

Volume Thirty, Number Four  
Winter 2013-2014, \$6.95 US, \$7.50 CAN

# 2600

The Hacker Quarterly





# Terminated Payphones



**France.** A rather unfortunate reality captured here in Paris, as a bunch of phones, complete with the booths they were housed in, are taken away to be... retired.

*Photo by Nicolas RUFF*



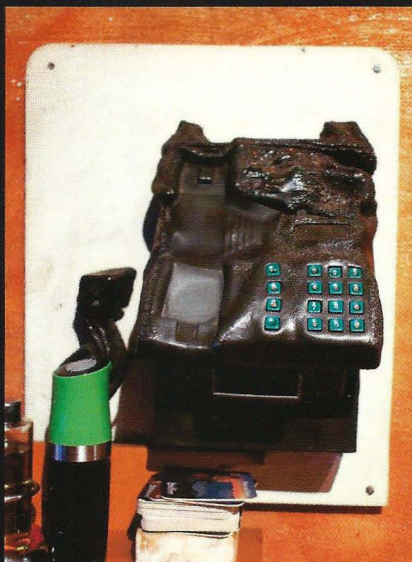
**United States.** And this is how it turns out for many of these unfortunate phones, destined to rot in a scrap heap with piles of junk, as seen in Culver City, California.

*Photo by jeff oconnell*



**Nicaragua.** In other parts of the world, however, abandoned phones are left to die in peace. This way, they're always there as a reminder and a curiosity for future generations. This one was found in El Bluff.

*Photo by Aaron Cotton*



**Germany.** And then there are those places that turn tragedy into something positive, such as here in Lübeck. It seems there was a fire at a local pizza place in the 1970s and they decided to keep the phone in its "altered state" after reopening.

*Photo by Craig Damlo*

Got foreign payphone photos for us? Email them to [payphones@2600.com](mailto:payphones@2600.com). Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)



# Etchings

Dissent or Descent	4
ID3 Tag Messages	6
Privacy - A New Hope Through Tails	8
Fun with the Minuteman III Weapon System - Part Two	11
TELECOM INFORMER	13
The Many Vulnerabilities of Verity Parental Control	15
Anonymity and You, Firefox 17 Edition	17
Identity and Encryption Verification	18
Wi-Fi Security: Attack and Defense	19
The Maturation Cycle of a Hacker	24
There is <i>Never</i> a Free Lunch	25
HACKER PERSPECTIVE	26
CYA Using a Pi to Pivot	29
Pretty Good Privacy	30
Hacking Your Mother Tongue to Obfuscate your Encryption	32
LETTERS	34
The Growing Schism Between Hackers and the Law	48
Netcam: Basics and Vulnerabilities	50
TRANSMISSIONS	52
All I Want is Total Freedom	54
Fiction: Hacking the Naked Princess 7-9	55
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66



# DISSENT OR DESCENT

This is the choice we face that has never seemed clearer. Do we allow so much that we value and that we've fought for over decades, even centuries, to be dismantled out of apathy, fear, or convenience? Or do we take a stand and fight back, knowing that any time we do such a thing, there are risks of one sort or another involved?

It shouldn't be too hard to predict which choice we would opt for. But choices only remain correct if they're revisited, analyzed, even second-guessed to a point. It's not enough to simply stand up for something because it's what we've always done. We have to know why.

The NSA revelations that continue to come out on a somewhat timed basis are the worst possible nightmare for those who embrace state secrets. But for those who believe in full disclosure and have never subscribed to the notion of "just trust us" by *anyone* in authority, these are the brightest days imaginable. What Edward Snowden has done is turn the intrusive gaze of the National Security Agency 180 degrees and allowed us to see what they do and what they want. We find that, at some point, there comes a revelation that offends each of us, even the NSA's staunchest supporters. When all is finally revealed, however long *that* will take, we believe there will have been very decisive and radical changes in intelligence gathering, both here and abroad.

Consider the fact that relatively few of us are bothered by the existence of spy agencies in the first place. People tend to accept them as a necessary evil and, as long as they feel safe and don't believe their privacy is being violated excessively, these agencies pretty much get carte blanche to do as they please. Even with the initial Snowden revelations, a sizable number of Americans were willing to overlook having their own privacy invaded a bit, so long as it was all in the interests of security and they didn't feel like *they* were actually being targeted. What's a little more private info being given out in this day and age when we're constantly advertising our location and innermost thoughts to the world via social networking?

We've seen this attitude steadily begin to crumble, as the scope of the surveillance becomes better known. Ironically, some of the harshest criticism has come from those in governments who came to realize that the NSA's unblinking eye has had them in its sights for years. Oddly enough, this is precisely what agencies like the NSA are *supposed* to be all about: gathering intelligence on leaders of other countries, even friendly ones. But when it was revealed that Chancellor Angela Merkel's cell phone had been tapped since 2002, the German government was outraged, and so were leaders throughout the world. There were even hints that Snowden would be welcome in Germany to presumably reveal more such details, an abrupt reversal of the unquestioning allegiance they - along with much of the world - have shown towards the United States in their desire to make him a fugitive with nowhere to go. Similar revelations have come out concerning the leaders of Mexico and Brazil, along with more than 30 other heads of state throughout the world. It seems everyone has a breaking point when it comes to their own privacy, even and especially those who routinely violate that of others.

But even though this is what many of the headlines focused upon, this is not where the true story lies. The real issue here is with the insanely thorough and ever-expanding spying being perpetrated against the average citizens of the world. Consider:

- The NSA stores metadata from half a billion telephone calls, emails, and text messages in Germany alone every month.
- In direct violation of the law, France has been revealed to have been intercepting and storing most of that nation's internal Internet and phone communications for years. The NSA is said to have obtained over 70 million phone records on French citizens in a single 30 day period.
- The "Fairview" program is being used by the NSA to spy on the communications of Brazilian citizens.
- Direct access to monitor communications lines has been given to the British spy agency GCHQ (Government Communi-



cations Headquarters) by Verizon, Vodafone, and BT.

- The NSA has cracked numerous forms of encryption used by private citizens and is planting back doors into consumer products with the help of the tech industry, often through the use of malware and outright theft of keys.
- Most major smartphones are now able to be tapped into by the NSA. These devices contain a world of information on many of us, from our personal correspondence to where we happen to be at any moment. We help make this form of surveillance possible because we want the convenience offered by this technology.
- Google and Yahoo have had their unencrypted data center communications intercepted by the NSA, allowing almost full access to whatever these companies store in "the cloud" on our behalf.

We could go on; there are many more revelations, but the point has been made. Everyone is affected at some point. And everyone should feel violated.

While we share in the outrage, we don't share in the surprise. As we put this issue to press, we're also digitizing Volume Three of our *Hacker Digest* series, comprised of our publications from 1986. What's interesting is that even back then in these very pages, people were concerned about what the NSA was doing and what they had access to. Before the Internet was even born, those who were paying attention could see the looming threat. There was discussion of the fact that warrants weren't needed for phone line monitors known as "pen registers," devices that simply collected the numbers that were being dialed on any line that was being watched, unlike an actual phone tap. This was the metadata of the time and the concern was that this information provided anyone watching with a pretty accurate assessment of who the target spoke to without any actual legal oversight. We are seeing the same concerns now being addressed with regard to the metadata in emails, and how thoroughly that information can paint a picture of who somebody talks to and where their interests lie. Over the years, these concerns haven't changed, but the technology and capabilities certainly have.

Through time, we also occasionally come to accept things that were once thought of as intrusions. An example we see from looking at

our earlier material centers on the initial suspicion that Caller ID was viewed with. Having one's phone number transmitted to the called party seemed an unacceptable sacrifice of anonymity. At first, phone companies resisted installing an option to block the number transmission and allow the caller to remain anonymous, but the prevailing concern of the time made this an essential part of the new technology. Today, we accept the fact that we share our phone numbers when we make calls, and relatively few people opt for the anonymous option. It makes things so much more convenient, after all. But while our perceptions may have changed, this doesn't mean that the initial concerns weren't valid and aren't still to this day. Consider that at the time we were discussing these issues back then, we were also amazed that in parts of Europe, it was considered a privacy violation for the phone company to even keep *any* record of who called whom. It was very difficult for us to understand this, as call records were something we were very used to and we saw it on our bills every month. But many in Europe knew all too well that this information in the hands of an evil government could easily be used to round up people based on their affiliations. Again, metadata being implemented as a means of intelligence gathering. And while we may believe we've advanced beyond certain depravities, history always seems to come back and haunt us. Whatever technological advancements we embrace will be used for good, but also inevitably for evil. And, unless a part of those advancements also includes some sort of defense against this, we will find ourselves more the victims of technology than its beneficiaries.

So the choice lies with all of us. Do we blindly trust those who have acted so deceitfully and sink ever more deeply into an Orwellian world of total surveillance? Or do we dissent and establish some boundaries as to what's acceptable and what is clearly not?

It's the citizens of the world, especially those in the United States, who can have a decisive role in what sort of authority we give agencies like the NSA. We don't agree with the overreaching power they have taken for themselves, we never agreed in the past, and we surely won't in the years ahead. Expressing this sentiment vocally is the only way to make such feelings relevant.



# ID3 TAG MESSAGES

by Donald Blake

Here's a riddle. What's the most annoying type of specification for a developer and the best type of specification for a hacker? Answer: An informal specification. It's difficult for the developer because they have to write code that matches the specification and they have to provide enough leeway in their code so that when it's reading a file that somewhat uses the informal specification it can still read it. However, it's great for a hacker because they can decide what parts of the specification they want to use and throw as much of it away as they want and their application will still follow the specification.

This is why informal specifications are great vehicles for secret messages. There are three traits to a secret message that make it a great message.

1. *Existence.* No one knows about it except for the sender and receiver.
2. *Readability.* No one can read it except the sender and receiver.
3. *Transportation.* One that is easily transmitted, received, and destroyed.

This is why ID3 tags are awesome for secret messages. The sizes of MP3 libraries are enormous. My collection is around 20 gigabytes, so have fun going through it looking for secret messages. You need a program to be able to read the ID3 tags or have an extremely keen eye. If the ID3 tag is messed up, the MP3 will still work and MP3s are everywhere. It's the standard media for listening to music today and it's growing. Another added benefit of ID3 tags is they can carry any type of data.

ID3 tags are used to hold the informational data about the MP3 file. The standard can be found at <http://id3.org/>. There have been some revisions to the standard over time. I'm just going to go over the two most popular ones: ID3v1 and ID3v2. ID3v1 is located at the end of the MP3 and it's the easiest one to work with because it doesn't provide very much leeway. It has to be in total length 128 bytes long, must start with the word "TAG", only has nine fields and each field has a defined set length. And as a developer, I love this form.

```
ID3v2/file identifier  "ID3"
ID3v2 version         $03 00
ID3v2 flags            %abc00000
ID3v2 size             4 * %0xxxxxxx
```

Figure 1 ID3v1

Source: <http://en.wikipedia.org/wiki>

→/ID3#ID3v1

As a hacker, I'd rather work with ID3v2 or greater. ID3v2 tag frames should be no larger than 16MB each and the total length of the tag should not exceed 256MB. They start at the beginning of the MP3 file and each ID3v2 or greater starts with a header. The header should be ten bytes long. The first three bytes are "ID3", then the version which is two bytes, a byte for flags, followed by four bytes for the size.

Figure 2 ID3v2 Header Layout (below)

Source: <http://id3.org/id3v2.3.0>

Within each ID3v2 tag there are frames that hold the specific information for the MP3 file, such as the title of the song and/or band name. These frames shouldn't be any larger than

Example  
MP3 Header



Colour-coding shows binary bit mapping to hex values below

Detail of an  
MP3 Header

Bits	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	
Binary	1	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	
Hex	F	F	F	F	F	F	F	F	0	0	0	0	0	0	0	0	0	0	0	0	
Meaning	MP3 Sync Word			Version	Layer	Error Protection		Bit Rate		Frequency		Pad. Bit	This Bit		Mode		Mode Extension (Used With Joint Stereo)		Copy	Original	Emphasis
Value	Sync Word			1 = MPEG 2.5 = Layer 3	1 = No	320 = 320		00 = 44100 Hz		0 = Frame is not padded		Unknown	0 = Joint Stereo		0 = Intensity Stereo Off	0 = MS Stereo Off	0 = Not Copy-righted	0 = Copy Of Original Media	00 = None		



16MB each. Each frame header is also ten bytes long. They start with a four byte frame name, four bytes for the size, and two bytes for flags.

Frame ID	\$xx xx xx xx (four characters)
Size	\$xx xx xx xx
Flags	\$xx xx

Figure 3 ID3v2 Frame Layout  
Source: <http://id3.org/id3v2.3.0>

The best way to understand what these things look like is to open any MP3 file in a hex editor and you'll see exactly what I'm talking about. Just look for the word "ID3" and any of the 100+ declared tag names defined in Section 4 on <http://id3.org/id3v2.3.0>. Some popular ones are the title "TIT1" and album art "APIC" frames. Another cool feature of the specification states that there can be more than one instance of a specific frame.

It's important to realize that an ID3 tag or any data that precedes or ends after the MP3 header and data is not needed to play the MP3 file. An MP3 player will play any file as long as it has valid MPEG-1 data within that file. MPEG-1 data always has a header and then data after it and these repeat for the rest of the file. The first 13 bits that are all set to one in a row is the header of the MPEG-1 data. This header includes all the data that the MP3 player will need to play the data such as version, bit rate, frequency, and many other fields. I included a layout of what an MPEG-1 header looks like, but you can find more information on it at Wikipedia [http://en.wikipedia.org/wiki/MPEG-1\\_Audio\\_Layer\\_3](http://en.wikipedia.org/wiki/MPEG-1_Audio_Layer_3). The MPEG data usually starts right after the ID3v2 tag. So as long as we don't mess with the MPEG-1 data, our MP3 file will still play and it gives us plenty of space and leeway to hide a secret message.

Figure 4 MP3 header (below)  
Source: [http://en.wikipedia.org/wiki/MPEG-1\\_Audio\\_Layer\\_3](http://en.wikipedia.org/wiki/MPEG-1_Audio_Layer_3)

Field	Length	Description
header	3	"TAG"
title	30	30 characters of the title
artist	30	30 characters of the artist name
album	30	30 characters of the album name
year	4	A four-digit year
comment	28[3] or 30	The comment.
zero-byte[3]	1	If a track number is stored, this byte contains a binary 0.
track[3]	1	The number of the track on the album, or 0. Invalid, if previous byte is not a binary 0.
genre	1	Index in a list of genres, or 255

There are a lot of MP3s and MP3 players out there. MP3s are copied and recopied over and over and people have a tendency to change the ID3 data in their MP3 files and the ID3 tag gets rewritten. Plus, every MP3 player implements the ID3 "Informal Standard" differently. Depending on which MP3 player you use, it may not care about all the tags that are defined in the ID3v2 standard because normally it only shows maybe a dozen of these tags and the rest get ignored. Depending on the MP3 player, it may not care about the size and flags in the ID3 tag header frame simply because it can't display the whole contents of that frame because of design restrictions. If that frame is rewritten, it may not care about what was there before. This is fine from a listening standpoint because the MP3 player will only play the MPEG-1 data and the rest of the file is just informational. Therefore, ID3 tags are usually a mess. Which means a secret message would hide very well among the garbage that is included in most ID3 tags.

We could copy our message into an MP3 file while keeping the MPEG-1 data intact and forget about the ID3 tag. The only problem with this idea is that if our MP3 song is only four minutes long and the file is 20MB large, it's going to look a little funny. If it doesn't have any ID3 tag, it will look funny too. So to avoid our message from being detected, we need to make it look like an ordinary everyday MP3 file.

