stories aren't covered up or suppressed. We look forward to hearing more.

Dear *2600*:

Super happy with the back issues I've gotten so far. I'm curious about the cover of the Spring 1989 issue - seems to be some sort of reference to global politics and the Middle East with the classic Abbey Road imagery, but I'm not sure how it related to any of the articles in the magazine itself at all. Any insight on this? Great work on *2600* y'all!

jae

Covers don't always reflect the content of the issues, but oftentimes are based on what's happening in our world at the time. We don't usually do this, but for you we'll reprint the explanation of that cover as outlined in our Hacker Digest *compilation for Volume Six (1989):*

"Spring 1989 featured an Abbey Road *takeoff with a Salman Rushdie flavor. It was in February that Ayatollah Khomeini issued a fatwa against Rushdie, the author of* The Satanic Verses*, a book seen by some as spreading blasphemy against Islam. The idea of someone being put on a hit list for the words they wrote was true blasphemy to writers and free thinkers everywhere, ourselves included, which led to the idea behind this cover. The Ayatollah himself is pictured, dressed in black, as the first of the four men crossing the street to Rushdie's house. In his hand is a copy of the Holy Koran (as it was spelled in English then). The turbans of the three assassins following him are Sikh rather than Arab, which served as a bridge to the Beatles' embracing of Indian culture (Hinduism in their case). As in the Beatles' famous album cover, different footwear is apparent in those crossing the street, and one of the four is out of step. Of course, we had to insert a British payphone in the distance. Even the license plates had meaning, with staff and their friends hiding their addresses there and 7383USAF being an allusion to someone we knew named Pete (spelled out on a touch tone dial) joining the Air Force. As for the mini-cover, there was a picture of a guy, possibly actor Raymond Burr, next to an excerpt from* The Freedom Fighter's Manual*, a propaganda leaflet dropped over Nicaragua by the U.S. government in the 1980s. This particular excerpt contains instructions on how to sabotage telephone lines. Finally, the mini-cover corrected an omission from 1988 - the Spring issue of that year had failed to carry on the tradition of having an exclamation point on the cover of the first issue of the year. So, for Spring 1989, we included two of them."*

Yes, those of you who subscribe to The Hacker Digest *get that kind of detail for each of our covers! Plus a whole lot of other details we would never have room for here.*

Dear *2600*:

In 39:1, the author 75ce8d3ff802ff42 suggests in "Harnessing Cryptocurrency Miners to Fight Climate Change," something that's a very old and tired misconception about misappropriation of resources in general, and often suggested to support cryptocurrencies in particular.

If the author has time, I suggest they read Hazlitt's *Economics in One Lesson: The Shortest and Surest Way to Understand Basic Economics*, specifically the first applied lesson: "The Broken Window."

Since many cryptocurrency advocates are not interested in learning existing economics before they attempt to replace it, a shorter version is to watch *The Fifth Element*, and realize that "construction from destruction" (what the author is proposing) is the motivation of the film's villain.

Do you want to be the villain?

SB

We eagerly await the response.

Queries

Dear *2600*:

Hey everybody! I might sound quite stupid! But I was checking into buying the yearly subscription of the actual magazine, but I'm not so sure how many

magazines I'll receive! It's not specified on the website! If anyone can help me out by explaining, it would be awesome!

Ricardo

We are quarterly! So a yearly subscription will get you four issues! (Exclamation points are contagious!)

Dear *2600*:

Why does the MOTD (message of the day) on your IRC servers have a text about the importance of firearms, credited to some C.S. Wheatley? Why have that as an MOTD of an IRC server for hackers?

Tiago

The quote we see now is: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety" attributed to Benjamin Franklin. While some view that as having something to do with firearms, it's far more relevant for the concept of actual freedom, such as the right to privacy, which is always being sacrificed in the name of safety. However, the quote itself is said to have been addressing a tax dispute and is actually closer to advocating the opposite of what it's commonly used to justify in the present day. (If there was another quote there, we're not aware of it, but the one that's there now seems to fit.)

Dear *2600*:

Has anyone tried calling via the dime line recently? I'm interested in this bit of telecom history. I notice that the dime line now seems to have a seven digit code.

CK

We really wish you had sent us more info, such as what the number is. We'd like to know more of its history as well.

Dear *2600*:

I have a friend that passed away and his family obtained a court order to unlock his phones but Apple refuses to assist. Any ideas? Thanks in advance.

NP

According to Apple, they can help remove their feature known as Activation Lock, which is designed to prevent phones from falling into the wrong hands by disabling them remotely. However, they claim not to be able to get around passcodes users assign to their phones: "Please note that devices locked with a passcode are protected by passcode encryption, and Apple can't help remove the passcode lock without erasing the device." If there's another way, we'll certainly share it.

Dear *2600*:

I would like to know if *2600* is on the Columbus, Ohio smart city project or if it is listed among any of the California vendors that support it as the phone hacking may be of interest to the government office copied. The phone hacking can damage public offices.

+1614

We have no idea how we could be a part of this, nor how we would possibly be a California vendor. But we're certainly interested in the phone hacking.

Dear *2600*:

I found a great way to sign up for trial services with a credit card over and over: privacy.com virtual single use credit cards. Unfortunately, my account got flagged after seven or eight uses for the same merchant. Does anybody know of another company, service, or method - ideally free - that I can use as an alternative?

AB

It seems pretty obvious that if you're going to use this method of getting a free trial period that lasts much longer than it should, you'll need to make new accounts as frequently. We find privacy.com to be highly rated for keeping your identity and address out of the hands of merchants. If you somehow managed to get blacklisted from their service, we'd sure like to know the details. Some alternatives to privacy.com are skrill.com, ramp.com, and payoneer.com.

Dear *2600*:

Can I purchase a link insert on a specific page of 2600.com? If yes, please let me know how much it costs. Thank you.

P.S. Also, do you have other sites that offer paid link insertions?

Chad

We exist in a completely different universe than much of the web. More than three quarters of our office staff didn't know what a link insert was. One hundred percent didn't care.

(So, the answer is most likely no.)

Dear *2600*:

Does anyone know how to produce a true random number in any programming language? I have been trying for over 20 years but have not achieved it. Every random script that I have ever analyzed can be reverse engineered to predict the outcome, so I'm wondering is it even possible to create a true random number?

DN

From The Algorithm Design Manual*: "Unfortunately, generating random numbers looks a lot easier than it really is. Indeed, it is fundamentally impossible to produce truly random numbers on any deterministic device. John von Neumann said it best: 'Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.' The best we can hope for are pseudo-random numbers, a stream of numbers that appear as if they were generated randomly."*

We probably can't say it any better than that.

Dear *2600*:

How does one stay anonymous and private in 2023? Yes, the mini-computer in my pocket that also makes phone calls is very convenient to entertain me or immediately answer any question I may have, yet isn't it also keeping a record of my thoughts and movements? Can you even get a pager anymore? And when you get paged, how do you call people back? (Keep a phone off and only turn it on when necessary? Then you are still revealing your location once you connect and how do you know the phone is really fully off? Use a stranger's phone? Then they still pick up the location. Also, can't "they" install a secret battery that powers GPS/location tracking without the user

knowing?) Or maybe this is a point where we realize that with Internet-connected cameras and satellites everywhere, there really is no option of staying off-grid. Bigfoot, Loch Ness Monster, and Abominable Snowman all don't exist or else we would have found them already with current technologies. Then again, maybe this is just wishful thinking I see in the movies because criminals still get away with crime. If the technology is open and available, why not let the robots track down every criminal and dissident?