Since MP3 players can be selective about what they read before and after the MPEG-1 data and the file can be as big as we want it to be and ID3 is an informal standard, we can create our own ID3 frame. Since there are over a hundred different defined ID3v2 frames this makes it easy for our own defined frame to hide out among the real ID3 frames. The size and flag data of the ID3 frames aren't always correct and, as long as we start with four characters followed by six bytes of data, we can make



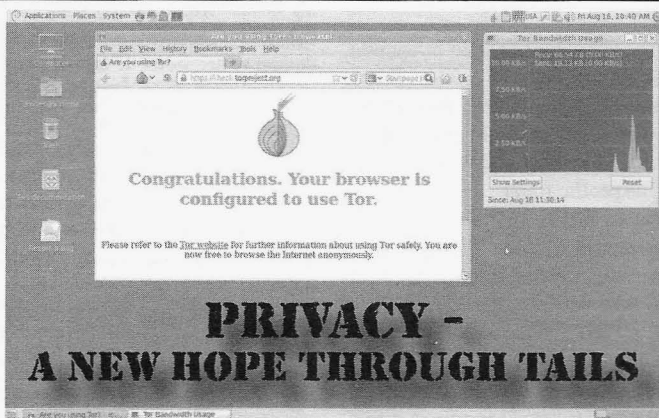
our frame look like an ordinary ID3 frame and use the other six bytes of data for whatever we want. We could do something cool like use it for an encryption layout. Or maybe we're lazy and just want to use one of the preexisting ID3 frames that go along with what we're doing. We would still be able to hide our message pretty well. Since MP3s are relatively small we can break up our message over a number of different MP3s, thus hiding our message even further. We could even define a decoding order

and make another ID3 frame to specify just that information. We can also use a song that drives most people crazy for another layer of security. The possibilities and complexity are endless.

This is why MP3s make the perfect place to hide secret messages. It's interesting that ID3's motto is "Audience is Informed." More than they realize.

Thanks for reading.

*Shout out to Violet.*



by Brainwaste

*"The evils of tyranny are rarely seen but by him who resist it." - John Hay*

In this era of new totalitarianism, state sponsored surveillance, and with what the government and ISPs can do legally (and illegally) to spy on you these days, it makes sense to protect your computer data and communications. We all want to avoid the prying eyes of intrusive data surveillance programs. You have probably heard about the NSA surveillance program PRISM, which has openly been used to conduct illegal spying on U.S. citizens. And with the recent attempt by the FBI to pressure Internet providers to install surveillance software that can intercept metadata in real-time, who knows where the abuses will end? The FBI and other federal authorities are used by those in power as a political weapon against hackers and those who embrace a free thinking ideology. Apple, Google, and Microsoft are all part of PRISM, so I strongly recommend avoiding their proprietary operating systems. Chrome, Internet Explorer, and Safari are not recommended. Instead, you should use Mozilla Firefox or the

Tor Browser Bundle.

There are a lot of sick dudes out there. There are a lot of real sick motherfuckers going around debating which is a better computer operating system for protecting your online privacy: Linux or Window\$. Hopefully, this article will put the debate to rest. Risk is a variable in any activity, but the objective here is to limit our vulnerability. The goal here is to work on a computer while limiting the risk of exposing our credentials and private data, as well as being anonymous.

So how can we achieve all this? By having a separate operating system which is used solely for sensitive computing. Why is the operating system important? Because virtually all of the data-stealing malware in circulation in the wild today is built to attack Windoze\$ systems, and will not run on non-Window\$ computers. For security purposes, almost any Linux OS is superior to Winblow\$, but a general purpose Linux distro does not make an ideal solution for security, and security hardening a general purpose Linux distro requires skills that most people don't have. So the solution here is to use a Linux Live CD distribution. The beauty

of Linux Live CD distributions is that they can turn a Windoze-based PC temporarily into a Linux computer, as Live CDs allow the user to boot into a Linux operating system without installing anything to the hard drive.

Programs on a Live CD are loaded into system memory, and any changes - such as browsing history or other activity - are completely wiped away after the machine is shut down. To return to Winblow\$, simply remove the Live CD from the drive and reboot. Thus, malware that is designed to steal data from a Window\$-based system will not load or work when the user is booting from a Live CD. Even if the Windoze\$ OS on the underlying hard drive is totally infected with a virus or Trojan, the malware cannot capture any information when booting with a Linux LiveCD this way.

The main reason to use a bootable Live CD is it's not persistent, unlike a hard drive install or a persistent bootable USB flash drive, offering the most security and privacy because absolutely nothing remains when the CD is shut down. Although a persistent install of Linux is better because it's a more secure OS, using a non-persistent system is the best because not even your browsing history will be saved when the system is shut down. Absolutely nothing is saved when it is shut down, not even apps you have installed. Linux never stores as much information as Windows and a Live CD stores even less. Even if you have Linux installed to the hard drive, using a Live CD or a non-persistent USB Linux bootable distro would give you the best protection of all. If your PC can be booted off a USB thumb drive, it is also possible to put the Live Linux distribution on a USB thumb drive, eliminating the need for a CD. Most distros have an option to create a bootable USB thumb drive. The advantage is that a bootable USB stick is faster than a CD.

A bootable Live Linux USB thumb drive can be very effective for security, but there are important differences in implementation one should be aware of. Bootable USBs come in two flavors: persistent and non-persistent. Thumb drives made with persistence means the software can be modified and changes occurring in one session will carry forward to the next. For security, persistence is undesirable because an attack in one session can corrupt actions taken in subsequent user sessions, compromising system integrity. Further, off-the-shelf Linux distros like Ubuntu and Linux Mint are

not designed for security. They are designed to be general purpose OSes with extra packages included for email, office productivity, multimedia, photo editing, and Flash which are all known to be vulnerable to attack. These packages increase the attack surface of the device, making it undesirable for security. Also, the typical OTS Linux distro is designed to boot with all ports open and local networking open by default. This is a major security vulnerability because it makes the system vulnerable to attack by other infected machines on the same LAN.

There are three basic types of threats to your data: 1) Data that is stored on your computer; 2) Data on the wire - your data that is transmitted over/on the Internet; and 3) Data that is stored by third parties like your Internet service provider and by the sites that you visit. VPNs and web proxies are a joke as they both do not provide any real online privacy protection. To save our online privacy, we cannot woo false Gods or evoke half measures.

All is not lost, as there exists a new hope to protect and preserve our online privacy and anonymity. And that is Tails: The Amnesic Incognito Live System. Tails is a Debian Live CD/USB/SDHC flash card for almost any x86/x64 system. Tails neutralizes all of the above types of threats to your data. Tails can be run on most computers independently of whatever the installed operating system is and is perfect for conducting sensitive activities from untrusted computers without leaving a local record of your surfing activities.

First of all, Tails is designed out-of-the box to be non-persistent, meaning every boot creates a separate yet exactly identical working environment. It is purpose-built for the task of privacy and uses a small fingerprint to minimize its attack surface. Tails boots up fast and the boot menu offers the user a choice of eleven languages for use on the system. Once Tails has booted, Tor automatically launches itself. All network traffic is routed through Tor, so you will be able to surf the Internet and access websites even behind the most restrictive firewalls. It is impossible for applications to connect to the Internet with your real IP. Thus, Tails is perfect for those who want to bypass Internet censorship imposed by corrupt governments whose internal politics repress freedom. I2P traffic is routed through Tor so you can browse websites with a proxy IP without any configuration. You can visit .i2p websites not accessible from the regular Internet. The user is provided with



Vidalia as a GUI for Tor and Firefox as a web browser. Flash and many other options which make it easy to track your IP address or load code are turned off by default. Firefox comes with a bunch of privacy add-ons like HTTPS Everywhere, Adblock Plus, Cookie Monster, FoxyProxy Standard, and NoScript. All cookies are treated as session cookies by default. The CS Lite extension provides more fine-tuned cookie control for those who want it. These add-ons give you real privacy protection: encryption, protection from tracking cookies, script prevention, etc. Further, Linux stores lasting configuration and cache data in "dotfiles" in the home directory (just files or directories whose names start with a period), but these files are not stored in the Tails Live CD. No trace is left on local storage devices unless explicitly asked.

Tails comes with a "camouflage option" which makes the default Gnome desktop look like Windows XP. I always use this option, as no one will suspect what I am doing. If any Geheime Staatspolizei types happen to be shoulder surfing on my activities, the XP desktop allays their suspicions. Tails comes with aircrack-ng, a non-graphical tool for checking the security of your Wi-Fi network.

Tails also can be used in "safe" environment mode. The user is provided with all the necessary software to view/edit files: OpenOffice, Audacity, GIMP, and more are all included in the distro. With these you are able to edit office files, watch videos, record sounds... all without leaving any trace of your activities on the physical computer. The default file manager to navigate through your folders is Nautilus. The Nautilus file manager has been installed with extensions for securely wiping files. You can delete files and be sure that no one can recover them. A simple right-click on a file, and then "Wipe" will do the trick. The file will be erased and the space written over with random data so as to make data recovery impossible. You can create a persistent storage volume on a Tails USB with `Tails > Configure Persistent Volume`, and delete it just as easily with `Tails > Delete Persistent Volume`.

A copy-paste manager and a virtual keyboard are two programs in the System Tray. The virtual keyboard is very useful in case the computer you are working on physically records what you are typing with a keystroke logger. The copy-paste manager is useful, but if you forget to erase it at the end of your session,

it does present a security risk: it might contain email addresses, URLs, passwords, and any information that was copied into the clipboard can be accessed. Network Manager for easy network configuration, Simple Scan, and SANE for scanner support, as well as Shamir's Secret Sharing for encryption are all included.

I also use Tails for secure communications. The IM/chat client Pidgin comes by default with the "Off The Record" plug-in which encrypts your messages. I also use the Claws Mail email client with OpenPGP encryption. In addition, Tails can be used for the encryption of physical drives and folders with the program TrueCrypt for a LUKS encryption. I understand that the developer is working on including a MAC changer program, but that it is not currently operational.

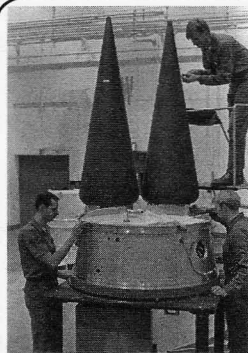
Cold boot attacks are also defeated. When you shut down your computer, the RAM will take several minutes to completely erase its contents. A cold boot attack is when someone makes use of this delay to recover all of the contents of RAM, which translates to almost everything you've done during your session. Tails automatically wipes and fills RAM with random data at the end of your session.

I have also used Tails on an SD memory card which I can use on many different laptops, as some laptops and netbooks don't have optical drives. If you do decide to use Tails on a laptop, I'd urge you to plug the notebook into a router via a networking cable, as opposed to trying to access the Web with the Live CD using a wireless connection. Networking a laptop on a wireless connection while using a Live CD distribution may be easy if you are not on an encrypted (WEP or WEP/WPA2) wireless network, but attempting to do this on an encrypted network is not for the Linux newbie.

So the Tails setup contains absolutely no personal information or files, and no software installed on it or services that are accessed from it can be tracked back to any one specific individual or organization. In the United Surveillance States, Big Brother knows *everything*. But not if you are using Tails.

### Links

<https://tails.boum.org> - Tails 0.21  
<http://cryptome.org/2013/07/nsa-tracking/nsa-tracking.htm> - Some details of NSA email and phone tracking programs



# Fun with the Minuteman III Weapon System - Part Two

## Intercepting Basic Nuclear Missile Communications

by Bad Bobby's Basement Bandits

Welcome to Part Two of fun with an active Minuteman III nuclear weapon system. In Part One, we examined how to activate one of the Minuteman III security system alarms, how a basic security strike team responds to the alarm, what you need to do to avoid dealing with the strike team, and how multiple alarms might be fun to observe!

I have received some feedback from Part One. The majority of feedback came from active and retired Minuteman III operators and maintainers. The active crewdogs were not that impressed with being able to throw snowballs and ice cubes to activate a security situation on a Minuteman III launch facility. However, most of them do not recognize the concept of hacking when it relates to having a hacker with no knowledge of an active Minuteman III system as new hackers begin to discover ways to interact with the system. This, of course, is the purest essence of hacking: taking an unknown system and discovering ways to make it known. As always, the contents of this article are completely unclassified.

First, a little bit on social engineering. The Minuteman III Intercontinental Ballistic Missile System is one part of the nuclear triad. The other two parts are nuclear bombers and nuclear missile submarines. Both the bomber crews and submarine crews receive extra pay for performing their nuclear mission. Your friendly neighborhood Minuteman III crewdogs receive no extra pay for performing their nuclear mission. I find this quite humorous, and see this as another weak link in the Minuteman III nuclear chain. If I were a representative of China or Russia, I would be sorely tempted to offer a Minuteman III crewdog some extra cash. Most of the Minuteman III crewdogs could not be tempted with extra cash but, sooner or later,

China or Russia would find the one crewdog who might need the cash.

To further weaken this third leg of a nuclear triad, the Minuteman III crewdog career field has been in a nearly complete state of disorder. Many of these guys don't know if they will be coded 13S or 13N until they're nearly through with their crew tour. These different job codes determine whether or not Minuteman III crewdogs will have a job in the space or nuclear career field, or whether they'll have to exit the Air Force. Clearly, the situation with the Minuteman III crew force is ripe for someone to employ social engineering techniques to discover what they will. Obviously, after printing this article things will tighten up for a while. But... the system is built on a dinosaur mentality and its equilibrium will shortly be restored to no extra pay and career uncertainty. Okay, enough social engineering for today!

Today we will be examining how to intercept Minuteman III ICBM communications. We will start with the basic level of communications. What communication system does a Minuteman III crewdog use when in route between the main base and their missile site? Minuteman III crewdogs depart the main base using one of two modes of transportation: either by vehicle or by helicopter. The majority of Minuteman III crewdogs depart the main base by vehicle, and this will be the focus of our discussion. These crew vehicles contain a radio that allows the crewdogs to communicate with the main base or the missile site. The transportation center mainly communicates with crewdogs on their way out to their missile site. Most of the time the drive is long and boring and the transportation center communications are tedious. Some crewdogs will unplug the microphone from the radio and then alternately touch it and remove it from the radio while communicating with the transportation center. The crewdogs' message



will be garbled and will allow them to tell the transportation center that their radio system is inoperable. This now gives them a free ride out to the missile site without having to deal with making stupid radio calls. Crewdogs leave the radio on so that they can monitor radio chatter. A hacker might say this is no big deal. So what if crewdogs hate using the radio?

Ahhhhh! This is where the fun comes in. Any person who lives in the area of our Minuteman III missile sites has witnessed crew vehicles and maintenance vehicles driving out to the various sites. Many people have CB radios in their vehicles and have probably noticed that they have never been able to pick up any radio communications originating from the crew vehicles and maintenance vehicles. This is because the crew vehicles and maintenance vehicles' communication systems consist of VHF radios and various repeaters across the landscape. Those people who own boats will immediately recognize and understand what VHF radios are used for. A short glance at FCC regulations will show that VHF radios are to be used by the civilian population only on boats and only when those boats are in the water. I can go into the technical details for this, and it would be long and boring. Most of you wouldn't want to know it anyway. Suffice it to say that many military, government, and law enforcement agencies use VHF communications on land. I think the bottom line is they don't want civilians clogging up their VHF radio network. If I had a VHF radio on land near Minuteman III missile sites, I would probably turn it on and listen to the radio chatter. I'm sure I would never transmit any message over a VHF radio while I was on land. You'd be surprised what you could learn from listening to your VHF radio. You would hear something like this:

*Crewdog: "Transportation center, this is trip 9-1 now arriving Charlie-1 request time and initials."*

*Transportation center: "9-1 acknowledged now arriving Charlie-1. 1800. Romeo Delta Sierra."*

This little communication between trip 9-1 and the transportation center is a good example of the type of VHF communication made by Minuteman III crewdogs and maintenance crews. If you are actually observing this crew vehicle, you would see that it pulled onto the access road to Charlie-1. It has not yet begun to try to enter the site. You can see that trip 9-1 is maintaining very good radio discipline by

only sticking to the business at hand. No one's asking about the guy's kids or how his sick aunt is doing or any of the normal types of day-to-day conversation. The next communication would go something like this:

*Crew vehicle: "Charlie-1 Security, this is trip 9-1 at your gate. Request permission to enter site."*

*Charlie-1 Security: "Roger that 9-1. Stand by while I verify your trip information and notify the site Commander."*

*Pause.*

*Charlie-1 Security: "Okay trip 9-1, you're cleared for entry on-site. Verify vehicle and weapons are secure."*

*Crew vehicle: "Charlie-1 Security, vehicle and weapons are secure. Please notify the facility manager to assist us in unloading the vehicle."*

As you can see from these two communication examples, they follow a very tight script. For the most part, every crew vehicle and every security check tends to go the same way. That, my friends, is the big deal! Think about when you were first learning to hack. When you turned on your computer, the operating system tended to show the same messages in the same way every single time. You know that after a while you began to examine every single message and learned exactly what they meant. What you began looking for were exceptions to the startup messages. You learned that those exceptions provided you an opportunity to tweak and change them to see what happened.

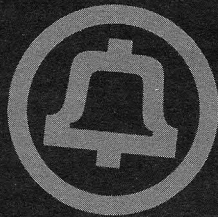
On the above communications, can you spot the one exception? Of course you can. One exception that's not always in the script is their request to notify the facility manager that they need assistance. I'm not saying that you can insert a lot of different requests in that spot, but if I were hacking that system, that's where I would start. Obviously, the more you listen to the active Minuteman III VHF radio traffic, the more exceptions you'll hear and you can build your new hacking library accordingly.

In closing, remember it's okay to listen to a VHF radio while on land. Just don't transmit on a VHF radio while you are on land!

*In 1987, Bad Bobby was the first kid (on his block) to hack the GEOS 64 operating system for the Commodore 64. By removing the security dongle code, he was able to recompile a security-free GEOS 64 operating system. Many kids in his neighborhood appreciated his efforts!*



# TELECOM INFORMER



by The Prophet

Hello, and greetings from the Central Office! I am writing to you from the tiny suburb of Escazu, Costa Rica, where I am ensconced in a compound two blocks from the U.S. Ambassador's residence. For the past month, I have been busily working with other "future leaders," as we are called, on an internship at a very large U.S.-based bank I will call GinormousBank™. Our top-secret project, which is intentionally being done in faraway Costa Rica: Closing bank offices across the United States and moving the work to low-cost locations like India. This will throw thousands of white collar American workers out of their good, well-paying middle class jobs. It's not just call center jobs being outsourced anymore; these are highly skilled financial industry jobs that require university degrees and years of experience. Many of the people affected, having spent their entire careers at the bank, will never find good-paying work again. It is without a shred of irony that the job title I have been temporarily assigned is "execution support" and I now have a taste of what it must feel like to be an executioner.

Thinking about the current state of the U.S. economy has led me to consider whether there are more sustainable alternatives. The economy in the U.S. simply isn't working for most of the people who are in it. Oregon and the Pacific Northwest are historically left-leaning places with a populist streak and, with an historically small and far-removed population from the rest of the country, these states have experimented a great deal with different ownership structures than the typical shareholder-based corporation. In many Pacific Northwest communities, phone companies are organized differently and operate differently than almost anywhere else in the world, and they might just serve as a model for how to organize other parts of the economy in a more sustainable way.

Although I grew up in the Bell System, I have a soft spot for small independent telephone companies. Across the country, there are hundreds of such companies that continue to provide service in small rural areas. I have covered some aspects of rural telephone companies before, such as the payment of access charges (which is mostly responsible for the large set of free teleconference services offered in Iowa and parts of Louisiana, where access charges are unusually high). I have also covered some of the great lengths to which rural carriers go to provide service in the most remote corners of America. However, I haven't really covered the history of

independent telephone companies, or how we can learn from them.

In the early part of the 20<sup>th</sup> century, most rural areas were not economically feasible for the Bell System to serve. A hodgepodge of small, independent concerns emerged to provide service to areas ignored by the Bell companies. In Eatonville, Washington, the phone company became a multi-generation family-owned business when Pete Christensen won the local telephone switchboard in a 1912 pinochle game. At the time, the phone company had only a small switchboard. Today, the company serves approximately 15,000 customers, has been renamed Rainier Connect, and is still a privately held family business.

Privately held family businesses are vulnerable to being sold, though. Louisiana-based CenturyLink built its business by buying up small phone companies across the U.S., before ultimately taking part of the former Bell System independent by gobbling up Qwest (ex U.S. West and Pacific Northwest Bell). While most independents sold to other independents, Woodbury Telephone went the other way. Woodbury Telephone was a family-owned company started in the 1870s by a local businessman who wanted to link the town railway station with his farm supply store. The company eventually grew to approximately 19,000 lines of service before it was purchased by Southern New England Telephone (SNET) in 1997. Interestingly enough, SNET was one of the two original parts of the Bell System (along with Cincinnati Bell) that was never majority owned by AT&T. All of that changed in 1998, when SNET was itself acquired by SBC Communications, which was then acquired by AT&T. Woodbury Telephone thus became the only independent operating company that has been fully absorbed by the former Bell System.

Another type of ownership structure for independent telephone companies is the cooperative. Cooperatives are different than other types of organizations because they are owned by their members, who are usually also their customers. If you are a member of a credit union, you probably notice that they have lower fees and pay higher interest on deposits. This is because members are the owners, so profits are returned to members in the form of better and lower-cost services. If you are a member of REI, the dividend check you receive each year is paid because you are part-owner of the cooperative. And in the state of Washington, even a large health mainte-



nance organization (Group Health) is organized as a cooperative. As with other cooperatives, members are owners of the cooperative, and elect the board of directors. Group Health has an incentive to keep its members healthy because this lowers its costs, and its strong emphasis on preventive care (with highly measurable results) is a frequently studied example of the potential for innovative health reform in the U.S.

In all cases, the interests of a cooperative generally differ from those of a corporation. Corporations are organized to produce income and pay dividends to their shareholders, whereas cooperatives are organized to provide the best service to their members at the lowest possible cost. Dividend-paying corporations can earn a profit by providing a useful service - AT&T and Exxon do this every day. However, they are answerable primarily to their shareholders and not their customers. This means that the interests of the two groups *can* be aligned, but aren't *necessarily* aligned. This is a big part of why the deferred maintenance backlog in my old Central Office fills two full-size binders and I suspect that a great deal of the trouble reports I filed will never be resolved.

There are about 260 telephone cooperatives in America - many of them in Oregon - and they serve over a million people. Most are in rural areas, originally founded by farmers who had been bypassed by the Bell System. Eventually, interconnection became possible, most often through GTE. GTE gave independent companies access to its tandems and sold them equipment through its Automatic Electric subsidiary. In turn, this gave GTE better economies of scale in equipment production and more leverage in negotiations when interconnecting with the Bell System. Today, telephone cooperatives are organized much as they always have been, with their customers considered members and with the primary mission as customer service. Many telephone cooperatives today offer services that are the envy of urban residents, with fiber to the home, video on demand cable services, and much lower prices than offered by Comcast or AT&T. With no need to pay dividends, well-run cooperatives have been free to invest their profits into better technology and a wider variety of services. Cooperatives can also operate on a longer-term investment horizon than is typical for investor-owned corporations.

Larger cities, noticing the success stories in areas served by cooperatives, are beginning to get in on the action. More enlightened city governments realize that availability of reliable high-speed broadband is now an American competitiveness issue. Seattle mayor Mike McGinn, embarrassed by the slow and expensive Internet service provided by CenturyLink and Comcast in one of the nation's most high-tech cities, made a big splash recently with his SeaFi initiative. This is a proposed public-private partnership to bring fiber to the home. The cable industry joined forces against Mayor McGinn, made large contributions to his political opponent in the recent mayoral election, and arguably brought

down the mayor (who lost the election). The SeaFi initiative now appears headed to defeat as well, although it may be difficult for the new mayor to kill it easily because SeaFi has proven wildly popular with Seattle residents. Other municipal initiatives around the country have been similarly defeated by entrenched interests, from Longmont, Colorado to St. Paul, Minnesota.

Could an old idea from the beginning of the 20<sup>th</sup> century, if imported to cities from rural areas, revitalize the landscape of American telecommunications? Are cooperatives a better way forward? The answer is a distinct "maybe." After all, not all cooperatives are well-run. And there is nothing like a profit motive to sharpen a company's focus. At the same time, American business has simply gone too far in its cost-cutting, and it's beginning to impact American competitiveness as infrastructure deteriorates. Rotting cables and failing batteries aren't fixed by raising dividends and having someone in India write the problems down (often incorrectly) in a deferred maintenance log. I think the ultimate solution is competition: both public and private systems should freely compete, which will keep both of them honest and ultimately benefit the consumer. Are all CLECs filthy? These days, maybe not.

And with that, it's time for me to get back to my important work at GinormousBank™ destroying the American middle class. If my work is successful, thousands more Americans will lose their jobs and the company may even be able to increase its quarterly dividend payout by up to one cent! Yes, the rewards of business school never end. Have a happy New Year and I'll see you in the spring.

## References

<http://www.seattle.gov/mayor/>  
➤ [seafigigabittechnicalfaq.htm](http://www.seattle.gov/mayor/seafigigabittechnicalfaq.htm) - SeaFi initiative FAQ

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/06/big-cable-helped-defeat-seattles-mayor-mcgin-but-they-couldnt-stop-this-colorado-project/> - *Washington Post* coverage about cable industry efforts to defeat new broadband cooperatives

<http://www.rei.com/about-rei/business.html> - Information about how the REI co-op is organized

[http://en.wikipedia.org/wiki/Woodbury\\_Telephone](http://en.wikipedia.org/wiki/Woodbury_Telephone) - History article about Woodbury Telephone

<http://www.rainierconnect.com/about-us/history> - History of Rainier Connect, a hilarious read!

<https://www.canbytel.com/about/history/> - History of the Canby Telephone Association

# *The Many Vulnerabilities of Verity Parental Control*

by Tyler Behling

Verity Parental Control is a software package designed to track and monitor the activity of users on a Windows 7, Windows XP, Windows Vista, or Windows 8 workstation. It's designed for use in a home setting for a parent to monitor and track what a child is using the computer for. Verity will show what websites were accessed, what programs were used, and also will provide screen shots at a predetermined interval. Verity also allows the ability to block websites, programs, and set daily time limits on computer, application, or website usage per Windows user login. Verity Parental Control can also count the number of keystrokes and mouse clicks by application. Usage reports can be viewed by the parent through a password protected web interface or automated emails.

Upon first glance, it appears that Verity Parental Control would be a great tool for a parent to ensure their child is staying safe on the Internet, and not viewing inappropriate content or accessing programs on the workstation that they shouldn't be. But I found many areas in this software that need improvement and methods that will allow complete access to previously restricted activities and content.

## **Verity Parental Control Bootable CD Exploit**

With a downloaded copy of almost any version of Linux, you can create an operating system that will run off of a CD/DVD disc. You simply need to download the operating system online and burn the \*.iso file to a disk using a program like Deep Burner CD software. After the disk is created, you can simply power on the workstation with the CD/DVD in the drive and you will be running your new operating system from the disc. Since Verity is installed on the operating system on the hard drive, in this case Windows 7, none of the configured features of Verity will be enforced.

## **Verity Parental Control Physical Key Logger By Sound**

"Researchers at UC Berkeley have now proved that, using a device as simple as a \$10 microphone, software can learn to recognize

the sound of keystrokes as they're typed, and reveal the characters with 96 percent accuracy." Over time, this would allow a user to eventually obtain the password for the web interface, thus having full control over Verity Parental Control and its settings.

## **Verity Parental Control Virtual Machine Exploit**

A user can install VMware Workstation 9.0 via a free 30 day trial download from the VMware website. Once VMware is installed, a user can download an \*.iso file for any operating system they choose. I chose Windows XP for this test. I then followed the very simple process for installing a virtual Windows XP workstation in VMware. Once installed, I was able to use the Windows XP operating system within VMware without any interference from Verity Parental Control. None of the configured features of Verity Parental Control were enforced on this virtual Windows XP workstation.

## **Verity Parental Control Portable Browser Exploit**

A user can download and install an Internet browser that will run off a USB drive. For this test, I downloaded Opera, Portable Edition. After installing it on the USB drive, I was able to use the portable browser to bypass any Internet security settings enforced by Verity Parental Control. Blocked websites were no longer blocked when using this portable application.

## **Verity Parental Control Proxy Site Exploit**

A very simple way to bypass Internet security settings is with the use of a proxy site. For this test, I used [www.prontoproxy.com](http://www.prontoproxy.com). *"ProntoProxy.com is a proxy site for schools that runs on a high performance dedicated server to allow for the fastest, most responsive, and secure browsing experience available. View sites like Facebook, Youtube, and Twitter without being inconvenienced by school filtering, this is the best proxy site for schools."* Once you navigate to this website, you simply have to input the URL of the site you wish to visit. Even if the site is explicitly blocked by Verity Parental Control, you are still able to navigate to it with the use of this proxy site.

## **Verity Parental Control IP Address/ IP Decimal Value Exploit**

Verity Parental Control can be set to restrict access to specified URLs. If <http://www.google.com> is a blocked



website, a user can alternatively browse to <http://74.125.26.147>, which is the IP equivalent. They now have full functionality of the site. This exploit works because Verity Parental Control only blocks the URL address and not the actual IP address of the site. Alternatively, a user can browse to <http://1249712787>, which is the decimal value of <http://74.125.26.147>.

### **Verity Parental Control Registry Exploits**

Verity Parental Control's settings can be accessed directly through `regedit.exe` in Windows 7. By Navigating to "Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\NCH Software\Verity" a normal user without administrator privileges can access settings such as "ProhibitedURLs" which is a list of URL addresses explicitly blocked by Verity Parental Control. The user can simply delete the data from the registry entry and sites that were previously blocked are no longer blocked. A similar registry entry called "ProhibitedPrograms" contains the list of applications explicitly restricted by Verity Parental Control. To gain access to a blocked application, a user can simply delete the application name from the data value. You can also disable chat monitoring, change screen shot interval timing, change time limits, or disable logging in the same fashion. By performing these registry changes, you essentially have full control over the software's restriction and logging functions.

### **Verity Parental Control Password Recovery**

When you first install Verity Parental Control, you are asked to designate an email address to use for accessing the web interface as well as receiving emailed logs. Verity stores this email address in the registry under "Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\NCH Software\Verity\Settings". A normal user without administrator privileges can access the registry entry "Email" via `regedit.exe`. A user can change this registry entry to a different email address of their choosing. Once the email address has been changed, you can open Verity Parental Control's web interface and click on "forgot your password?" link and input the email address that they previously entered in the registry. Verity will then reset the password and send you an automated email containing the new password

to the email that you specified. You now have access to the web interface and full control of Verity Parental Control.

### **Verity Parental Control Password Registry Entry**

Verity Parental Control stores the login and password information in the registry. The login name is listed in a registry entry named "Email" while the password is listed as a registry value in an entry called "\_AdminPassword". The password is not displayed in clear text. Upon changing the password several times, which could be done using the password recovery method explained above, I was able to determine the value for a lower-case alphabetic character based on position in the password. I created a table based on lower case alphabetic characters for passwords up to 12 digits in length. The same could be done for upper-case alphabetic characters, numerical characters, as well as special characters. This could take a considerable amount of time to go through, change the password through the "forgot your password?" link on the web interface, and compare the password in the automated email and the registry entry, but it is doable. Once enough values are determined, one might also be able to crack the algorithm they are using to assign a value to a character.

### **Verity Parental Control Registry Password Exploit**

Verity Parental Control stores the password for the web interface in the registry value for the entry called "\_AdminPassword". A normal user without administrator privileges has the ability to open `regedit.exe` and navigate to "Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\NCH Software\Verity\Settings" and delete the data for the registry entry. This will then blank out the password for the web interface and a user can log in using the email address that is also listed in the registry, leaving the password field blank. This will allow a user full access to the web interface and all of the settings of Verity Parental Control.

### **Verity Parental Control Logging**

Verity Parental Control stores the log files and screen shots for any user in the directory "C:\programdata\NCH Software\Verity\Archive\user". In this directory, you will find the following folders: "ProgramActivity",

"Screenshots", "SecurityEvents", and "WebActivity" which contain all of the logged information regarding activity for a user on the workstation. The information is stored as either a text file, Excel spreadsheet, or JPEG image. A normal user without administrative privileges can go into these folders and remove entries from logs and delete screen shots.

### Verity Parental Control Shut Down

Verity Parental Control has "Taskmgr.exe" on the list of prohibited programs by default for users. This prevents a user from shutting down Verity from within Task Manager by performing ctrl+alt+delete. There are two ways a user can completely disable Verity and all of its restrictions. From what was discussed concerning going into the registry using regedit.exe, you can change the "closeprohibited" value from "1" to "0" which will then allow you to have access to Task Manager and the ability

to shut down Verity Parental Control entirely. The second way is to remove "Taskmgr.exe" from the list of "prohibitedprograms" in the registry. You can then perform a ctrl+alt+delete and access Task Manager and shut down Verity completely. Your workstation would then not be affected by any of the restrictions previously configured and no logging will take place.