GC

At some point, we need to accept where technology is and figure out ways to manipulate it to our advantage. If we have to jump through hoops just to live our lives, we've already lost. There are always going to be clever ways of subverting the system and of polluting databases with bad and/or inaccurate data.

But we also don't have to always be tied to the devices we're told we need. We get to decide if, when, and whether they're needed. So many of us have a phone on us at all times and are always on call. But there's no law that says anyone has to do this. So why don't we unplug more often? The fear and anxiety we feel whenever we don't have our phones are programmed into us. We can train ourselves to not need most of the devices we're told we can't live without. And when we succeed in doing that, we take back a good degree of control of our lives and take it out of the hands of those who want us to submit, always be available, and constantly have our whereabouts be known.

As for pagers, apparently there are still over two million of them in use in the United States. We suggest visiting pagersdirect.net if you want to go down that road.

Dear *2600*:

Hello, I'd like to submit an article to *2600*. What format do you take and do you have length guidelines?

Karl

We can pretty much handle any format, so send us what you're most comfortable writing in. As for length, the sky's the limit. Our editorial staff would prefer longer, more detailed articles, but that doesn't mean short ones aren't also welcome if they adequately cover the topic they're focusing on. The address to send submissions to is articles@2600.com.

Possibilities

Dear *2600*:

We are reaching you once again as regards the estate of Late George, you were made one of the beneficiaries of his estate. Do get back to me at your earliest convenience.

Trustees

Guys, seriously. You need a proofreader. It's not even the .kr (South Korea) domain. It's everything else. Give the guy a last name; it's highly unlikely his first name was "Late." Don't say "me" when signing in the plural. And this was your first email to us, so why are you saying "once again?" We can help you get this right. We'll continue emailing you until you agree to hire us. Let's get this done before the will is read.

Dear *2600*:

I'm following up to confirm if you are interested in acquiring the registrants/attendees list for Information Security Conference BSidesDayton (Dayton, USA, 19 Nov 2022). Attendees Counts: 1,000. Awaiting your response, so that I can share the cost and additional details.

Iliana
Event Coordinator

In case anyone gets such an email, be assured that BSides is not selling or sharing their attendee lists. This is a scam and it comes from all different official-sounding domains. We're told BSides has even gotten this email for their own conferences with claims of a much higher attendee count than the actual number. There is no shame.

Dear *2600*:

Ahh, what to do, what to do... I found this flash drive on the ground at a gas pump driving down the New York State Thruway. The top was caved in; it had been run over. I took my pocket knife and straightened it out enough to fit into a USB slot. Since I was in a rental car, I figured that plugging it into the radio would be something they wouldn't notice when I returned it, so I did, and it started playing marimba dance music. (There were five videos in the root folder.) But do I dare plug it into a computer?

Dave

It looks like you've replicated exactly what this drive was intended for by using it to play music in your car. But on the off chance there's something more, it's always a good idea to have a cheap laptop somewhere that never connects to any other machines so that you can experiment with drives that literally fall off a vehicle.

Dear *2600*:

I am here representing the sale of the "GetSmartCars.com" domain name for $99 on behalf of our client. The domain name is something I believe will be profitable for your business. If interested, kindly let me know your thoughts. Have a great day ahead.

Emily Jones
Domain Consultant

You put one Smart car on a cover (2005) and you're forever hounded by these people. But we're going to adopt "have a great day ahead" as our standard greeting from now on. At least we got something out of this.

Dear *2600*:

Last night I had a dream that I got to a technical interview, and they gave me an easy problem to solve in Python. But I had to cut my code into a sheet of PVC and make stencils of it. Then I had to make pancake batter out of limited ingredients and with no recipe. The pancake batter was then pressed onto t-shirts with the stencil I had made. I had to bake the shirts and send them to the interviewer by USPS. I had seven minutes.

As someone who is very new to this field, are these realistic interview expectations?

Joshua

This indeed seemed quite realistic until you introduced USPS as a means of quick delivery.

Dear *2600*:

I get frustrated with the whole YouTube thing... I already raised this question with others in the hacker community. It will be nice to avoid YouTube, but I am not asking for that. To avoid loss of history, please sync your videos to Odysee, PeerTube, or even archive.org. There are many reasons, but here are a few:

YouTube/Google etc. own the platform. It is not a public space. It is private and they can and *will* ban you eventually; you should not have to change your personality for anyone, not even YouTube unless you're doing things with a bad intention.

Lots of us in the hacker community try to avoid YouTube and other similar centralized sites. It goes against the hacker ethics of decentralization and openness, which is why we build the fediverse and other open, libre, decentralized tools.

Give options to people; do not close them into a monopoly. I know *Off The Hook* is not because of the MP3 and RSS feeds, but what about the HOPE videos? They used to go to archive.org and we used to show them from there to avoid promoting evil sites like YouTube.

I get that you are frustrated about YouTube issues, but get disappointed that nothing is done. But these tools are already there and made by hackers.

Rek2

***2600* Madrid**

It's great to hear of these developments. We want to see all of the new options test driven by the community to see what works and what's sustainable. We support having our videos pop up on all of them, but we can't commit all the extra time required as we're super busy just creating content in the first place. We suggest people check these out and let's see what develops. We're not sure you're aware that Odysee was acquired by Google, but their site is odysee.com while PeerTube (still independent) can be reached at joinpeertube.org.

Dear *2600*:

There is an app called Instacode that tells you the combination or key code for padlocks. It costs $10 a month. Wouldn't this be a very finite amount of information that could be looked up and kept in a text file?

Peter

It would be a pretty big file and it would have to be updated almost constantly. People who have reason to be doing this sort of thing would likely find the app more convenient.

Dear *2600*:

This transaction is secret to protect my job. I contacted you for a reason, I am a bank manager here in Cambodia and one of my late customers who has the same name as yours. He died ten years ago and left a huge amount of money in his account. Since then no relatives have come to claim his money.... I think we can work this out together for mutual benefit. I will give you more details on hearing from you soon.

smey

This actually came in to our articles email address. Imagine their surprise upon hearing there was someone else out in the world named 2600 Article Submissions. And that this coincidence was enough for them to be able to get that person's fortune.

Dear *2600*:

With all the fuckery going on at Twitter, how likely (or possible) is it that they get completely pwned? Lose control of the site completely? I don't mean it breaking, I mean something like North Korea taking it over.

PXD

Doesn't North Korea have enough problems? And we're not sure how it would be any more managerially unhinged in that scenario than it is already.

Conclusions

Dear *2600*:

Snowden granted Russian citizenship? Sounds good to me. Now that he is Russian, he can be conscripted and sent to Ukraine to become sunflower fertilizer. It'll be the most useful thing he's ever done.