### Works Cited

- Verity Parental Control - <http://www.nchsoftware.com/childmonitoring/index.html>
- Pronto Proxy - <http://prontoproxy.com/>
- Opera Portable - [http://portableapps.com/apps/internet/opera\\_portable](http://portableapps.com/apps/internet/opera_portable)
- VMware Workstation - <http://www.vmware.com/products/workstation/overview.html>

## Anonymity and You, Firefox 17 Edition

by l0cke

I want to address this recent thing going on with the Firefox exploit used to break Tor's anonymity. Anonymity is important to have. Privacy is a right, if not a privilege, and definitely not a privilege that can be taken away for an arbitrary reason.

Someone had asked me years ago about how to track someone down over the Internet at one point and I said, "Just get someone to click a link or use an exploit like the Chinese were using with Flash to track down dissidents." I'm not surprised. I've made my opinion on it well known to many parties and I've kept my mouth shut about it because at every turn privacy activists or programmers tell me that "Tor isn't broken and your attempts to point out our flaws are assbattery," whether motivated by wanting to keep things like that secret or to comfort themselves and others who use the service. There are many means one could use to break Tor's protection, including taking advantage of OS and software components or by using analysis to make educated guesses about the location of both Tor users and Tor services.

There is no such thing as true anonymity, though one might be able to set up a VPN or proxy like JonDonym, or another instance of Tor, or maybe even chain them without much, if any, technical knowledge whatsoever to prevent

vulnerabilities like this from hitting. One could also make Tor the operating proxy for all of one's Internet traffic on a machine or entire network via firewall, or by using a special app that only allows traffic through that proxy and/or VPN and disconnects any traffic outside of it before it reaches the physical network connection - or via software on the router/firewall that drops anything not going to Tor or whatever anonymity service.

I've pointed out to many security software developers that the security of the Tor software just isn't there. I suggested that either there was something in the code or something the code interacts with that was exploitable. What it was, I don't know. But take everything that's connected to software you use as an extension of that software. This recent event proves that even more. I know people who think there are magic services that make one anonymous. There aren't. And with our knowledge now of PRISM - if someone can see the traffic on both ends and just match up timestamps and file size transfers, then guess what? You're on candid camera, a lead to be pursued by someone wanting to track down who received or transferred those files or both. By files, I mean even web traffic.

Five things to take into account that aren't being done right now in any anonymity service:

- 1) *No Real-Time Communication.* A true anonymous service would be like old FTPMail. It will send a request at a randomized time that has nothing to point it back at the user. An even

smarter one will send or receive traffic at a time that's generated based upon human psychology, i.e., no porn requests at night or on weekends.

2) *Fabricate Clues to Location.* Create blocks of downtime that have no reason because one's downtime can show one's location.

3) *Do Like UPS.* Make the anonymity node perform the request - it sends and receives all data so that it's not parsed by the web browser directly. Think the way a parcel service delivers mail.

4) *Sterilize All Content.* Perform transforms on text - the easiest is to translate text from an original language through several others. I'd go one step further because this can be reversed and use a mathematically generated dictionary or array using dictionaries, thesauri, and the like to add even more randomness. Plus it'd look kinda crazy and reminiscent of leetspeak. "Thee hast better not g0nn4 speek dat 2 dem, boy" for "You'd better not tell them that," etc.

Sterilize images, audio, video, and the like as well - at least insofar as what created the container, any information in the images, etc. Killing lighting and replacing it with a solid color would be good too - filters so that someone can't use the sunlight or stars to tell where one is based through an image or video. Also, creating blocks over all people in images and blocks over any visible text in any language.

Sterilize all hypertext and code - any kind of code or markup or uncommon phrasing that might be found if reposted as a fingerprint (i.e., using "hast" a lot in text instead of "has") or processed by a computer like the code that created the GET request.

5) *Use or Adapt Third-Party Tools.* For now, use whatever you can on top of your anonymity

services. Use NoScript and make sure that DNS requests don't leak. Make sure that whatever IP protocol you use is stable and doesn't send information to servers you request to. Don't take a program author's word for anything, ever. Test against tools that benchmark and look for those things or figure out how to test them yourself. Also, be wary of services that may contact another server for certificates or verification - HTTPS ends up connecting to an index to verify the certificate a site gives. If you're not careful, some tools can contact DNS servers you already use. Use a plugin that makes sure that a proxy (like Tor) is always enabled if connecting to a site. Some services, even when working, have a big flaw: the operator. If you forget to turn on the anonymity service or ensure that it's running, that's on you.

I believe that's why TorButton is no longer a standard option in Tor. Become a programmer in spirit if not in mind. To do any less is to invite disaster. Learn how these things work and chances are if you think of some new way to do something, someone else has or you can figure out how to adapt their work to your own use.

I'd go so far as to make it impossible to easily upload or download images via Tor, even if it means you have to kill all forms of compression or make them readable by a "processing node" that handles the no-real-time rule as well as sanitizing the stuff, killing all content that isn't text or isn't hypertext to be sanitized and shown as a special local only-viewing-markup in JSON or XML. That might not stop people from creating new versions of uuencode out of text or hypertext, but it would make easy access to sending and receiving child porn harder.

## WI-FI SECURITY: ATTACK AND DEFENSE

by ternarybit  
austindcc@gmail.com

This article seeks to examine the current state of Wi-Fi security, with a practical emphasis on attack and defense methodology.

The proliferation of mobile devices, decreasing cost of deployment, increasing speed, and overall convenience all play huge roles in the swelling popularity of wireless networking. These benefits do not come without drawbacks, however; it seems convenience and security are inversely related. Wi-Fi security has matured significantly since its birth around the turn of the millennium, starting with open

networks and WEP encryption. With insecure networks declining along with the ratification of WPA2 in 2004, it would seem we are moving toward a more secure wireless world. Experience, however, may tell a different story.

I ask the reader to use this information to explore and not exploit; please treat others' networks the way you want yours treated.

### A Brief Overview of Wi-Fi Security WEP

The initial ratification of IEEE 802.11 in September 1999 brought with it Wired Equivalent Privacy (WEP) as the only means of encrypting traffic. WEP uses a 40- or 104-bit



key combined with a 24-bit initialization vector (IV), which are then processed through the RC4 stream cipher to achieve communication privacy. Only two years later, security researchers Scott Fluhrer, Itsik Mantin, and Adi Shamir published the first cryptanalysis of WEP. They demonstrated that an attacker can recover the key by eavesdropping on enough encrypted traffic. Numerous successive cryptanalyses have been published, offering more and more efficient attack methods that reveal the key in a matter of seconds.

These weaknesses have been implemented in widely available tools, such as aircrack-ng, and automated with scripts like wepbuster. It is now utterly trivial to recover any WEP key almost immediately. As such, in 2004, the IEEE officially deprecated WEP in favor of the newly-ratified 802.11i standard, commonly known as Wi-Fi Protected Access II (WPA2). Statistics available on [wgle.net](http://wgle.net) show that about 20 percent of networks still implement WEP, even after nine years of well-documented weakness. We will not examine attacks on WEP or its defense further; attacks are well known, and the only defense is to simply not use it.

## **WPA**

The Wi-Fi Alliance developed Wi-Fi Protected Access as a replacement for WEP, starting in 2003 with WPA. WPA, also known as 802.11i draft, was intended to offer better security to Wi-Fi networks before official ratification of 802.11i, which would become known as WPA2. The most common deployment method, known as WPA-Personal, uses an 8- to 63-character pre-shared key (PSK) as a shared secret in favor of the hexadecimal string in WEP. By implementing Temporal Key Integrity Protocol (TKIP), which generates a new 128-bit key for every packet sent, WPA mitigates one of WEP's major weaknesses. An attacker can no longer recover the key by simply eavesdropping on enough traffic.

Additionally, TKIP improved WEP's practices by introducing packet sequencing and a true message integrity check (MIC) in favor of CRC-32 for integrity. Packets received out of order are rejected, and MICs offer better assurance that packets have not been intercepted and altered by an attacker. Since WPA was intended to run on the same hardware that implemented WEP, TKIP also uses RC4 to encrypt traffic. In 2008, Martin Beck and Erik Tews released a keystream attack on TKIP that allows an

attacker to send between 7 and 15 packets of their choosing, by exploiting weaknesses in WPA's MIC mechanism. Though the attack does not reveal the PSK, it does demonstrate a design flaw in WPA that will likely lead to its deprecation in favor of WPA2. [Wgle.net](http://wgle.net) reports that about 11 percent of networks currently employ WPA, with an overall declining trend.

## **WPA2**

Wi-Fi Protected Access II, officially standardized as IEEE 802.11i-2004, is the current, preferred, and most secure method available to encrypt wireless traffic. It superseded WPA in 2004 when it became an official IEEE standard, and addresses most (if not all) weaknesses found in WEP and WPA. Most commonly deployed as WPA2-Personal, it uses the same 8- to 63-character PSK from WPA as the shared secret. WPA2 comes without the cryptographic weaknesses found in both WEP and WPA by replacing TKIP and RC4 with the very robust AES block cipher, employed as CCMP. As of this writing, no one has published a cryptanalysis of WPA2 or full 14-round AES. The emerging 802.11n specification mandates use of WPA2-AES/CCMP as the only acceptable encryption mechanism. [Wgle.net](http://wgle.net) reports about 25 percent of networks currently employ WPA2, with an overall increasing trend.

## **Attack**

### **WPA(2) Authentication**

During authentication with an access point (AP), a client station (STA) engages an Extensible Authentication Protocol over LAN (EAPoL) 4-way handshake. During this exchange, the STA and AP authenticate each other by generating a 256-bit pairwise master key (PMK), which is then used to generate a session-specific pairwise transient key (PTK), which then encrypts traffic.

To generate the PMK, both STA and AP pass the pre-shared key, salted with the AP's ESSID, through 4,096 iterations of the password-based key derivation function (PBKDF2), using HMAC-SHA1 as the cryptographic hash function. The PTK is computationally trivial to derive from the PMK; possession of the PMK offers an attacker all the information necessary to potentially derive the pre-shared key, and then subsequently decrypt all network traffic.

Salting the PSK with the ESSID ensures that no rainbow table of universally-usable PMKs will ever exist. The same pre-shared key

used on networks with different ESSIDs will generate different PMKs. Utilizing 4,096 iterations of HMAC-SHA1 stretches the key, which makes generating PMKs computationally expensive. Whereas most modern CPUs can calculate millions of SHA1 hashes per second, in most cases they can only compute thousands of PMKs per second. Both salting and stretching were designed to deter brute force attacks on the captured PMK.

### **Obtaining Handshakes**

Probably the most well-known attack on WPA(2) involves an attacker eavesdropping on the 4-way EAPoL handshake between an authorized STA and target AP, then using a dictionary attack to derive the original PSK. On busy networks, sniffing a handshake can be trivial. On quieter networks, an attacker may send deauthentication packets to an associated STA, forcing the STA to re-authenticate (which usually does so automatically), thereby revealing the PMK to the attacker. On very quiet networks, eavesdropping a handshake may become very difficult and time-consuming.

Tools like Kismet and airodump-ng are capable of such eavesdropping, the latter more commonly used for this purpose. Assuming the attacker possesses a Wi-Fi chipset capable of RFMON mode with appropriate drivers, issuing these simple commands within BackTrack 5 sets up an eavesdropping session:

```
# airmon-ng start wlan0
# airodump-ng -w pentest mon0
```

These commands initialize a monitor interface, and log all frames from all channels to files prefixed with 'pentest'. Assuming the attacker is within range of an authenticating client and the target AP, airodump-ng will report the capture of the WPA handshake, which is then immediately ready for dictionary attack.

### **Attacking Handshakes**

Various tools exist to mount dictionary attacks on captured handshakes, most notably aircrack-ng and pyrit. Aircrack-ng is part of the canonical Wi-Fi auditing suite of the same name, but pyrit has overtaken the spotlight as the most effective tool for attacking handshakes. This is because pyrit has leveraged the massive computing power of graphics cards to dramatically increase attack speeds - often by orders of magnitude - compared to CPUs alone. For example, my Core2 Quad computes PMKs at about 2,300 per second, whereas my

Radeon HD 4890 computes PMKs at about 27,000 per second. Multiple GPUs, cloud-based computing, and FPGA- or ASIC-based platforms offer even faster speeds, increasing feasibility of dictionary attacks dramatically.

A successful dictionary attack consists of at least four elements: the pairwise master key captured from a legitimate authentication, the ESSID of the target network, an appropriate dictionary file, and sufficient time. The heart of any dictionary attack requires that the PSK used to generate the captured PMK exists within the attacker's dictionary - these attacks simply exploit weak passphrases. True brute-force attacks are infeasible on PSKs eight characters and longer because of the very large keyspace and relatively slow attack rate. For example, attempting all possible eight-character mixed-case alphanumeric passphrases would take approximately 256 years at 27,000 PMKs per second - and this doesn't include any special characters. Obtaining an appropriate dictionary for specific networks remains the attacker's challenge in mounting successful attacks. Very weak, common passphrases are easy to crack, but longer and more complex passphrases may never capitulate; there is no guarantee of success with a handshake attack.

Not only can pyrit leverage GPU power, but it also leverages the convenience of a pre-computed database of PSKs, ESSIDs, and PMKs. This means an attacker can begin pre-computing PMKs for a given ESSID with a chosen dictionary before capturing a handshake. Looking up pre-computed PMKs takes a fraction of the time computing them does, so cracking an obtained handshake may only take seconds in an ideal scenario.

Assuming airodump-ng reports successful capture of a WPA(2) handshake in the example above, an attacker can mount a basic dictionary attack with the following approach:

First, import a basic wordlist, included with BackTrack, into pyrit's database:

```
# pyrit -i /pentest/passwords/
↳ wordlists/dark0de.lst import_
↳ unique_passwords
```

Second, supply pyrit with the captured handshake and attack it, saving computed PMKs in the database for future use:

```
# pyrit -r pentest-01.cap attack
↳ _batch
```

Assuming pentest-01.cap contains at least one valid handshake for a single network, pyrit will automatically select that handshake and begin attacking it with the passwords imported

with the previous command. If the capture file contains more than one handshake from multiple networks, one will need to specify which to attack.

Over time, an attacker may collect and pre-compute PMKs for many millions of PSK/ESSID combinations, making future attacks less cumbersome. However, success still relies on the AP using a PSK within an attacker's dictionary; strong PSKs will withstand dictionary attacks from even advanced hardware and software.

By default, pyrit only supports CPU-based cracking. Various guides exist online for compiling CUDA and Cal++ modules, for NVIDIA and ATI/AMD GPUs, respectively. I leave this as an exercise to the reader.

### Attacking Default Configurations

In an effort to mitigate security risks, vendors have generally improved their hardware's default configurations. While these changes improve upon open or weak configurations, they often fall prey to basic attacks. I will examine two cases from AT&T and Netgear.

#### AT&T Default Configuration

The latest modem/WAPs that ship with AT&T DSL service in the U.S. come configured with WPA2-AES/CCMP encryption, using a ten-digit numeric PSK printed on the unit. Such networks are identifiable by their ESSID in the form of ATT###, where ### represents a three-digit number. This number is the last three digits of the unit's serial number. Some experimenting revealed that the unit's serial number is simply the decimal form of the AP's hexadecimal BSSID. Interesting, but not necessarily helpful for auditing PSKs - I could find no obvious way to derive a default PSK from its serial number.

The keyspace of a ten-digit number is 1010, or ten billion. With my hardware, I can exhaust this keyspace in a theoretical maximum of four days and seven hours - but this assumes the target PSK resides at the end of the list. In practice, attacks usually take around half the theoretical maximum time. This means any AT&T AP with default configuration is severely vulnerable to a dictionary attack.

Generating a list of all ten-digit numbers is trivial with sufficient time and disk space. The program crunch does this effortlessly:

```
# cd /pentest/passwords/crunch
# ./crunch 10 10 0123456789 -c
➔ 1000000000 -o /path/to/media/
➔ START
```

The first two arguments tell crunch the minimum and maximum line lengths; the third argument is our character set; the fourth and fifth arguments instruct crunch to split our list into files of one hundred million lines for ease of management. The files will be named <start of range>-<end of range>.txt in the current working directory. If you're running BackTrack on a live medium, you will need to mount an external storage device and specify that in the output parameter. The uncompressed final list will occupy about 102GiB.