AM

We hope you at least understand that Snowden did not choose to be in Russia. He was stranded there when the United States canceled his passport back in 2013. So if the implication here is that he fled to Russia, it needs to be corrected. Snowden has often said he would willingly face trial in the United States if he could be assured of a fair one. People who want him imprisoned tend to be the only ones who claim to believe this is possible.

Dear *2600*:

Wow. The fact you support Ukraine speaks. Volumes. You're def not you were 20 years ago. Sorry that you aren't.

NB

Please enlighten us as to who we were. Because if we weren't the type of people who stood up for the underdog and fought back against bullies and oppressors, then we probably wouldn't like ourselves very much.

Dear *2600*:

Hacking, to me, has always been about finding a way to get things done. Whether that be thinking outside of the box, pushing items to their physical or virtual limits, or probing and testing to see where weaknesses are... the end goal being "to do what I need it to do, even if it wasn't intended to do that..." and it's not just "things" either. I grow with each experiment/experience. Each failure is just as important as each success. I've seen some pretty hot topics recently that turned into political fights. I just wanna remind everyone that while we don't all agree on everything, we should all strive to see what makes us the same, instead of the differences that drive us apart.

Using myself as an example, if I told you I loved solar power for the freedom it offers, some would paint me as some hippy liberal bent on destroying

fossil fuels. If I told you I owned military vehicles that will happily burn virtually any combustible liquid (gasoline, kerosene, diesel, waste motor oil, etc.), you'd call me some right wing doomsday nutjob hell bent on destroying the environment. Surprise! It's possible to believe in both things.

Point being, we don't have to label everything. It all doesn't have to be a fight. Not everything has to fit into nice little corners with labels and all that. If you really wanna learn about things, ask questions. That's why I'm a huge fan of the Socratic method. Always strive for the truth, and make sure you have citations to back up your data. If you have an opinion not backed up by data, that's fine too, but realize it's just an opinion, and not factually based, and should not be asserted as fact. Just my 3.7 pennies (adjusted for inflation).

Robert T.

Typical logical letter writer, if we're going to assign a label here.

Dear *2600*:

I've been questioned about why I don't use a password manager, pressured to use one, and, heck, even made fun of because I don't use one. I do not use a password manager, and the recent hack of password manager LastPass is one reason why. If you use a password manager and it gets hacked ("experiences a breach"), your account could be compromised and the hacker/s would have *all* passwords you have "linked" with that manager. How is that better/safer than not using a password manager?

Bryan

No matter how good an idea may appear, poor security will quickly negate any advantages. That's why it's always good to ask questions and never believe everything you're told. There's always something that hasn't been thought of. If you can come up with a system that works for you, then don't let anyone talk you into one that you're not comfortable with. Just remain open to new possibilities and ways of improving your security.

Inspiration

Dear *2600*:

Ten years ago I became disabled. I literally used a computer just for the web and maybe a torrent or two. No background in tech. Maybe jailbreaking iPhones or whatever. Out of boredom and the desire to tinker, I installed Gentoo Linux on an old iMac. After distro hopping for years, I settled on Arch. For seven years, I've been using my Btrfs Arch workstation with i3wm to run Debian seedboxes, play with pentesting, and run/network *lots* of containers and VMs. Anyway, last month I put together a resume, just to see what happened. Being a writer, the only credentials I had to list were my handful of published open source and cyber security articles and a strong hacker ethic. Today, I was offered a job as a Linux support engineer with a web hosting company. No degree. No fancy certs. Just a passion for hacking and a near neurodivergent commitment to open source. Job is 100 percent remote and more salary than I've ever reasonably believed I'd be getting. Goodbye Social Security. Hello world.

Joseph

This is a great story of triumph in the face of adversity. We hope it inspires many more.

Meetings Around the World

Dear *2600*:

Hello, I am currently living in Santa Fe, Argentina, CP 3000 and I would like to know if there is a *2600* meeting in my city. Also, I travel frequently to Buenos Aires, so if there is a meeting there, I would like to know where it takes place. Thank you in advance and have a nice day.

P.S. I subscribed to your magazine for the first time last month and I'm delighted with the quality of your job!

Nicolas

Welcome aboard. We've recently added meetings in two districts of Buenos Aires. We don't have any in the Santa Fe area, but you can try and start one by following the guidelines on our meetings page (www.2600.com/meetings) and letting us know. That's how meetings all over the world get started.

Dear *2600*:

I would like to know what days you do your meetings. I live in New York City and I see you have a meeting in the city but I see no time or days.

GM

As stated on our web page, "All meetings occur on the first Friday of each month, starting at 5 pm unless otherwise noted." If there's another place you're seeing a listing without this info, please let us know where that is. We hope you enjoy the meeting!

Dear *2600*:

I showed up for the Seattle meeting at Cafe Allegro this evening, and asked the staff about the meeting. They indicated that the cafe has been closing before 6 for the last couple of years, and there haven't been any meetings at that time at least for the last few months. I don't see a way to contact anyone in the community around here yet. Would you mind checking in with any of the Seattle folks to see if a meeting is happening anywhere else?

cathos

You're not the only one who's pointed this out. The meetings now have a new location.

Dear *2600*:

I was seeking a *2600* meeting near me and found one in my state a bit of a ways away. I was just wondering if you had any points of contact that I could reach out to in order to get more information regarding the meeting. Thank you for your time!

Christopher

We don't give out any personal contact info. But if you go to our meeting list at our website (or look in the back of each issue), you'll see links to Twitter accounts for those meetings that use that service. (We hope to see enough meetings put up their own websites that we can also link to.) That should enable you to reach out to people who know more specifics.

Dear *2600*:

So today was fun.

The past two times here in Stockholm, it's only been me and a friend from work: an infosec expert who's been learning Linux. Our deal was that if no one else came, he could ask me Linux questions.

But today was different.

My regular work friend joined and I managed to bring an old crypto architect from work who said "Oh that old mag, I used to read it back in the day." And another guy who we met at SEC-T also joined. We talked tech and we talked about finding a better meeting place. Then, an hour and a half in, something really unexpected happened: a woman came by who was originally from the New York City *2600* meeting and who has been to meetings in different cities. This was our very first encounter with *2600* visitors from other cities. She gave us a lot of good info on how to find a better meeting spot.

And then, completely by happenstance, the group decided we should form a Signal group chat. This thing is starting to move on its own.

/Psychad

That is truly the magic that can come from the meetings. If you stick with them, inevitably new people will show up and oftentimes travelers who happen to be in town that day. The connections that are made can be priceless and long lasting.

Sheer Stupidity

Dear *2600*:

Gotta love Coinbase, lost access to my old phone number, went to change it. Guess what they do. Automatically text the old number a login code. Went through all of the ID verification and, yup, the account is cleaned out and still tied to the old phone number. Forced two-factor authentication is absolute trash; can we stop doing that?

Taylor

No matter how good a security concept is, it can easily be unraveled by bad policy. This is another shining example.

Dear *2600*:

How to kill a Fortune 500 company's stock in five minutes: Open a verified Twitter account for $8, pretend to be that company, and then tweet something ridiculous.

MP

We think everyone in the world knew that already. Except maybe one person.

Dear *2600*:

Just got a new vacuum at work and found out that management is making us download an app in order to use it because the vacuum does not come with the ability to control itself. I feel as though this crosses a line. I'm just not sure where that line is.

Pjotr

It most definitely crossed the line into absurdity. Why on earth would you need an app to control a vacuum cleaner? It sounds like a fun thing to experiment with, but then someone went and took it way too seriously, making it into the normal method of operating such a device. Of course, you didn't tell us anything about this vacuum, so if it's some kind of robotic device that humans don't actually operate, an app might make a little more sense. But if multiple people have access at the same time, it could quickly devolve into pandemonium. Now that we've thought about it, we think this might be really fun to play with.

Injustice

Dear *2600*:

Hello! My name is Tamara and I'm from Serbia. On Friday, a big Internet scam happened and I, like many others, lost money. We desperately need help. I don't know if this is a stupid thing to try and if I'm even turning to the right address, but hope dies last.

Tamara

It's unlikely that we - or anyone - can do something that helps with the immediate situation. But what we can do is help spread awareness and keep others from being victimized. For that, we need actual details. If knowing those details would have protected you from being scammed, then it's a certainty that sharing them will save others. And we're sure that karma will come back to visit you at some point.

Phone Phun

Dear *2600*:

I admit that I am old school and haven't done much in the way of messing with phones since the days of POTS, payphones being common, and various "colors" of boxes, and I haven't been keeping up with telecom technology and techniques for messing around in the VoIP world. That being said, I have an interest in accurately tracing phone numbers. What's the best way to accurately (if possible) trace phone numbers of scammers, spammers, and just people pulling pranks these days?

Jason

There are as many tricks in getting someone to reveal their true number as there are tricks in keeping it hidden. Caller ID is easily manipulated to display virtually any number the caller desires. Often that will include local numbers to make it seem as if a neighbor is calling. More sophisticated scams involve spoofing a number already known to the called party, which adds a level of believability to the call. In other words, you should never take as gospel anything you see show up on a Caller ID display, landline or cell phone. That said, there are methods of getting true numbers to show up, most of which are because of technical flaws that haven't been discovered. For instance, sometimes a spoofed Caller ID will reveal the actual number when the caller leaves a voicemail message. This also can happen on various follow-me services where a call first goes to one line, then another in an attempt to find the called party. We've seen the spoofed number show up at the first location but the unspoofed one show up at the second. This is likely due to Automatic Number Identification (ANI) being passed along at the point of transfer instead of the Caller ID data. ANI is harder to spoof and tends to be used when calling toll-free numbers of anything where the billing number needs to be known. Caller ID, on the other hand, is only used to identify a number to a subscriber.

Dear *2600*:

In the 1990s, I programmed a game on very expensive (at the time) answering machine equipment that was used for telemarketing. It's an audio adventure where you just point the direction you want to go and hit the * (asterisk) button to do anything in any of the rooms. The objective is laid out when you first log in (call it). Only one person can call it at a time. So, call back later if you do not hear "Welcome to my answering machine." If you get killed in the game, it hangs up on you. The system takes about 30 seconds to reset before someone can connect again. You can call it at 630-847-5241 with any touch tone phone.

Dino

Well, at last, a reason to make phone calls again. This is almost as much fun as our old voice BBS, also from the 1990s, which we have been working on archiving. There are maps available online for this audio adventure game or you can make your own.

Dear *2600*:

Does anyone remember using a safety pin stuck into the wire connecting the handset to a payphone to get a dial tone without a coin? It worked in the early 1960s on rotary phones by touching the pin to the finger stop. The cords back then were just insulated; there was no metal shielding on them.

George

This is similar to the famous WarGames *trick that's demonstrated early in the film where the detached top of a soda can is used to connect the inside of the unscrewed mouthpiece to the phone's keyhole, applying ground to the ring wire, and thereby getting a dialtone. In places where you couldn't unscrew the mouthpiece, sticking a paper clip into one of the holes and touching that to a metallic surface would also do the trick. We're told that many payphones throughout the country had holes in the mouthpiece that looked like something had been crammed into them many times, so it seems likely this remained commonplace for as long as non-dialtone-first phones existed.*

Dear *2600*:

I got a text from PayPal with a code to reset my password, so I called T-Mobile about my SIM card possibly being cloned. The first support lady tried to sell me a new SIM card and charge me an activation fee. I asked to get transferred to tech support. The tech support guy not only put an alert on my account for new IMEIs/phones, but was willing to let me turn off the phone and verify that my E911 information was correct first. I didn't have to do any social engineering or anything - this dude was just super excited to give me the physical location of a SIM card hijacker and deliver some "street justice" (his terms). It seemed like he'd been waiting his whole career for this moment. That's why having one of the most ghetto phone carriers rules.

Zach

We can't argue with that statement.

Experiments

Dear *2600*:

Just now, I made a post on Facebook and included the words Climate Change. The post had nothing to do with climate change. After hitting Post, Facebook showed a pop-up informing me that Facebook will add links to articles about climate change. After posting, another dialog pop-up told me my comments will be posted as soon as they are ready. I'm wondering if this is a new thing. Just never seen this before.

Bob

These little features are typical of social media companies trying to act socially responsible. They can be annoying and are certainly easy to mock and, as you did, falsely trigger. Of course, the real issue is the fact that not only are outright lies and harmful calls to action being posted, but that they're being spread rapidly on these networks. No matter how clumsy the companies' reactions are, the real problem is the poison and venom that's being given life in these environments. Regardless of how we feel about the reactions, let's continue trying to find an effective solution to what they're reacting to.

Oh, and climate change is real, by the way.

Suspicion

Dear *2600*:

I just had an interesting/disturbing thought. I switched Internet service from cable to AT&T fiber a few months ago. Cable throughput per speedtest.net was decent, but the new line is downright spectacular; typically 360 down/350 up and 25-35 ms ping for rated 300 meg service, any time of day or night, local network idle or with a streaming TV or two operating. Impressive, but the speed plus strange consistency got me to wondering: Could AT&T be pulling a VW and optimizing/prioritizing their network to maximize speed tester throughput? Maybe even hijacking the DNS requests and routing to an in-house lookalike server? If they are, is there any way to detect that kind of trickery? Reality check: I doubt they're actually pulling stunts like this. But if they are, and the actual non-speedtest rate is half the rated speed, how would I know?

Richard

You are right to be suspicious, but we doubt they would be able to get away with such shenanigans for long. Everyone has the ability to run different tests and share their results with everyone else. But you touch upon an interesting point regarding speed upgrades. Oftentimes, it's really hard to tell if your speed has actually improved, apart from the higher numbers on the various speed testing sites. This is because you may be running into caps imposed by sites you visit or due to wiring deficiencies in your home or office which result in a weaker signal to some areas and a slower overall speed. A connection is also only as good as the links it follows, so if there are any non-dependable hops along the way, that will adversely affect speed. Our advice is to keep on top of this so you know right away if you're not getting the results you're paying for.