If you're running BackTrack on a live medium, we need to change pyrit's database location to external storage. Open the config file in vim:

```
# vim ~/.pyrit/config
and point the default_storage directive to external media.
```

Next, import the word lists into pyrit:

```
# for i in *.txt; do pyrit -i $i
➔ import_unique_passwords; done
```

This tells pyrit to import every file ending in '.txt' as a unique password list. Expect this to take quite some time. Importing the passwords into pyrit's database compresses them and makes them most readily accessible by pyrit for future attacks.

Then, attack the handshake:

```
# pyrit -r att-01.cap -o att-
➔ owned.txt attack_batch
```

In this example, I've added the -o parameter to save the recovered PSK when found.

#### Netgear Default Configuration

Netgear's latest crop of routers ship with default ESSIDs and PSKs designed to give the user enhanced security out of the box. The ESSIDs take the form of NETGEAR##, with ## representing two digits. I was interested to find the default PSK on two routers I tested take the form of <adjective/verb> + <common animal> + <3-digit number>, e.g. smilingrabbit318. The use of words and numbers seems to offer a secure approach to default PSKs. The English language employs hundreds of thousands of words, and using two of them with three digits would seem to offer a robust, yet memorable, default passphrase.

However, this approach degrades quickly under closer examination. Netgear has not randomly chosen any two words - they are two fairly common words in a grammatically correct order. After some searching and hacking, I came up with a reasonably comprehensive list of common adjectives and present-tense



verbs which came to only 1,715 words. A list of common animals came in much smaller, at only 171 words. I didn't include highly esoteric animals (like archaeopteryx), or very specific ones (like saber-toothed tiger - just tiger). I also didn't include adjectives or verbs that a Netgear customer would view as offensive or inappropriate. Somehow, PSKs like "murdering-lion666" and "sexygorilla690" seem unlikely. I used crunch in much the same way as the example above to create a list of all 1,000 three-digit numbers, and wrote this simple script to combine them into a master PSK list:

```
#!/bin/bash
PRE=$1
SUF=$2
NUM=$3
OUT=$4
echo "Creating a list of all
➔ combinations of the files
➔ <$PRE>+<$SUF>+<$NUM> in word
➔ list $OUT."
TOTAL=$(expr $(wc -l $PRE) '*'
➔ $(wc -l $SUF) '*' $(wc -l $NUM
➔ ))
echo "Total combinations: $TOTAL"
echo "For large dictionaries,
➔ this will take significant
➔ time and disk space."
while read PREFIX
do
    while read SUFFIX
    do
        while read NUMBER
        do
            echo $PREFIX$SUFFIX
➔ $NUMBER >> $OUT
            done < $NUM
        done < $SUF
    done < $PRE
done

echo "Done."
exit 0
```

Usage example:

```
# chmod +x netgear-psk.sh
# ./netgear-psk.sh adj-verbs
➔ animals numbers netgear.lst
```

In my case, the final wordlist weighed in at a mere 293,265,000 lines and 4.8GiB - less than three percent of AT&T's default keyspace. It's possible my list isn't exhaustive and, in the absence of several networks to test it on, I can't say for sure. Even if it won't crack every default PSK, it probably will succeed at least 75 percent of the time, and maybe more. My retired gaming rig chews through this list in just over three hours, which means I could pre-compute PSKs for all 100 default Netgear ESSIDs in

about twelve and a half days, making recovery of any default Netgear PSK utterly trivial.

### Wi-Fi's Achilles' Heel: WPS

In 2007, the Wi-Fi Alliance sought to unify the diverse auto-configuration methods sprouting up from various vendors, which purportedly offered consumers the ability to easily set up secure networks, without any knowledge of networking or security. They published the Wi-Fi Protected Setup (WPS) protocol apart from any involvement with the IEEE, which uses hardware or software buttons and PINs to set up secure networks. At the heart of the protocol is an eight-digit PIN, usually printed on the hardware itself, which allows its possessor full control over its configuration, including any currently employed PSK - no matter how long or complex.

In theory, such a protocol is not inherently unwise or insecure. It is reasonable to accommodate inexperienced customers who can't intelligently decide between various encryption options, who will very likely choose insecure configurations. The use of an eight-digit PIN also need not cause concern, since  $10^8$  offers some hundred million possibilities. An example of one such secure deployment would instruct the customer to press the physical WPS button on the router, then enter the PIN on the computer. The router will accept a PIN for up to 30 seconds after pressing the button, then lock itself to further PIN requests. This would render PIN brute-forcing completely infeasible.

For inexplicable and inexcusable reasons, WPS is not deployed this way as of this writing. Quite the contrary, it suffers from several critical design flaws that now threaten the security of millions of networks worldwide. In December 2011, Stefan Viehböck publicly announced this vulnerability, which currently has no known countermeasure aside from disabling WPS entirely. Tragically, this isn't even possible on some APs, and firmware updates to address this have come slowly - if at all.

Very few routers limit the number of allowed PIN attempts in a given time interval. Some allow for one attempt every 1-2 seconds, while others will lock WPS for a paltry five minutes after approximately 25 incorrect attempts, barely delaying an attack.

Most appalling yet, WPS also does not employ the full keyspace offered by an eight-digit number. The last digit is a checksum, and the remaining seven digits are divided

into groups of four and three digits, which are confirmed independently by the AP. This effectively reduces the keyspace to a mere 11,000 possible PINs ( $10^4 + 10^3$ ). At two seconds per PIN, an attacker can recover the AP's PSK and gain authority to (re)configure the device in a theoretical maximum of about six hours. In practice, WPS PINs usually crack in roughly two to ten hours, depending on the AP. Any AP with WPS enabled is vulnerable to this brute-force attack, which has been implemented in the program reaver, also available on BackTrack 5.

Reaver offers an attacker many options, and comes paired with a tool called wash which identifies vulnerable APs within range. Assuming one has enabled monitor mode on a wireless interface,

```
# wash -i mon0
```

shows all WPS-enabled APs in range along with some basic WPS information. One only needs the BSSID of the target AP to begin a basic reaver attack:

```
# reaver -i mon0 -b <BSSID of  
➤ target> -c <channel of  
➤ target> -v
```

Using -v tells reaver to enable verbose logging, printed to standard output. Most often, problems carrying out the attack are solved by achieving better signal quality with the AP. An RSSI of -65dB or better offers the best chance of success. Depending on the AP, the attacker may need to adjust the delay between PINs with the -d option, or set a recurring delay after a number of attempts with the -r X:Y option, which sleeps Y seconds after X PIN attempts. Using small Diffie-Hellman numbers with the -S option may also speed the attack. An alternate invocation will log reaver's progress to a file, with optional monitoring from a separate terminal:

```
# reaver -i mon0 -b <BSSID of  
➤ target> -c <channel of target>  
➤ -v -o reaver.log  
<Alt-F2>  
# tail -f reaver.log
```

Bear in mind that MAC spoofing works with reaver only when the physical interface is spoofed (e.g. wlan0), not just the monitor interface (e.g. mon0).

The only major drawbacks to a WPS attack are that they generate a lot of traffic, and the attacking device must remain within range of the target for the duration. Even still, this attack remains very attractive because it offers a guarantee of success to reveal any PSK, no matter how long or complex.

## Defense

Disabling WPS and deploying WPA2-AES/CCMP with a strong passphrase offers very good protection in most circumstances. I recommend ten or more mixed-case alphanumeric characters, using at least one special character. In this scenario, an attacker would probably move to side-channel attacks, like social engineering - or just move along to lower-hanging fruit.

Since the wordlist is at the heart of any handshake attack, it's wise to take measures to ensure your PSK never ends up in one. Various password database leaks form the basis of many likely wordlists. For example, RockYou.com was compromised and leaked some 32 million plaintext passwords. More recently, attackers released about 450,000 plaintext passwords from Yahoo, many of which may be considered "secure" passphrases. I have personally verified that none of my PSKs were part of these disclosures, and I suggest you do the same.

Some APs offer the option to schedule downtime, which automatically disables the Wi-Fi radio at certain intervals. This narrows an attacker's window of opportunity, which is especially relevant to WPS attacks.

If disabling WPS is not possible on your router (for example, some Linksys units won't actually disable WPS even if you opt for manual configuration), consider flashing it with DD-WRT, a free aftermarket firmware that does not support WPS. Verify none of your networks employ WPS by running the wash tool described above.

Arguably the most secure wireless protection comes from deploying a RADIUS (802.1X) server and WPA2-Enterprise, but this is not practical for many small networks. If your network runs a candidate server and the increased security merits the investment, consider this option.

Finally, in some circumstances, Wi-Fi offers more risk than reward and should not be deployed at all. Networks that house very sensitive information would do well to avoid the risk altogether; an attacker cannot crack a PSK or PIN that doesn't exist.

*I would like to thank Jesus, my wife, and the entire staff and community of 2600 for many years supporting my hacking endeavors.*

# THE MATURATION CYCLE OF A HACKER

by Ig0p89

Over the years, it has become apparent that there is no such thing as complete computer security. There is always a flaw somewhere or an opening for an exploit. For some people, this draws them to our game (to breach the subject's system). It is the thrill of the chase that brings them back for more and more. For some, this is for personal gain. They may code a new virus or exploit. At some point, because the user is generally the weakest link, access is gained to their email and system. The subject's login codes are gained, as well as trade secrets.

What would drive someone to do the above mentioned activities? The hacker starts young. They are generally drawn to the tech-oriented activities. This could take the form of electronics or computers. After their appetite has been whetted, they seek more information and experience with the computer and its ability to reach and touch nearly everyone. They may, for example, start to show more interest in the local high school's lack of security. For instance, many years ago, to access the local high school's heating and cooling system, one could dial in using a modem connected to a handset. As long as you had the password, the A/C was at your disposal.

The hacker life cycle may be comparable to a tree. The first is much like the seed being planted. The hacker begins to be interested in computers. This may start with video games or other electronica. They bore with this and move on. The newly minted hacker may start coding. They are drawn to this as a basic curiosity. There are no malevolent thoughts or actions. They just want to know how it works. If brazen enough, they may even try to upgrade their rights on a system.

After this area of expertise has been fully explored, the hacker may move forward into the next stage; let's call it the sapling stage. This is done without thought due to boredom in school, personal pursuits, or other avenues drawing their attention. They start to enjoy learning more about IT and security. This is further enhanced as they find systems are not appropriately patched and compromising them would not take all too much work. They may find this exciting, which only further fuels the fire.

The last stage would be analogous to a mature tree. The hacker has a good sense of who they are and their self-identity. They are comfortable spending time with other hackers. If they don't know something, they are comfortable with asking an associate for a second opinion.

Some people may view this as a bad thing. The knowledge is more of a tool, void of feelings and intent. The writer views this more as a positive thing. The curious mind is ever expanding and creative.

To remove any potential issues, there are ways to help keep the hacker on the more appropriate (i.e., legal) path. The friends and associates may foster the curiosity and grow this in a positive manner by encouraging them to explore and think about the processes. The mentor could be helping one of the next STEM generation. In this, they can guide the hacking. The parent, if this is the person helping the hacker/child, should not be what the writer calls a DVD parent (gives the child a DVD and tells them to watch; practically uses this as a baby sitter and a way to socialize their child), but should engage them in this.

The potential greatness is limitless.



# There is *Never* a Free Lunch

by Ig0p89

Overall, technology is a great thing. I cannot imagine what life would be like without my iPhone, laptop, etc. It would simply be a mental drain, as everything would slow down exponentially. Technology has made us more productive, given us the ability to contact family and friends in an instant, and, in general, made our lives so much simpler. This is clearly the positive side.

As with anything, if there is a positive, there is a negative to counterbalance this. There is always someone working to get something for nothing (and the checks for free; sorry for the 80s reference, but it was fitting). These scam artists offer you something to make your life easier. After all, this is exactly what we want. This could take the form of a call or email stating the lottery has chosen you as a winner. This could also manifest itself as you - Joe or Josephine Consumer - being called out of the blue by a Microsoft customer service representative letting you know your system is corrupted with a virus. He can certainly fix the issue in a very expedited and quick timeframe. He would just need remote access to your machine.

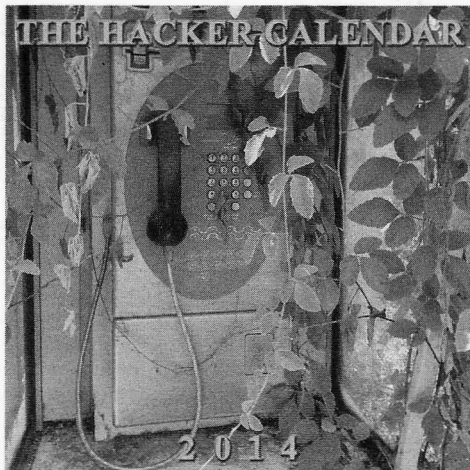
This sounds easy enough. You just allow

him access to your computer and all will be fine in a few minutes. The alleged Microsoft representative stated there are viruses on your system that could cripple it.

The person on the phone really is not working for Microsoft. I know you are as surprised as I was (sarcasm) to hear this. This clearly is nothing more than scamming a gullible person. Microsoft does not cold call a consumer regarding their PC having a virus. It just does not happen. As a rule of thumb, there probably is nothing wrong with their system. If they do allow the scammer the remote access, the bugs the scammer was supposed to protect the consumer from are put on the machine (malware, keylogger, or other software apps). They could collect the consumer's credit card information and numbers, passwords for everything the consumer has logged into, and other private or confidential information.

The lessons to be learned abound here. As a consumer, don't purchase computer services over the telephone. This is only going to be a problem. Also, don't let someone you did not initiate contact with have access to remote control your system. If you do, you will have a bad day. A little common sense goes a long way.

## WELCOME TO 2014!



Anything missing? Take a look right now at the nearest wall. If it's not adorned with a genuine full-size 2014 Hacker Calendar, then you're at risk of a) not knowing how the dates this month are configured; b) not being aware of what happened on this day in hacker history; and c) not being able to admire the beauty of this month's payphone displayed as a 12"x12" glossy photo. \$14.99 includes domestic shipping

[store.2600.com/calendar](http://store.2600.com/calendar)

# The Hacker Perspective

*Synstr*

To answer the question of what defines the word "hacker" is to take on a seemingly impossible task, one that arguably still has yet to be resolved. Just as the media wrongly portrays hackers as evil, lawbreaking individuals, so do the hackers themselves often question what exactly the term means. I am going to attempt to answer this question in a way that will not actually define the word, but instead share what the word means to me, as a person.

As long as I can remember, I have had an extreme passion for technology - computers and the Internet, in particular. When I was just five years old, I had the privilege of owning my own computer. It was a Commodore 64, and I primarily used it to feed my growing addiction for video games. One day, my grandfather (rest in peace, Grandpa) came over to our house to visit, and in the process, he brought me a huge case of floppy disks that each contained one or more games on them. I was ecstatic. As happy as I was to see Grandpa, when I found out that he had brought me video games to play, I wanted to boot them all up right then and there, and play all day and night. And he knew it.

I played my heart out that day and, eventually, Grandpa ended up showing me how to use a program called Copy II 64. Initially, I thought it was quite boring - I mean, it wasn't a video game - how fun could that be? However, I let Grandpa finish telling me about the program. It was the least I could do. After all, he brought all of these cool games for me to whet my appetite with.

It turned out that, using this Copy II 64 program, I could take a blank floppy disk that I bought from the store and copy a game that Grandpa brought for me onto said disk so I could have my own copy. Suddenly, this "boring" program became much more interesting to my five-year-old mind. I could get floppy disks from the store, copy all of Grandpa's disks, and keep the copies for myself so I could play them anytime! I think Grandpa was able to tell that computers were going to be big in the coming years, and he realized while watching me play all of those games and loading them up by myself that, with little assistance, my profound interest in them would benefit me in the long run. So Grandpa let me keep all of those games until I

had copies of all of the ones I wanted.

It took a few run-throughs with Dad helping me out to learn exactly how to copy the disks the right way, but after about five or ten disks, I was able to do it by myself. At five years old, I was inadvertently a part of the "warez" scene - a scene I never even knew existed, one that I didn't even know I was a part of until many years later.

Dad realized, like Grandpa did, that I had a certain "knack" for technology. He realized this as soon as I was three years old and able to go outside and tune our satellite dish to the Disney Channel so I could watch cartoons. So Dad encouraged my experimentations with our C64 - he supplied me with the floppy disks, and I copied damn near all of Grandpa's collection. Soon, I had my own archive of video games. And I was a happy kid.