Remembering

Dear *2600*:

Thinking about the old days... there was a year or two in the 90s where BBSes and the Internet

coexisted. In 1995 through 1997, the Internet wasn't yet in most homes so a good way to gain BBS clout was to download files off the Internet and upload them to BBSes. If you noted in the file description that it came from the Internet, it was just that much cooler.

Eddie

Then people began to read the actual content and suddenly BBSes didn't look so bad.

Dear *2600*:

Can anyone tell me how call tracing and *57 worked in the landline days? I remember getting harassing calls and being told they could only be traced if you dialed *57 after the fact. What did *57 do in terms of logging the call that wasn't already happening?

Adam

*This was basically a scam perpetrated by the phone companies. By dialing *57, you would get to pay them $1.50 or so for them to tell you that they had traced the call. You would then have to follow up by filing a police report. You would never find out the number, but they would supposedly contact the calling party to tell them to stop calling you. (It's unclear whether they would be given the number of the person complaining, which would make this doubly insulting.)*

*The phone companies were already making money by selling Caller ID, which allowed numbers to be sent in the first place, and *69, which allowed people to call back unblocked numbers that had called them (for another fee, of course). *57 was designed for those numbers that were blocked, using either all-call blocking or *67 before dialing. Intense lobbying from consumer rights groups kept the phone companies from charging yet another fee to keep your number private.*

What phone companies didn't readily tell consumers was that annoyance call bureaus existed for the sole purpose of tracking down malicious callers effectively and with no charge to the complaining party.

Dear *2600*:

I can still remember file names and complete web addresses from 20 plus years ago and can't remember why I walked into the kitchen....

Paul

In the end, which of those is actually more important?

Privacy Intrusions

Dear *2600*:

Is there any way to protect one's address and privacy from voter registration databases? I am generally good with avoiding junk mail. In fact, I've removed myself from the DMA and other databases and am usually prudent about whom I give my address to. But one loophole I've been unable to plug is the voter registration database - specifically in California. I recently got a handwritten letter begging for my vote from some politician who scraped my address from a database. Then I sent an angry email expressing my annoyance and frustration to said politician and how her intrusive letter actually guaranteed that I'll never vote for her... along with a request to stop doing it. Her solution was for me to stop voting altogether so that my address isn't scraped for marketing purposes. Some questions for ya'll: 1. Excluding a P.O. box, is there anything one can do to prevent this? 2. Where is this open database of voter records located and how does one access it? Is there a link? Thanks.

DM

The rules are different for every state. Some actually allow anyone to download the database free of charge. Others restrict it to state residents. And there are a few that charge exorbitant prices. (For some reason, Alabama charges $37,000 while Florida doesn't charge anything.) Each database is also structured differently, with some including phone numbers and/or email addresses. But it's very hard to avoid having your street address appear to anyone looking through it. Some states restrict the sharing of information of individuals in certain professions, such as police, judges, and people who work for reproductive justice, so it's certainly possible to not have that info be displayed to everyone. But then there are also "enhanced voter records," which are marketed to political campaigns and can include even more personal info, such as religious affiliation and social media profile details.

You are right to be concerned about this. We believe this will become an even bigger issue in the years ahead.

More Feedback From A New HOPE

(Note: Here are a few more letters that contained feedback for A New HOPE and, as per tradition, we thought they might be of interest to readers. Names have been omitted since we didn't explicitly tell writers that their comments might be printed.)

Dear *2600*:

I would like to provide the following feedback for A New HOPE.

Please stop using Zoom. Zoom was also used for HOPE 2020. We are hackers and need to set a good example for everyone in the world and using Zoom does the opposite of that.

Please stop using YouTube. I'm sure everyone on your end is aware that big ol' g00g shut shit down on their end.

Please have a Matrix chat room to engage those in-person, those remotely attending, as well as the others who are financially struggling and could not afford a ticket this year (but have supported *2600* and HOPE financially in the past). It would benefit all of us to help build our community both before and after each HOPE. This is important with everything going on around us today.

A New HOPE Attendee #13

All good suggestions, but all unfortunately are affected by reality. We spent a considerable amount of time working with numerous different programs, apps, and services with the exact goals that you outline. In the end, though, we have no choice but to go with what is most accessible and easiest to use for our attendees. And often, this is not the same as what we would ideally like to use in order to make a statement.

We've been down this road many times. Do we stop using Amazon and not put out a Kindle edition? Do we make a statement against independent bookstores being forced out of business by not supplying Barnes and Noble? Had we taken those higher roads years ago, we indeed would have made a statement, but we wouldn't have survived in order to make any more. And we would find ourselves in a similar place of high virtue but low audience if we stopped using those outlets that everyone else uses. We're not thrilled about it, but it's reality.

But instead of bemoaning this state of affairs, we have the opportunity to reach more people and help inspire them to create tools that can do a better job. While you may believe that those tools already exist, what we found was that they just weren't as easy and intuitive to use for those who aren't really good at this sort of thing. And if we ignore those people, we believe it's a bigger disservice than choosing software that doesn't check all our boxes.

We notice you didn't criticize Matrix which we assume means you approve of it. We have received a lot of positive feedback on that front and believe they are a better fit than something like Discord. We'd love to be able to give out free access to that part of the conference, but we have way too many expenses to make that feasible. We already publish all talks for free online, which is more than what most other conferences do, and much more than what we were able to do in the past.

Dear *2600*:

I stayed on the St. John's campus in a townhouse, and found it perfectly fine for the price and ease and location on campus. The talks were fine, and a few were absolutely outstanding. There were talk overlaps as always, and I await the recorded sessions. Which, after everyone recovers or comes back from a well deserved vacation, will be up for sale or on a thumb drive, if not on the *2600* site or YouTube channel.

Even the hot weather was mitigated by the campus mighty air conditioning units. The onsite Starbucks was fantastic, and the expertise behind the conference to make it run was top notch.

Well done, all!

Maybe next con we could rent electric scooters?

A New HOPE Attendee #14

Thanks for the comments. As we used a couple of different buildings with potential to use even more in the future, the idea of scooters or possibly golf carts to ferry people around has come up.

As mentioned, we were hit by a severe heat wave that weekend, but the university did a great job keeping the insides cool, far better than Hotel Penn ever did. In fact, some people asked us to turn the temperature up a bit!

We had everything up online within a couple of weeks after the conference and better quality non-DRM versions remain available on thumb drives as well.

Dear *2600*:

Thanks for A New Hope! Wanted to say it was great to be back at the con!

A few pieces of feedback:

Track Four was pretty great and I appreciated the announcement post with the calendar over the constant checking of that room in the corner of past cons. Would be great if we could get these into the schedule app so we can get full schedules and notifications like everything else.

I noticed that remote talks were called out well on the paper and app schedules, but *not* on the website which I used when initially planning my time.

There was some great RF content, but did not notice any representation from local clubs. Wondering if anyone does outreach to them as part of the con.

Overall, great con and looking forward to 2024.

A New HOPE Attendee #15

Outreach is always where we fall short. So many people and groups have contacted us after the conference, frustrated that they missed out. We do our very best to get the word out, but the social media giants make it very difficult to go viral.

Remote talks should have been indicated on the website, especially if they were in the printed program. That may have been a software issue which we'll look into.

Dear *2600*:

First, thank you for the awesome conference!

I think next time it would help if we can get a bunch of food trucks somewhere on the campus close to the talk venues. When it was at Hotel Penn, it was very easy to go get a bite and come right back. Here at St. John's, it was quite a walk.

I think food vendors would also make some really good money, so it is a win-win for everyone.

A New HOPE Attendee #16

We agree 100 percent and that's one of the things we'll really push for next time. While there were a lot of really good places a block away, we know that in the middle of a conference, even that can be too far. Now that we've done this once, it's a lot easier to make these suggestions to the university and make the whole event that much more pleasant.

Dear *2600*:

Thank you! Genuinely. Over and over and over. *And,* again, particularly for live streaming and having the Matrix up and running for all of us unable to attend in person.

My first HOPE was The Last HOPE in 2008. My husband (who lives in Canada) and I met at HOPE X, and we've attended in person and virtually since.

We were incredibly looking forward to this year in person, but I got hit with the virus a week prior. My husband decided to stay up north, and even as I tested negative, I chose to play it safe and fully recuperate. It wasn't fun, laying low whilst only a bikeable distance from all the action at St. John's, but walking around the 3D virtual hub, watching and even just listening to fascinating, useful, and entertaining sessions was a boon for my mind and for my recovery (I'm convinced).

Mad respect and appreciation to you all; every volunteer; and the incredible, greater hacker community.

A New HOPE Attendee #17

It means so much to us, as well as everyone who helped make this event happen, to hear stories like this one. If there's anything positive that came out of the past few years, it's the realization that the HOPE crowd is no longer limited to just those who can attend in person. Through Matrix, people are able to attend in a different way and experience much of the same enthusiasm and inspiration that in-person attendees have been doing for decades. And paid virtual attendees have become crucial in keeping the conference and the magazine going. We hope you're able to attend our next event in person, but it's great to know that online attendees are also getting so much out of HOPE.

Dear *2600*:

I had a great time at HOPE and met a bunch of awesome people! Can't wait to see you all again! Hack the planet!!

A New HOPE Attendee #18

We received variations of this sentiment more times than we can print. We couldn't ask for anything more.

Dear *2600*:

Thank you for all the work everyone put into this conference. HOPE has long been my favorite conference, as the people are always friendly and I do not see that cliquey behavior so common at other conferences.

The feedback I have is: I understand venues are challenging and while the campus was lovely, honestly it was the middle of nowhere with limited things to do. Over an hour by public transportation to get to Manhattan for a show was unfortunate and getting to or from a place now had to be a big consideration for planning.

In the July heat, the con at a hotel where you do not need to go outside unless you really want to is a major plus. The weather was horrible.

Again, thank you for the wonderful conference and for everyone's time and efforts!

A New HOPE Attendee #19

We understand the challenges and it sounds like a mixed bag of good and bad for you. We have a few suggestions that might help.

Assuming you're from out of town, we don't suggest trying to pack in too many activities during a HOPE weekend. Going to a show in Manhattan is certainly going to take away from the fun you have at the conference. We had activities going around the clock and there were certainly all kinds of places to go to in the surrounding neighborhoods. We need to do a better job directing people to those places, which is one of our main goals for next time. The venue is most certainly not in "the middle of nowhere" and is considerably livelier than the main parts of other major cities. But at the same time, the campus provides a nice level of insulation for those who just want to focus on the conference.

Obviously, we can't control the weather. But having an entire multilevel building to hold the conference in meant many of us never had to venture outside. But we are looking into ways to make it even easier for those who choose to wander around the campus and surrounding neighborhoods.

Dear *2600*:

Thanks to all - your team, the speakers, the volunteers, the venue, the sponsors, etc. - for a wonderful celebration of all facets of hacker knowledge, culture, and fellowship.

I wish I could have attended in person, but the live streams were an excellent gift to the larger community that could not be present. I really appreciated it and camped out all weekend at my terminal with HOPE in one monitor and work in the other.

So many great topics with variety of content, skill levels, and personalities.

I'm hoping the talks will be posted on the YouTube channel so I can recommend some to peers, others to friends, and rewatch my favorites. Will that be the case?

The only sad part of my feedback is that the YouTube copyright system ruined the hacker movie panel since it kept flagging (then banned) the channel right as we arrived in the early 90s. Wish I could have seen that presentation in its entirety - so much fun, nostalgia, and laughs.

The new venue seemed great and the concluding ceremony was also very fun/interesting.

A New HOPE Attendee #20

As you probably know by now, everything has been posted and we won our appeals to Google. Their paranoia ruined the ability of attendees to go back and view previous talks on that stream during the conference. But it was our fault for allowing them to become the main stream for the conference, a mistake we will not make again. We also used the opportunity to educate many others on these issues and we dare say it made a difference with a bunch of other events. We're glad this hiccup didn't detract from your enjoyment of the event. In the end, they tend to be learning experiences which make us all better informed.

Dear *2600*:

Thanks for a really great event! I'm interested in volunteering next time.

A New HOPE Attendee #21

We've received many similar inquiries and this is really key in keeping the conference successful and growing. It's simply not possible to pull this off without the efforts of our many volunteers. And what's really cool is the fun people have while volunteering and helping to make the conference even better. We look forward to working with you the next time around.

Dear *2600*:

Just wanted to say thank you so much for a great conference. The location was top notch, the team were amazing helping me get set up for my talk, the location for my workshop was perfect - and that's before getting into the rest of it.

Great range of really interesting talks and workshops, everyone was amazing. The whole conference was fantastic.

Was a privilege to be invited to talk and run a workshop and be part of it.

Thank you all so much.

A New HOPE Attendee #22

We really did have such a terrific lineup of speakers and workshop presenters. For the first time, we actually had enough space to accommodate them! And it's great to have access to working resources, everything from audio/visual to network tools. So a big thank you to everyone who played a part in the presentations.

Dear *2600*:

I've been hearing and reading about HOPE since The Last Hope in 2008 and have been wanting to go since then; due to various reasons this was the first time I was able to attend. Being my first time, I feel I should share my opinions on how I felt it went. I know you all probably have a ton of these to read through, so I'll try to keep this down to a simple pros and cons list to keep this short and to the point.

Pros:

- Many good talks, many good speakers, I learned a number of new things.
- COVID protections seemed very well implemented.
- The combination of vax check and masks definitely made HOPE feel a lot safer than other cons I've been to.
- It was great to catch up with old friends and meet new ones.

Cons:

- The hotels chosen were very far from the con.
- I have foot pain issues so this was especially bad for me personally.
- I felt uneasy walking alone in an area of New York City that I didn't know. I have to assume this feeling was amplified for women who also didn't know the area well.
- The venue for the con did not seem like a good fit for our crowd.
- The Christian school and banning of alcohol definitely set a specific tone, and it was not one that I or anyone I spoke with seemed thrilled about.
- There didn't seem to be any good dedicated "hang out" areas to set up laptops and do some impromptu hacking/learning/teaching/experimenting.
- Being central on the campus meant the nearest restaurants were quite a walk to get to.