Fast forward a year or two and, after exhausting my entire archive, I began to instinctively question things. I had this entire collection of games at my disposal, games that I played until I knew every nook and cranny. I knew everything about them. But eventually, a question came to mind: how were the games created in the first place? How did the Copy II 64 program know what to do to get the games from Grandpa's disks onto mine? Was it magic?

During these periods of questioning and wonder, I had access to a lot of magazines of Dad's and Grandpa's, such as *Compute!* and other such publications. These magazines often included games that you could type into the computer and save onto a tape or disk. I never typed any in because my young mind felt that playing these games wouldn't be worth the work it would take to type them in. However, as I was curiously scanning over the lines of so-called "BASIC code" that had to be typed in, I wondered why they had to be typed in to get the game to work? How do these lines of "code" create the game? As far as I knew, the white-headed dude named Jumpman in the Epyx classic of the same name just appeared from thin air, and it was my job to help him disarm the bombs and save Jupiter from being blown up by the bad guys. I knew I had to control him with the joystick - I never knew why he couldn't move without my help, nor did I care. I just wanted to win the game!

Then, one day as I was playing, I noticed something on the title screen that I never really noticed before. In white text below the colorful Jumpman logo, were the following words: "CREATED BY: RANDY GLOVER".

Who was Randy Glover? And how did he create Jumpman? How did he make Jumpman move, dodge, and most importantly, jump? Did it have something to do with these codes, like the ones I saw in *Compute! Magazine*? How did he know which codes to put in to make all of this happen? I had to find out, I was too curious to let it slide. So I began reading everything I had to get clues: issues of *Compute!* and the other magazines I had, and the manuals for the Commodore itself. I eventually unearthed the *Commodore 64 Users' Guide* from the cardboard tomb it laid in. This book eventually became my Bible. I saw commands within its pages that I was familiar with from the magazines: PRINT, GOTO, IF...THEN, etc. This manual, however, told you exactly what each command did, and how to use them. Being a child at the time, I had no idea what the commands meant, even with the detailed syntax descriptions of each one, but I'll be damned if it did not blow the roof off of my curiosity.

As I read this manual, I found a command called LIST. According to this manual, you could use the LIST command to show you all of the codes that comprise a program. Bingo! This was the holy grail I was looking for! The key was to LOAD the program into memory first, which I was already familiar with from booting all of my games up. So, I put in my Jumpman disk I copied from Grandpa, typed LOAD"\*",8,1, and after the game loaded, instead of typing RUN to run the game program, I typed LIST. My screen started flooding with BASIC code, and my eyes lit up like a Christmas tree as I watched them all fly by. I had absolutely no idea whatsoever what they all technically meant, but at that point I didn't care - because I knew I had just found what made Jumpman jump!

These codes whisking by my screen were Greek to my child mind, but I knew that they were what made Jumpman come on the screen, acknowledge what I was doing on my joystick, react to it, avoid that pesky white bullet-thingy, and defuse the bombs on every stage. This was how Jumpman knew what to do when I told him to do it. And the fact that I was able to find all of this out on my own was a catalyst not only for my future synergy with technology and computers, but also for the very foundations and principles I would build myself upon. It sparked the beginning of my way of life.

My research did not stop there. I looked into BASIC coding a little more and, while I didn't go too far with it initially, I did code my own program eventually. It was a program that acted like a clerk

at a store. It would greet you with a message, then ask you for five things you wanted to buy. After entering what you wanted to buy, it would thank you and say "here's your receipt:" and list off all five things that you bought. It wasn't much at all, but the fact that I was able to write this, save it to a floppy disk, call it my own creation, and achieve this feat all by myself filled me with joy. I created my own computer program, just like Randy Glover did with Jumpman!

We got rid of the Commodore 64 eventually, along with my game archive, passing it on to my aunt and cousins for them to use. We moved into the Windows world, which carried on well into high school, where I met another friend who was into computers. Until then, I had been the "computer guy" at my school. Everyone would see me and think "there's the computer kid." But as I talked with my friend, who had the same creative writing class in tenth grade as I did, I realized that he knew way more than I did. I kind of looked up to him. He told me about all kinds of computer tricks he did, and introduced me to something that I knew of, but didn't know too much about: hacking.

I figured that hacking was something I would never be able to do. I didn't possess enough know-how to be able to do it. While never telling me outright, he showed me that anyone could do it. He even brought in old issues of a publication called *2600 Magazine* for me to read. The stuff in this magazine blew my mind. It kind of took me back to when I was browsing through *Compute! Magazine*. I had no idea what the articles in *2600* were actually talking about but, man, did it ever interest me.

One day during class, I was on the computer that we had in our classroom. I made a joking comment about how I wished they hadn't locked down Internet Explorer so I could play Flash games on the Web. My friend kind of smiled, and then proceeded to tell me how easy it was to "break" that lock. Knowing his technical aptitude, I didn't doubt that he was able to do it. Hell, he brought in pirated movie bootlegs of movies that were still in theaters, and watched them during class. I figured anyone who knew how to do that knew what they were doing. So I asked him how he defeated the security locking down the computer, because I wanted to try it too. His response was that he was not going to tell me outright how to do it, because he wanted me to learn how to do it for myself. Frustrated, I tried everything I could think of: opening the FORTRES security program itself and trying different passwords, removing the program outright, finding alternate paths to the Internet Explorer executable.... Nothing worked.

My friend, knowing that I would eventually learn and succeed, and that I was genuinely interested in how it worked and not just being a "skript



kiddie," gave me a hint. He told me there was a certain file in the Windows operating system that made the program start when the computer boots up. He didn't tell me the file nor how to access it, just that it existed. Grateful for the tip, and his mercy towards my undying will to find out how to break the security, I researched the issue.

It turned out that there was a file called AUTOEXEC.BAT, which contained commands to load programs at startup. Perfect! This was exactly what I needed. However, when I tried to open that file to edit it, I was unable to. It was most likely the security that was preventing me from doing this. As I was experimenting with the computer, I restarted the PC and, for some odd reason, it dropped me to a command line. I had noticed that I had accidentally left a floppy disk in the drive and forgot to take it out, and that the disk must have triggered the command prompt for some reason.

Then it clicked. I had a command line staring me in the face and the security had not loaded yet. I had full access to the system! I opened the EDIT program through the command prompt, and opened AUTOEXEC.BAT from the C: drive of the computer, and voila! There was the file, in plain sight. After some searching, I found the line that contained the command to boot the FORTRES security program that I wanted to disable. I saved the current, unaltered AUTOEXEC.BAT to the floppy disk and then removed the line telling FORTRES to start, and saved that as a different filename, also to the floppy. I then exited EDIT.

Now, the moment of truth had arrived. I deleted the AUTOEXEC.BAT from the C: drive of the computer, copied the altered version from my floppy with the FORTRES line removed, and renamed it to AUTOEXEC.BAT. I then restarted the PC and, when it booted up, I double-clicked on Internet Explorer, and the MSN welcome page popped up, ready to take me to any website I wanted! Then I rebooted the PC again, this time deleting my altered AUTOEXEC.BAT and putting the unaltered one I saved earlier in its place, and restarted. The security came back up, just like it was supposed to. I could now turn the security off, do what I wanted, then turn it back on, and no one would be the wiser!

I hurriedly showed my friend what I did, and he gave me a pat on the shoulder, and told me something that would stick with me for the rest of my life, something that I will never forget.

"If you give a man a fish, he will eat for a day. If you teach a man how to fish, he will eat for a lifetime."

It was then that I realized that not only was hacking something that I could indeed do, but also that I had already done it prior to this feat. What I had just done, finding out on my own how to disable the security and re-enable it, was exactly

what I did when I was a child, when I found out on my own how to view the code of the Jumpman video game. I embraced my curiosity, and never stopped learning and teaching myself how to do things until the task was done.

That is what hacking is to me - having a curiosity that you embrace, and using that curiosity to fuel your need to learn and accomplish a task, no matter how impossible it may seem. It need not even apply to computers - it can literally apply to anything.

I just turned 28 years old last month, and have never felt happier and more accomplished with myself and my life. And the main reason for that is because the hacker mindset has been ingrained so deeply into my very existence that I know there is absolutely nothing I cannot accomplish, no obstacle I cannot surpass, and no problem I cannot solve. Knowing that I can overcome anything life throws at me, one way or another, gives me the confidence to throw all of the sorrow and pain that often comes with the problems of life away, and focus on the positive. Trusting my instincts, questioning everything, and staying true to myself are what carry me through life's hurdles. And before I knew what hacking was, I did not realize I even had this power.

And implementing the hacker mindset is not only for a select few. Anyone can do it. As I said previously, and as many other hackers have said before me, hacking need not be applied only to computers and technology. Whatever your passions in life are, you can apply the hacker mindset to them. Maybe you like cooking, and experiment with different recipes that nobody has ever come up with before. That's hacking. Perhaps you like playing card games, and you came up with a game no one has ever played before. That's hacking. Perhaps you are into woodworking, and constantly use your skills to craft new types of structures or items that can be useful in everyday life, or solve a task in a way that no one ever thought of before. You hack every time you do that. Or maybe you are just a normal person, with a normal 9-5 job, who throughout your monotonous day, comes up with different little things to do or try to make the day go by faster and retain your sanity, while not impeding on your job performance. That's an awesome hack! These are just examples, there are many, many more ways to apply the hacker mindset to your life, no matter who you are or what you do.

As undefined as the actual term "hacker" may be, the hacker mindset is something that can be understood and applied by anyone. And that is what I choose to focus on.

*Synysr is currently enjoying life, working on a computer helpdesk in Michigan. He is in the process of planning his most elaborate hack - hacking himself.*



# CYA Using a Pi to Pivot

by 0rbytal  
0rbytal@burntmail.com

This article explores one method to cover your tracks online (I haven't actually tried this), and is for educational/informational purposes only. As with every decision you make in life, if you decide to use this information for nefarious purposes, be prepared to face the (likely negative) consequences.

If you're not familiar with the Raspberry Pi, you've been missing out on a trending piece of hacker hardware! The Raspberry Pi is a computer about the size of a credit card that runs an ARM processor and has exposed general purpose input/output ports, HDMI video output, SD card slot (used to load the OS), two USB 2.0 ports, and a standard LAN port - all for around \$35. Once you install Raspbian, PwnPi, Arch, or some other Linux distribution onto your SD card, the Pi boots from the SD card (which also doubles as the "hard drive" for the system).

I only suggest getting the Raspberry Pi because it's the most affordable portable computer, and I have one. The technique detailed in this article could just as easily be implemented using a BeagleBone, Parallella, or other super-portable computer. Since I do not own one of the others, it is up to you to apply this technique to your own configuration.

One of the most important steps in penetration testing and remote exploration is to *Cover Your Tracks*. If your activity is traced, you don't want the trail to lead back to you. For this reason, many explorers base their operations from a free/open Wi-Fi spot or Internet cafe. However, a cunning (or lazy) digital explorer would prefer to stay at home but make their activity *look* like it's coming from somewhere else. This method is called "pivoting," using an intermediate system as a conduit through which all activity is transmitted and received. Any hacker familiar with the Metasploit Framework understands pivoting, and prefers to pivot to cloak their activity behind another source.

Because the Raspberry Pi can run on Linux and be powered by any source with a micro-USB adapter, a creative hacker could design an inconspicuous case for his Pi and stash it somewhere that might be easily overlooked, or never discovered! So, here's how I might pull off a Pi-Pivot *if* I were to try it....

*Step 1:* Identify an open Wi-Fi connection, or a Wi-Fi access point (AP) "secured" with WEP (because it's *ridiculously* easy to crack).

*Step 2:* Register a free No-IP account ([www.noip.com](http://www.noip.com)), or some other dynamic DNS provider that can resolve my registered sub-domain name to my dynamic IP address.

*Step 3:* Set up PwnPi (like BackTrack for Raspberry Pi) or Kali Linux on my Raspberry Pi. Write a script that automatically connects to the Wi-Fi AP (identified in Step 1), then every five minutes tries to connect to my No-IP sub-domain name (registered in Step 2) on some high port number that I'll remember. By having the Pi call *out* to us, we don't have to worry about breaching the firewall to the Wi-Fi AP. The Pi would be pushing a remote shell script to my system prompting me to enter a password. This way, if the Pi is ever scanned and the open port is discovered, the curious port-scanner would have to know the password to get the shell.

*Step 4:* Set up a listener on my home system and port forwarding on my router to direct the traffic (on the port chosen in Step 3) to my listening system.

*Step 5:* Travel to the Wi-Fi AP (identified in Step 1) and find an inconspicuous place to leave the Pi so it is highly unlikely to be discovered... like sitting atop a ceiling tile. If there was no outlet nearby to power the Pi, I'd bring some sort of battery pack with a micro-USB adapter to supply the power for my clandestine PiPivot. *Turn on the Pi and leave it.*

Once the Pi Pivot connects to the Wi-Fi AP, it calls out to the No-IP sub-domain name I registered (e.g. [pivotpi.no-ip.biz](http://pivotpi.no-ip.biz)), shoveling a shell to my home system that is listening for the

connection on the high-numbered port. Upon successful connection to my home system, I enter the password, and I'm given a shell to my Pi to be used as a pivot. Now all of my exploration looks like it's coming from the Raspberry Pi hidden somewhere near the Wi-Fi AP.

*Tracks are now covered.*

Things to keep in mind about implementing this:

- You should be willing to sacrifice this Pi. You can't expect to *always* retain access to this Pi once it is hidden.
- If you power your Pi with a battery, your

connection is only good until the battery dies.

- Your pivot is only available if the Wi-Fi AP configuration stays the same. If the SSID changes, or the AP owner decides to secure it with WPA2, your pivot is down until you can regain physical access to it.
- If your Pi is discovered, it's possible that your activities *could* be traced back to you if you haven't thoroughly covered your tracks on it as well!

Go get a Raspberry Pi, explore it, share your results, and Hack *All* The Things!



## PRETTY GOOD PRIVACY

by Klaatu

Not that it probably came as much of a surprise to most regular 2600 readers, but the revelations that the NSA has been monitoring nearly all Internet communications with the acquiescence of some of the largest and most popular service providers does reinforce the importance of encrypting web traffic.

Obviously there are no guarantees with any method of encryption; any encryption could theoretically be broken. However, using the OpenPGP protocol to encrypt files and emails can be made basically transparent to the user, so there's hardly an argument against using it since, at worst, it adds at least a temporary layer of obfuscation to online communication.

### History of OpenPGP

The back story of OpenPGP is well documented online, but here's a brief summary. Phil Zimmerman developed PGP and distributed it amongst friends so that they could encrypt communication. Once PGP left the U.S. borders, Zimmerman was accused of exporting munitions and was brought to trial by the U.S. government. He won the battle in the end, and PGP itself has since been owned by a few different corporations and has also become an open standard.

The theory of OpenPGP involves key pairs. Each party involved in communication has a public and a private key. Each message is encrypted using the sender's private and the

recipient's public keys, and then decrypted using the recipient's private and the sender's public key.

It might help to think of it in simplified algebra.

For instance, a very simple formula such as:

$$x + 2 = y + 1$$

is fairly easily solved, or at least it is easy to iterate through many possible solutions. However, a more complex example such as:

$$\begin{aligned} &(\text{private\_x} * 2) * e = \\ &\rightarrow (\text{private\_y} / 4) * e \end{aligned}$$

is quite a lot more difficult and, in fact, mostly impossible without at least one of the private values.

The actual algorithm for OpenPGP would be quite a bit more complex with far longer numbers involved.

The most common implementation of OpenPGP is GnuPG (Gnu Privacy Guard). This is available built-in on Linux, and is freely downloadable for Windows and OS X.n

### Basics of GnuPG

Once you have installed GPG, you must create a key pair for yourself. There are probably GUI programs to help with this, but it is easily done via a UNIX or UNIX-like shell (such as Cygwin or PowerShell on Windows). This article provides instructions for Bash or zsh.

In a UNIX terminal, type this:

```
gpg --gen-key
```

A text menu pops up, giving you a choice

of encryption methods, and how many bits you want your key to use. The defaults are always safe.

You then must choose if and when you'd like this key to expire. The default is Never (0) and, for personal use, that's probably what you want. Confirm all of your choices, and then assign a user, email address, and an optional comment to that key. GPG prompts you for each of these, so enter the email account information you wish to use with this key.

Once your key pair is generated, you can try a test encryption. Since you have no one else's public key incorporated into GPG yet, this test will encrypt and decrypt a simple message for yourself:

```
echo "hello world" | gpg
➔ --encrypt > ~/hello.gpg
```

Now a fully encrypted file called hello.gpg exists on your hard drive. Were you to attempt to open the file, you would see naught but gibberish.

To decrypt it:

```
gpg --decrypt ~/hello.gpg
```

These examples have used GPG directly. You are free to do this for files or even tarred and zipped directories as an alternative to something like TrueCrypt, and on Linux most of the popular file managers feature full GPG integration so that when you attempt to open an encrypted file, you will be prompted for your key passphrase. Likewise, for email, it's usually convenient to let your email client do the work. There may be PGP plug-ins for the email client of your choice. This article covers Enigmail, a plugin for Thunderbird.

### Distributing Public Keys

Before you can encrypt an email message for someone, you must import their public key and they, in turn, must have access to yours. The easiest way to distribute your public key is to send it to a keyserver.

First, determine your key's ID:

```
gpg --list-keys | grep pub
```

This returns, for example:

```
1024D/BC9AE666 2009-09-11
```

The number following the slash is your key ID.

Push it to a key server thusly:

```
gpg --send-keys --keyserver keys
➔ .fedoraproject.org BC9AE666
```

There are many key servers on the Internet and they regularly duplicate one another's list of keys, so you need only to pick one at random and use it. keys.fedoraproject.org is

as good as any other, but there are lists online.

To import someone else's key into your own GPG keychain, use the search function of GPG. You can search by name or email address.

```
gpg --search-keys klaatu
```

This will return a list of keys that seem to match your search; import the one that you feel is appropriate.

### Encrypting Email

Using GPG with Thunderbird is made possible by the Enigmail add-on. Install the Enigmail add-on via Thunderbird's Add-On menu option.

Once Enigmail is installed, your Thunderbird client will have a new menu option for OpenPGP, and a new button or two. If you are averse to the shell-based interface of GPG, the openPGP menu allows you to do most everything already covered in this article. Assuming you have already generated your keys, however, all you need to do to set up Enigmail is to confirm your key via OpenPGP Menu > Key Management. Once this exists, you can either sign or encrypt (or both) your emails any time you enter an email address that matches a public key contained in your GPG keychain.

When composing a new email, use the OpenPGP button to tell Thunderbird to sign (use your key as a digital signature) or encrypt your message. The default behavior for this can be set in the Preferences submenu of the OpenPGP menu.

When encrypting email, you will be prompted for your GPG password. This gives Enigmail access to your private key for the encryption process, and then sends a fully encrypted message to the recipient. If someone responds to your email with an encrypted message, Enigmail will automatically detect the need for decryption and display the message for you.

### Encrypt All the Things

Increasing the usage of encryption for even casual, everyday communication will also help draw less attention to the traffic that, for whatever reason, needs to be encrypted. It just reduces the signal-to-noise ratio, making the pool of information murkier for anyone trying to take an uninvited sample.

*Note: For any readers in Pittsburgh: I am attempting to revitalize the 2600 meetings. Check the meeting list in the back of this issue for time and location.*



# Hacking Your Mother Tongue to Obfuscate your Encryption

by Israel

When most of us in this day and age think about encryption, we think of complicated mathematical algorithms to hide data. When we think of breaking decryption, most would probably think of brute-force programs and clusters of high-powered computers. This was not always the case until the computer generation came along, as encryption dates back to the time of Caesar. In the not-so-distant past, people broke encryption with nothing but pen, paper, and their heads.

In the case of the English language, there are hints that may allow someone breaking encryption to get an advantage. For older or simpler encryption, the first thing you would be looking for is the character that occurs the most. This would be the letter "e". The letter "e" occurs more frequently than any other letter in the entire English language and it's very easy to see why. Take into consideration the following words:

1. Me
2. Meet
3. Met
4. Close

Here are four common examples of how the letter "e" is usually used. In Example 1, there is the hard "e" sound. In Example 2, there is the hard "e" sound again, but used with double "ee". In Example 3, we have the soft "e" sound. In Example 4, the "e" is silent and does not make any sound. The letter "e" kind of runs rampant in English when you really think about it.

Before I proceed, please do not feel intimidated by what I'm about to suggest. I am not asking you to learn Russian fluently, nor any other language. Sadly, I myself am not fluent in anything besides English. We are merely going to talk about some of the concepts of Russian as examples to use in obfuscation. Did you know that in Russian schools there are no spelling classes for any of the grades? Imagine what we could have learned during the time wasted in an hour of spelling everyday. The reason behind this is that in Russian, everything sounds exactly

as it is spelled. The Russian alphabet uses 33 characters, whereas the English alphabet uses 26. Quick searches online can show you how their alphabet can easily translate English words. With one site, I found I was able to start using their symbols to read English words in about 20 minutes.<sup>1</sup> However, the sentence structure of Russian is very different than English. For example, this sentence in English: This is a very old table.

Would translate to the following in Russian: This old table.

If we combined the English sentence structure with the characters of Russian, we can add a level of obscurity to anyone trying to break our code. If a cracker was able to deduce we were using a Russian alphabet, they would most likely assume we would be speaking Russian as well. However, let's try to take this further.

So if we were to take the phrase "This is the message" and translate it to Russian we would end up with Это сообщение which literally says "This message". However, this is not what we get when translating the English letters to Cyrillic. Instead we end up with Тхис ис тэ мессаге. This phrase roughly translates back to "This study the message". Where did study come from? This is what is known as getting lost in translation. From the standpoint of obfuscation, this can be an advantage. Also, note how these phrases all look totally different from each other:

Это сообщение (Real Russian)

Тхис ис тэ мессаге (English with Cyrillic)

This is the message (English Plain-text)

We have taken what would be two words in Russian and made them four. The number of words would most likely be irrelevant as many encryption schemes will leave no empty spaces between characters. Yet the real Russian phrase was 12 characters. Our obfuscated phrase came to have 15 and the original phrase "This is the message" has 16. While this is not a lot of difference, you can see how over a long amount of text this would greatly differ from the English or Russian versions of the plain-text.

In Russian, there are other characters we can use such as the symbols Ъ and Ь. These denote if the hard sound or soft sound is going to be used with the letter following them. So ЪА would be the hard “a” sound and ЬА would be the soft “a”. If we represented these two sounds as numbers, we would most likely have them as two completely unique numbers and grow our alphabet even further. In order to do this with mathematical algorithms later we would probably be changing any characters into numbers anyway for computation. Essentially, we could make each unique phonetic sound represented by its own number. We could also change this by using one number to represent double-constants such as the “Fr” in Frank or the “rk” in Mark. This simultaneous inflation and deflation of the number of characters used would add more complexity as well.

I leave this as an exercise to the reader to create their own language hybrids. Imagine something like the Chinese characters where whole words may be represented as one character. I would love to see this added to something like the Spanish sentence structure where the verb of the sentence comes first. You may even think of much better anomalies than I did!

After we have encoded all of our newly plain-text into our Cyrillic obfuscated text and then to numbers, we can proceed with real algorithms and modern cryptography. I would like to show how this can be applied to modern cryptography, but the encryption laws in my country are rather strict when it comes to out of the country exportation. On the other side of

the coin, readers in some parts of the world have very strict laws on the importation of encryption as well. While I see punishment for sharing what I have created for myself a gross violation of free speech, I do not wish to endanger others because of my protest without their consent. I would rather take this time to encourage people across the world to speak your voice and demand freedom to express and share your own ideas. I fear that one day soon, encrypted text may be the only freedom of speech or right to privacy we have left.

For those who may be in doubt of the effectiveness of this, let’s observe history. During the Second World War, the United States did not use encryption in the usual sense. They transmitted their communications using the Navajo Indians’ native language.<sup>2</sup> The Nazis intercepted these communications and assumed this was English that had been encoded. Code crackers worked hard for a decryption key that would never be found because it didn’t exist. This illustrates the point that language is powerful! It can change minds and can even win wars.

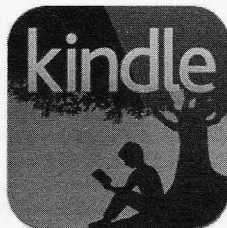
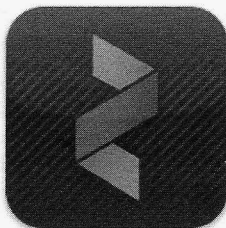
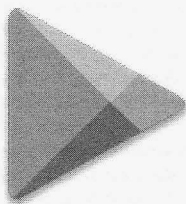
In closing, all English speakers may not be familiar with the phrase “mother tongue” in the title. This simply means the first language you learned. I only know this phrase due to someone running a scam that kept spamming my work. May they live long and prosper.

<sup>1</sup> <http://www.dorogadomoj.com/se03>

↳abv.html

<sup>2</sup> <https://en.wikipedia.org/wiki/>

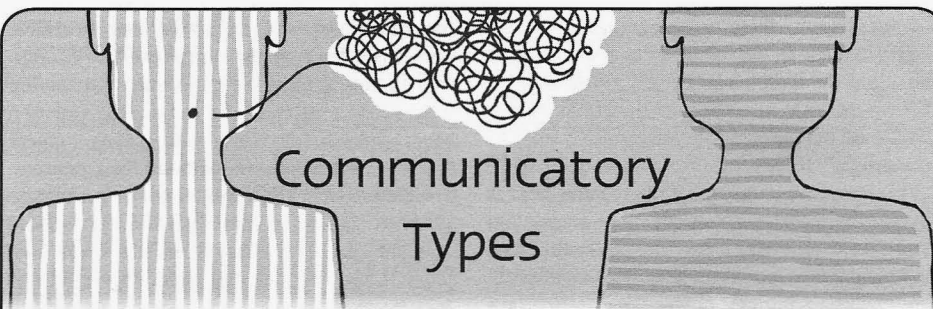
↳Code\_talker#Use\_of\_Navajo



There have never been so many ways to get copies of 2600!

In addition to the good old-fashioned paper version, you can now subscribe via Google Play, Zinio, and the Kindle. We're also increasing our library of back issues and Hacker Digests.

**Head to [digital.2600.com](http://digital.2600.com) for the latest**



# Communicatory Types

## Queries

**Dear 2600:**

My company would like to post my article in full on our corporate blog. Is this OK, now that the article has been printed in 2600?

I searched 2600.com for information regarding this matter, but found none. I vaguely remember reading somewhere that it's OK to reprint an article after it has been published, but I don't recall where, so I wanted to ask for permission to republish explicitly.

If we may republish, we will be happy to link to 2600.com, the magazine on Amazon, etc., at your preference.

As an aside, I've got other important business to address with the lot of you: now that I've been published, how do I receive my t-shirt? (I'd take the one-year subscription, but I already buy all of the issues anyway.) It's important for the kids at my Hackerspace to know that I'm an uber 1337 h4x0r.

I'm working on another open-source security project at the moment, and hope to submit another article within the next few months to introduce it as well.

Thanks for your help, and for the work that you do.

**Chris**

*You have the right to do whatever you want with your article, including putting it online, broadcasting it through a megaphone, or handing it to a politician to use in a future filibuster. As a 2600 article, it may also appear in a future collection. We appreciate the offer to link to us - our general website address is fine.*

*As for getting the shirt you're owed, you no doubt have been contacted already. The way it works is that sometime after an article or photo is published, the author is emailed with a request for their info so the item(s) can be sent.*

**Dear 2600:**

I'd like to ask you if you are interested in publishing an article about our latest discovery - we successfully exploited NFC MIFARE Ultralight tickets in order to gain free rides on our local transport system. This should also work on any worldwide transport system that has not fixed it yet.

**bughardy**

*This is exactly the sort of thing we're interested in. We believe such info has been presented at various hacker conventions, but nothing beats a printed*

*article insofar as reaching the greatest number of people and lasting forever. We find that nothing causes panic in the corporate world as much as a printed release that can't be deleted or taken down.*

**Dear 2600:**

I am part of the global team of hackers called White Hat Alliance. Our hacking group helps companies to protect themselves against malicious hackers.

Would it be possible to have an article on 2600.com? Is that possible? What actions are required from us to proceed with the article?

**Damien**

*We suspect since you refer to our website and not our magazine that you're looking for an article about your organization to appear on our site. That's not something we do. If, on the other hand, you're looking to write an article for the magazine, it's as simple as emailing articles@2600.com with your submission.*

**Dear 2600:**

Do you want a free root shell on my server? (No strings attached.)

-----BEGIN PGP MESSAGE-----

Version: SecuMail 2.4

-----END PGP MESSAGE-----

**Michael**

*We really didn't need a free root shell - thanks - but, once again, this illustrates the problem we have with those who insist on sending encrypted messages. The key used here was not one we control, so we had no way of reading whatever was contained. While PGP works great when used properly, we don't have the time to go back and forth multiple times to figure out what's causing the communication problem, only to finally get a letter that is completely innocuous and ultimately intended to be seen by many thousands in print. Don't get us wrong - we believe everything should be encrypted by default. But until we can ensure that people only use the right key when communicating with us, it's simply not worth the effort. What we would like to do is wipe out every existing key that claims to be affiliated with 2600 and start fresh so that there's no confusion. Right now, that doesn't seem to be possible, which results in people using keys that we have no control over, which means unread messages. We really hope a better system is in place soon. Incidentally, on those occasions when we're corresponding with people we already know who have sensitive*

*info to convey to us, we create a key just for that purpose and discard it afterwards. Even then, there are invariably problems, but it gets the job done. One day soon, we hope it's that easy for everyone.*

**Dear 2600:**

In the 30:2 issue there is an article entitled "How a Prehistoric Hacker Got Started" by DarkAudax, which is a very good article. Only one problem with it: I believe years ago this same article appeared in 2600 and I was wondering how many times can someone submit a article they wrote and get it published?

**Anonymous**

*Only once. People who submit the same article multiple times wind up being ignored permanently. And, unless we make a horrific mistake, an article only appears once. We searched our entire catalog and didn't see this article anywhere other than the issue you cite. Thanks for scaring the crap out of us.*

**Dear 2600:**

Hello, are you a hacker? I need somebody who is great and sneaky. If you have this skill, please contact/email me as soon as you see this message. The cause of this letter is I was hacked by PayPal a certain amount, so I want that amount back in the most secure way. Please reply to this as soon as possible if you are a sneaky and great hacker.

No money will be sent - not unless the hack is done - due to me being completely broke so please have mercy upon us. Thank you for your concern.

**Nam**

*Well, you are most certainly somebody who knows how to get things done. You say PayPal "hacked" you and, clearly, the appropriate response is to bring in a complete stranger (a sneaky one, at that) who will get it all back for you. How could it be any simpler? And we're impressed by the fact that you know not to send such a sneaky stranger money in advance to pull off this job. You have done your homework in the ways of the world. Because we are so enamored, we've decided to take on the job gratis. You should see your PayPal balance restored. If not, keep refreshing your screen, at least once every ten seconds. Don't stop or a hacker might grab it from under you.*

*And that, dear readers, is how you keep someone busy so they don't hurt themselves.*

**Dear 2600:**

Recently I purchased a book called 2600. I found this to be very interesting and it piqued my interest in learning more about hacking. I now have a subscription to 2600 and read your quarterly publication electronically. I am in my 70s (old fart/alter cocker). I enjoy investigating and learning new things. Living in a rural community, I would like to know about meeting members of the hacking community and learning more.

My technical knowledge is not as in depth as many of your contributors, and about half the time I get lost in the articles and have to read them twice so as to have an idea of what is being stated. I agree with many hackers and value privacy which is the reason I use this mail server and others along with

Hide My IP and Tor. I would appreciate your ideas etc. on how to meet others in the hacking community to expand my interest, computer literacy, and knowledge.

Keep up the excellent work you are doing. I am looking forward to hearing from you shortly.

**Auggy**

*First off, don't feel at all bad or inferior if you believe you're not as technically adept as others. It only means you have another perspective to offer. And those who are extremely proficient in a field will always know of someone with more skills. It's how we all interact with each other that determines what, if any, forward progress we make.*

*Clearly, the best way to meet people is to go to one of our monthly meetings. As you didn't specify where you are, it's hard to recommend one in particular, but a full listing can be found in the back of this issue in microscopic print. And you don't have to be in your 70s to complain about that.*

**Dear 2600:**

Did you get my previous email? Would be happy to hear from you.