All in all, I had a great time and learned some new things, but if the next HOPE is scheduled to be at St. Johns, I likely would not come back. I would much rather see the ticket price increase and do a location where everything was close by, we could be ourselves, and we could all enjoy drinks together if we wanted. I understand that more expensive tickets could make the conference inaccessible to some, however things like student discounts could help to resolve these issues.

A New HOPE Attendee #23

We're glad you appreciated the COVID restrictions and we're thrilled that everyone respected them and still managed to have a great time. Unlike many other gatherings at the time, there were no reports of infections related to HOPE. That really was our biggest worry and it was why we put a cap on attendance, even though we really needed a bigger turnout to make the whole thing viable. Being responsible was far more important.

The issues you raise are well worth addressing. The main hotels that were affiliated with HOPE were the closest ones to the venue. But if you stayed on campus, you really couldn't get any closer. We know that not everyone wanted to follow the no alcohol, same sex dorm policy on campus, but that was the tradeoff for staying onsite. If you stayed at the hotels, there were no such restrictions. (Many of our attendees were happy not to have alcohol at the event as it's always caused problems in the past.)

Concerning spaces to hang out, we had more of those this year than ever before. Whether it was at the coffeehouse, the fireside lounge, the place with all of the desks by registration, or the numerous areas in hallways and gathering points, this was probably our biggest gain from our previous space. In fact, there were many outdoor locations with chairs and tables where people had impromptu gatherings after midnight! Space is a wonderful thing to have.

The religious background of the school had no bearing on HOPE whatsoever and we found the staff to be far more open and accommodating to us than Hotel Pennsylvania had ever been. (It was also nice to not be paying Vornado as they helped destroy that part of the city.) Hackers have held conferences at military sites, Communist Party headquarters, and casinos. We can handle an occasional church bell.

The possibility of having a conference at a venue in midtown Manhattan or equivalent is one we explored tirelessly for years after it became clear that Hotel Pennsylvania was no longer an option. For that to work in the few places that have adequate conference space, ticket prices would have to double or triple, assuming we could even get the same number of people to attend. And offering student discounts wouldn't help the situation if they weren't funded somehow. The cost of taking or sharing a brief cab or Uber ride from the hotels near St. John's to the conference would be negligible compared to such a huge price increase.

We miss Manhattan too. But the hacker community is nothing if not flexible and adaptable to change. We managed to create something entirely different when we couldn't meet in person at all in 2020. And we believe this new location for 2022 and beyond has opened a completely unprecedented and unique chapter for all of us. The overall reaction was far more positive than we had hoped for, so we're eager to start working on ways to make this event even better.

Dear *2600*:

To make more money on t-shirts, sell us the brightly colored ones like the volunteers got (bright

blue, purple green) after the conference. There is more to life than black t-shirts.

The workshops and the hacking room were awesome for keeping 17-year-olds entertained and educated. Hurray for lockpicking, soldering, and Arduinos!

Maybe we just missed it: Shout "Enter by Gate 6!!!" in a prep email soon before the conference and put a "Go To Gate 6!!" sign at Gate 1.

In that same prep email, a note that you can park first, and *then* come get the permission yellow form. We were very nervous parking, and wasted time driving around.

There must be some way to get all those musicians onto the stage for the talent show - someone local brings a keyboard and some guitars? The place was literally dripping with musicians....

There must be some solution to "we can't read the slides because you made them tiny to also show the speaker's face on the stream." (Tell everyone to log into talk on computer and zoom in. That's what we finally did. Maybe should have been obvious.)

A New HOPE Attendee #24

All good suggestions. Much of these little frustrations came about because all of this was a first for us as well. We pride ourselves in never making the same mistakes twice. What we need to work on is not making too many new ones.

The way talks were presented on streams was a choice. We don't have to do it that way in the future if another method is preferable.

Dear *2600*:

Thanks for yet another great HOPE! I'm glad HOPE survived the pandemic and the loss of the old Hotel Pennsylvania. It must have required a mammoth effort from the HOPE team. Here's some feedback on A New HOPE:

I liked the St. John's venue! Since the HOPE staff was so conscientious about keeping the talks and Q&A to 50 minutes, there was always plenty of time to walk between buildings and get some sun. I stayed at the Sheraton LaGuardia in Flushing Chinatown, left my car in their reasonably priced garage, and took the bus to/from St. John's most days - two nice walks to bookend the days and a bus tour of everyday life in Queens. This location might be a bit far to make your list of hotel options, but it worked for me. Not every city has a system where busses run reliably every ten minutes; people unfamiliar with New York may be surprised to learn that this is a convenient option.

I became a fan of the "Sup" Thai place on Union Turnpike. At one point in mid-afternoon, I was the first of a series of at least three HOPE attendees to arrive at Sup. We arrived at ten minute intervals and each took up a table. If I had thought of it ahead of time, I would have looked for or started an effort to organize a table-sized group on the conference chat to avoid DOS-ing the restaurant's limited space. This might be something to suggest at the next opening ceremony.

My favorite talks are the ones where the speaker is obviously grateful to have finally found an audience that appreciates whatever peculiar thing it is they like to hack, and they go on to explain some interesting exploration or problem-solving. Sometimes these talks are a useful alert that the cost of the tools needed to play has shrunk to the point where I might consider jumping in. Other times they're simply an opportunity to vicariously enjoy something I'd otherwise never have heard of.

John and Laura Leita's talks on urban exploration at The Fifth HOPE and HOPE Number Six are my go-to examples of this kind of talk. There's no way I'm going to explore an abandoned New York State mental hospital, but they had fun doing it, they were obviously having fun sharing their experience, I had fun listening to them, and everybody at HOPE had fun. I thought many of this year's talks were fun in the same way: Davide Semenzin's talk on book scanning, Joshua Fried's talk on his music-making, Steve Bossert and Joe Cupano's talk on radio experimentation, the Dunin-Jacobs-Schmeh talk on cracking 19th century encrypted ads, and the Peon/Clamp talk on filling in the blanks were some good examples.

I also enjoyed Vlado Vince's talk on Yugoslavian retro-computing; HOPE does good work in keeping the hacker community in touch with its roots. Brandon Roberts' "Hackers Can Help" talk deserves special mention for identifying interesting challenge problems towards which people looking for a project might direct their efforts, work hard, gain some expertise, and ultimately come to a future HOPE and share with everyone.

The hope.net schedule table was excellent; I used it to choose talks on my phone through all three days.

Many thanks, and see you next time!

A New HOPE Attendee #25

Thank you for all of that acknowledgment, particularly for the speakers who really brought so many interesting and unique topics to the audience, not to mention the world through the HOPE archives. (All talks for all HOPEs can be found at youtube.com/channel2600.)

We're glad to hear of another solution for places to stay. This is how others can be guided in the future. As hackers, we sometimes have to think creatively to make something work well and it seems like you did just that.

We hope to do a much better job in the future of guiding people to food places, as this location is right smack in the middle of one of the most ethnically diverse urban areas in the world. We found there to be many great food options on Union Turnpike alone (one block away from the campus) and all of the marvels and late night activities of what many call the biggest Chinatown in the world are only ten minutes away.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Digital Edition Layout and Design
flyko, TheDave

Paper Edition Layout and Design
typ0

Covers
Dabu Ch'wald

PRINTED EDITION CORRESPONDENCE:
2600 Subscription Dept.,
P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

PRINTED EDITION YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate

BACK ISSUES:
Individual issues for 1988-2022 are
$7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2022) available
digitally as annual digests.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept.,
P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

"There's just not that many videos I want to watch." - Steve Chen, co-founder and former Chief Technical Officer of YouTube

"What about Facebook using the system to steer people? We know for a fact all the major Internets do that." - Wyoming State Senator Anthony Bouchard at a debate during his campaign for the U.S. House of Representatives

"The lowest form of popular culture - lack of information, misinformation, disinformation, and a contempt for the truth or the reality of most people's lives - has overrun real journalism." - Carl Bernstein

"I just want to retire before I go senile because if I don't retire before I go senile, then I'll do more damage than good at that point." - Elon Musk

MEETINGS

2600 MEETINGS ARE STEADILY RETURNING. PLEASE CONTINUE TO TAKE PRECAUTIONS WHERE WARRANTED. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aire: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: The HUB, Shibuya Center-Gai. 7 pm

PORTUGAL

Lisbon: Amoreiras Shopping Center, food court next to Portugalia. 7 pm

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid: Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.
Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat and Tricycle, 27-29 W Hill Rd. 6:30 pm
London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Hurts Donut. 2161 E University Dr. 6 pm
Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm
Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes and Noble cafe area, 1599 South East Rd.

Florida

Boca Raton: Barnes and Noble on Glades Rd.
Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.
Titusville: Krystal, 2914 S Washington Ave. 6 pm

Illinois

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Jaffrey: Cafe 532, 79 Hadley Rd. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm
New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.
Rochester (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co. Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Pennsylvania

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell. 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm
Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.
Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm
San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Suite #B. 6 pm

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, *2600* meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle or hashtag so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

NOTE: Please do not come to meetings if you're not vaccinated. This is for your own safety. Proof of vaccination is not required but we hope that common sense prevails.

www.2600.com/meetings

The Back Cover Photos

What's funny here is that we assumed this was the seafood restaurant that grabbed the Twitter handle before we could for our *Off The Hook* radio show. But guess what? There's *another* seafood restaurant in Bethany Beach, Delaware with that name and *they're* the ones with the now seemingly abandoned Twitter handle. It's all good - it's only Twitter - we don't care. Thanks to **murph** for reminding us.

The Back Cover Photos

What a great picture, *also* found by **murph**. It's a little gas station sign in Hope, New Jersey and a great reminder of our upcoming HOPE conference in July. It also reminds us that we didn't get the Hope Twitter handle either. Amazingly, that one appears to be abandoned, too. Again, we're fine. Frustration is what keeps us moving forward, after all.

The Back Cover Photos

You'd think we would have heard of this by now, but there's actually a Hacker beer made in Belgrade, Serbia by Robocraft Brewery and discovered by **Sam Pursglove**. Their web has a description of the character the beer is named after which translates to: "Hacker is a developer who is tired of working for the big corporations that run our lives, and his mission is to decode the industrial matrix in brewing that we are bombarded with by the mass media." Maybe we'll get around to importing it someday.

The Back Cover Photos

Observed somewhere in Wyoming by **Grace McNerney**, who theorizes that "maybe it's the Matrix trying to tell us Wyoming really doesn't exist." That's exactly what they'd want us to believe.

The Back Cover Photos

Yes, this is quite real. Made by the Ferro13 winery in Verona, Italy and discovered by **Patrick Bureau**, we have yet to try it but fully intend to. They also have wines called Nerd, Link, and Hashtag, among others. None of us were in the mood to try and decode the binary, but we'll probably have done it by the time this issue hits the stands.

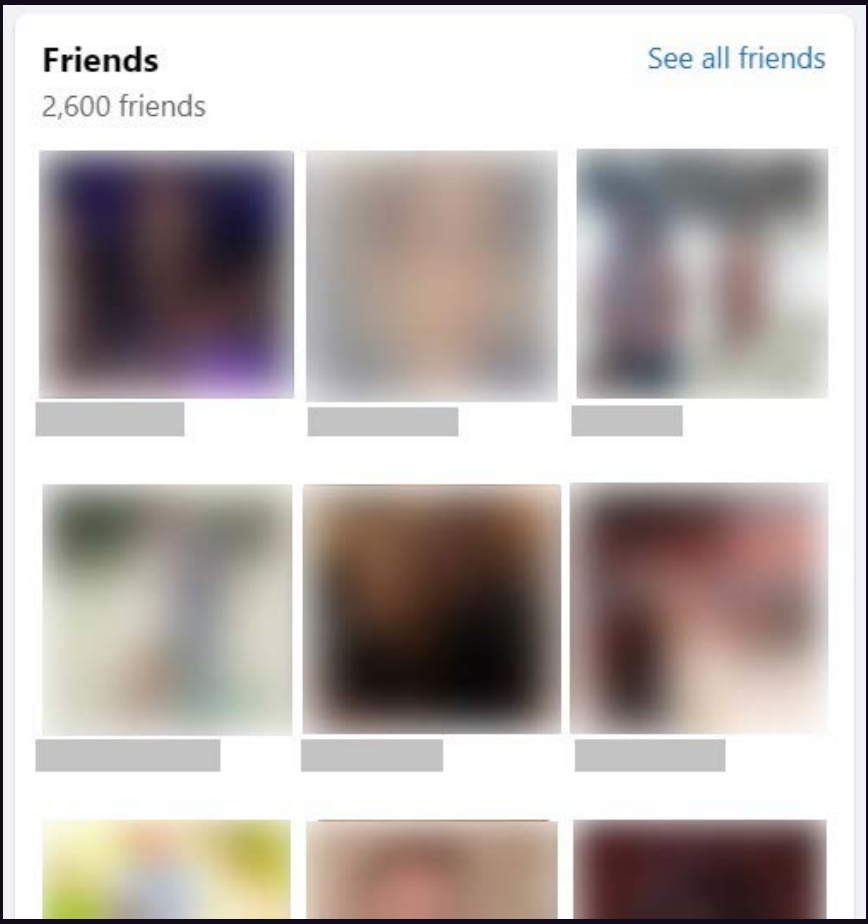
The Back Cover Photos

This was found by **Brandon** on the 2600th step of the Manitou Incline in Manitou, Colorado and it deserves a special mention because it means he had to actually climb that many steps in order to take the picture. (And it's close to the top as there are a total of 2768 steps!)

The Back Cover Photos

We had quite a reaction to the picture of the typewriter repair shop we printed a year ago. **Dan Grebb** found *another* one, also in Pennsylvania! This one is in Lansdale and has been around since 1945 - and hopefully will be much longer. Having "1337" as an address just adds to the magic.

The Back Cover Photos



So this is an accomplishment to be proud of: hitting the 2600 mark in Facebook friends. While **dsttyy** considers most of these people to be acquaintances and not actual friends, it's really all about the number for us. And they swear this wasn't Photoshopped. (And obviously, there's no reason for anyone to ever send us another picture when this exact scenario happens to them.)