Thanks.

**Damien**

*You again. We thought something like this might happen. When people ask about publishing on our website, we wonder if they even know that there's a magazine attached to all of this. And when they get an auto-reply from our letters department thanking them for writing us a letter, they often assume they're talking to a human who types very fast. It doesn't really matter how clear we make the instructions, as the dialogue will just continue into infinity. The short answer here is: you have already heard from us and if you read what our computer wrote back to you, it would all become very clear. We hope, but hardly expect, that this will be the end of it.*

**Dear 2600:**

Is there an easy way to listen to your program if I missed it? I looked at the info online, and all I got was really, really confused.

**Ruth**

*While it may make sense to us, it's always possible that it's not so obvious to others. This is a truth we wish more software developers realized. On the main 2600.com site, simply click on the "Radio" section, then select the show you're interested in. From there you can go to the "New Show" section, which we assume is what you're looking for. At that point, depending on your system, connection speed, etc., you should select whether you want the high fidelity (128k) or low fidelity (16k) version, as well as if you want to download a copy to have on your own computer or stream it over the net. If you don't know which is best, just try each of the four options until you find one that works for you. Your machine should have a program to play audio files and, if you download one of the shows, your browser should tell you where it is so you can open it. Good luck.*

**Dear 2600:**

I haven't had a 2600 subscription in a long time. Just wanna know if it's okay to use some covers of



past issues of 2600 in a movie I am planning. Do I have your permission?

**Derneval**

*We don't know how you'll see this if you don't check the magazine but, yes, we grant permission to virtually anybody who wants to use our material in such projects, commercial or independent. We wish Hollywood producers would take a chill pill and not send us forms that they expect us to get notarized so that their asses are covered for having a 2600 cap on someone's head in a TV show. Just go ahead and use whatever you want, just as you should be able to use anyone's shirt or magazine cover in a production. The other thing that really bugs us is when these same people won't even buy the items they want permission to use in their multi-million dollar production. We'll probably never understand the entertainment industry.*

**Dear 2600:**

I have sent you email few days ago. Did you receive it?

Thanks.

**Damien**

*Wow. If we wanted to reply, surely we would have by now. But perhaps sending us a reminder every couple of days is what will eventually win us over. Keep trying.*

**Dear 2600:**

You guys still accepting Hacker Perspective submissions? I have a great idea.

**herp derp**

*They're closed at the moment but we suggest writing your submission while it's in your head and sending it in when we announce their reopening sometime in the future. Just make sure it's at least 2500 words and focuses on your story, what makes you a hacker, and what the hacker culture means to you. Don't send it in before the submission period opens again as it could easily be misplaced.*

**Dear 2600:**

I'm an author working on a new novel (my eighth) that features a hacker. While he isn't a prominent character, he does feature into a bit of the storyline and I would very much like to get his voice right. I'm wondering if there is someone at 2600 who might be willing to answer a few questions (in email format) to help with authenticity.

**Danielle**

*Please don't take it personally that we have no time to help people with books, stories, and movies while we're putting out a magazine, which is pretty much always. This is not the only such request we've received - this week. Perhaps we could start a consulting firm, but that doesn't solve the problem of having to clone ourselves in order to find the time.*

**Dear 2600:**

Would appreciate the update.

Thanks.

**Damien**

*And then there's this guy. He never lets up. Is this how you do system penetration tests, by relentlessly pounding away until you find a weak point? It's actually quite effective, as some of us want to*

*take the time to compose and send you a detailed response, while others just want to link our website to yours and be done with it. Another week of this and we would be completely and hopelessly divided. In the end, there's really only one thing we can do.*  
[Firewall Installed]

**Dear 2600:**

I was just wondering, not so much about the technical content, but about the tone and style, etiquette, so to speak, of your considerations for writing submissions. Is there any standard(s) of style anywhere that you follow? Just wondering. Thanks a lot.

**Daniel**

*We want you to use the style you're most comfortable with. Just remember to approach your subject matter from the perspective of a hacker and most any topic will become relevant and interesting.*

**Dear 2600:**

Hello, I was inquiring if you can hack a website for me and get me the admin access. I will be paying for your services. Thanks you.

**Yahia**

*Someone, somewhere has been spreading this image of us throughout the planet and we've been getting such requests on a regular basis for decades, since even before websites existed. We've never asked for this, implied that this is what we do, or voiced anything other than disdain for the type of people who think they can pay hackers to break into sites for them. Can you imagine how many requests we would have gotten had we expressed any interest at all in this sort of thing? The money we could have made? The fame, the notoriety?*

*Suddenly, at 30 years of age, we realize how foolish we've been....*

*Yahia, expect our call.*

## **Additional Info**

**Dear 2600:**

Not looking for a t-shirt or anything like that, but thought you would be interested in this collection of phone booths published in the *San Francisco Chronicle* on August 8, 2013.

**jim**

*Thanks for the tip and, for our readers, searching for the above online will quickly take you to that collection. But why would you not be looking for a t-shirt? We just assume everyone is.*

**Dear 2600:**

I hope this note finds you well. I was in Wildwood, New Jersey on the night of August 4th looking for a slice of pizza. While walking down the boardwalk, I scored this shot. Computer geeks like pizza.

Happy Trails.

**Larry**

*This happens more times than we can count and it's so very frustrating. People think they're sending us really cool stuff but forget to include the attachment! Don't let this happen to you. Or to us.*

**Dear 2600:**

Pays off to be a geek! Thinking of you!

**Rachiee**

*We assume there was more to this message, too.*

**Dear 2600:**

As an old Minuteman missileer myself, I was particularly interested in the article in your Summer 2013 issue entitled "Fun with the Minuteman III Weapon System." It's certainly true that outer zone security alarms can be triggered by a variety of inconsequential things: birds, squirrels, gophers, hail, blizzards, and random UFO flyovers. It's also true that Alarm Response Teams may take their sweet time in responding to outer zone alarms. By the time they arrive on site, the perpetrating bird or rodent is long gone. This makes for a boring and unexciting trip. Still, a coordinated effort to keep the outer zone alarm lights going off throughout the missile field would soon become apparent to those monitoring things from the launch control centers. Such widespread and recurring alarms might incentivize the team to make a more spirited effort. Alarm response teams, already fatigued and bored from chasing down birds and squirrels, would no doubt welcome a chance to use their training to apprehend, spread-eagle, and handcuff actual human beings. As it is, they only manage to apprehend the occasional aging nun or elderly peace activist. Admittedly, my knowledge is somewhat outdated, but I also question whether hitting the 110 ton launcher closure lid at the center of the missile site with snowballs or ice cubes would be sufficient to cause an inner zone security alarm.

One might stay on site long enough to work at causing an inner zone alarm, but that is a more difficult endeavor and carries its own risks. In sum, I recommend following the author's advice: "Now for some real fun. Do not do this."

**Capt. Jay**

**Dear 2600:**

127.0.0.1 localhost  
216.218.239.164 google.com  
216.218.239.164 www.google.com  
Just thought I'd help spread the word.

**rixter**

*We suppose every little bit helps. That first one belongs to our internal network and we're now paranoid as hell wondering how you figured it out.*

**Dear 2600:**

I have listened to the Dish Network channel 144 clip referenced by reader Jim in 30:3, and the Morse code message is:

WQ35 13013443 860 585 2289 ESPN2

repeated over and over. The beginning is garbled and, in the noise, the starting and ending elements may be shifted from the original, but the sequence repeats in the order shown.

If you ever need any additional Morse analysis, I'd be happy to help. Ham radio contester since 1966.

**KSTA**

*Just further proof that there's no puzzle our readers can't get to the bottom of.*

**Winter 2013-2014**

**Dear 2600:**

In light of Verizon and AT&T's recent antics in the media regarding POTS and DSL, I thought I might say a word about the phone network as we know it. Strange as it might seem, the current generation of voice switches are a lot more interesting than you might think - much to the point where you can tell what kind of equipment you're calling (and, to a much lesser degree, what long distance network you're using) just by listening to the sound of ring-back from it. There's a quick recording of a bunch at <http://ge.tt/7TmPVKv/v/0> if you'd like to try it for yourself. The difference is subtle, so be sure to wear headphones. The order of the equipment is DMS-10, DMS-100, DCO, GTD-5, SESS, and EWSD.

There are a couple of other things I'll mention later but, more to the point, why is VoIP or wireless such a bad thing compared to the traditional network? Performance and efficiency. IP over ATM, for example, has an overhead of about 9.4 percent according to [http://pflog.net/dsl\\_overhead/](http://pflog.net/dsl_overhead/). This seems to drive most of the ISP people I've talked to absolutely nuts. But a SIP call by contrast will take up roughly 110 kbps for a call using uLaw. This would normally fit into a 64 kbps circuit - that's 46 kbps (or 71 percent) overhead per call. Packet loss in and of itself is a whole other topic, but latency is one of the issues that tends to be overlooked. Latency on Voice over IP calls can get to be 150 milliseconds, according to an ITU recommendation, anyway. I encourage you to measure what it actually is in practice. That's something we haven't considered acceptable for most domestic traffic since the days of dial-up! By contrast, an all circuit switched call rarely exceeds 30 milliseconds of latency from one end of the country to the next.

As for wireless, the problem resides mostly within the codec. All major wireless standards rely on a method of compression called Code Excitation Linear Prediction to achieve very aggressive compression ratios at the expense of adding a characteristic "underwater" quality. To put it in perspective, Verizon Wireless uses the 4 kbps bitrate of EVRC-B, which employs a vocoder along with CELP techniques, so what you end up hearing is closer to T-Pain's autotune effect than the person you're speaking to. Sprint, AT&T, and T-Mobile (using 8.55 kbps EVRC-B, 6 kbps AMR, and 12 kbps AMR, respectively) don't tend to be much better. Even the coming voice over LTE with its promises of better sound quality relies on just a wideband version of AMR.

"But who cares?" you might ask. Maybe you can live with crappy sound quality so long as you understand who you're talking to. That's fine, but consider this: much of the speculation around the interception technologies of our good friends at the NSA seems to indicate that to feasibly intercept and store *all* PSTN traffic, they'd need to be archiving it with similarly aggressive compression. I know this isn't concrete evidence, but if you've ever heard a 911 call when it's released to the media, it's always through something that uses a linear predictive

**Page 37**

model, and some independent research from another phreak seems to suggest CALEA voice intercepts do the exact same thing. So it's certainly not out of the question.

If it's true, the flexibility of uLaw can give us a strong advantage; a layer of obscurity can be added to whatever encrypts your call. It could be analog voice scrambling, a made up implementation of 8PSK with obscured trellis modulation, morse code tapped into a song using a notch filter, whatever. As of right now, the aggressive compression makes this difficult, if not impossible to properly log; there's no packet format you're necessarily limited to.

Anyway, getting back to the phreaking aspect of it, the DMS-100 (which is a bit of a marvel within itself - its current generation of hardware revolves around a redundant pair of Motorola 88k CPUs of all things, and manages to process about 1,500,000 calls in an hour) can give a good demonstration of some of the things the network hides. At first glance, 212-346-9922 is a ringing number. If you're using a phone that speaks uLaw and passes network audio before the call answers, you'll probably know from the sound clips that it's a ringing number on a DMS. While it's ringing, go ahead and make a call to it from another phone. The calls should both go off hook, and you'll be bridged together! Nice, right? These bridges tend to be all over the place, and will hold a good number of callers.

Now, if you happen to be calling from a POTS line, there's also a lot of stuff that only you can reach. For example, 958 and your last four digits will get the switch to run a ringback program in a lot of areas. In a lot of former Embarq areas (mostly Centurylink stuff that isn't ex-Baby Bells), 959-xxxx is an internal range that has all sorts of strange goodies; test numbers for IVRs, CNAM readback machines, and so on. It's like an ongoing episode of *Coast to Coast*, but with real machines instead of theoretical beings hiding stuff.

So - why am I telling you this? I don't expect you, or anyone, to run out and become a phone phreak tomorrow. I mean, the more the merrier, but 2013 alone has been a very, very strange time for any politically aware American. I just ask that in between the ever more revealing Snowden revelations; the ever more expanding articles of governments, companies, or trade acts pushing for Internet restrictions; and the ever more incessant whining of large carriers to regulators to get out of wired telecommunications altogether - voice, data, FTTP, and everything, please don't dismiss the phone network as "that garbly thing from yesterday that's probably a series of tubes now."

I can honestly say some of the best times I've had in my 23 years have been on the phone network. By writing this, I'm hoping you can eventually experience them too.

**Brandon**

*We're so happy to be hearing from people who can appreciate this sort of thing and who continue to give out interesting phone numbers to call, not to mention sharing an incredibly relevant perspective*

*on the changing phone network and how it relates to the surveillance society being constructed around us. This knowledge and analysis is at the very core of who we are as hackers.*

## Critical Observations

**Dear 2600:**

I find it somewhat ironic (and disturbingly hypocritical) that a group as concerned about technological privacy issues as you guys claim to be would not only put a search bar tied directly to Google, but also their own Javascript code on your web page (and a YouTube file, but that's something else entirely).

Could just be me, but wasn't Google one of the first parties to (unsurprisingly) be outed as a participant in the National Surveillance Authority's US-984XN (a.k.a. "PRISM") scandal a few months back? You do realize Google itself is basically a public-facing component of the NSA and that they're keeping records of every single word searched from your site, do you not? And isn't 2600 the very magazine wherein I regularly read articles detailing what a security and privacy hazard Google is? Wouldn't the anonymizing Google frontend Ix-quick or, by extension, Startpage have been a safer (and more logical) choice instead?

Just something to think about. I'll continue to read your magazine and get the radio programming from your FTP server, but I can no longer trust the safety or privacy of your HTTP site.

Thankfully you guys haven't strayed down the dark, twisty path to inescapable ruin known as Facebook. Let us hope that you never do.

**phreakin5ess**

*We actually do have a Facebook group, and it's filled with people who would never trust Facebook with anything truly private. Simply because there have been abuses and privacy violations attached to a particular service doesn't mean you need to go to great lengths to avoid any use of that service. We believe in diving in and figuring out what's really going on, in addition to figuring out new and better ways of using things to our advantage. This is best achieved through participation, especially when so many people are already using these systems without questioning any aspect of them. We can use the power of Google to educate people on what's wrong with it. What better way to teach Facebook users how to protect their privacy than to talk to them on Facebook? And just because you see a Google search bar on our page, it doesn't necessarily mean your privacy is being abused. It's how you interface with Google and what information you give through your browser that determines this. And you can use that very search bar to learn more from our site. We're not sure what YouTube file you're referring to - our page links to our YouTube channel (Channel2600), which is again a good way of reaching people already on that hugely popular resource. That really shouldn't cause you any grief. We're always open to alternative and additional services, but avoiding the ones that are in the mainstream will*

have no effect on them and prevent us from getting our stuff out there to the maximum degree.

**Dear 2600:**

I like the way the magazine encourages exploration. However, there remains one huge flaw on how articles are accepted. By requiring every article to never have been published before, article quality is affected.

The fact is that the content of an article appearing somewhere else does not mean 2600 can't have an original article based on that published content. With the Net giving us instant information, a three month delay for the print magazine is too long. And it doesn't take into account peer reviewed articles - for example, someone testing their research to see if it actually works. Simply put, the first publishing rights puts untested ideas in the trash.

I believe that 2600 should be like a scholarly journal. I see many of the articles in the magazine are political. I see this on many message boards. The message board is for science or computer graphics, then all the topics become political arguments. I think if you lift the first publishing rights, it would open the door for many technical articles.

Just a thought.

$5 * 17 = 85$

Prime Number + Prime Number = Product = N

$y = ((85/x) * 85 - x^2)/x = ((85^2/x) + x^2)/85$

$p = ((85/x) * 85 - x^2)/x * (85^2/((85^2/x) + x^2)) - 85;$

$\text{sol} = \text{NSolve}[p[0], x]$

$\{\{xR-86.893\}, \{xR-7.50438+19.0222 \ ?\}, \{xR-7.50438-19.0222 \ ?\}, xR16.9017\}\}$

**Bobby Joe**

*We honestly weren't sure if all of those equations were germane to your argument, so we left them in. To address the actual words, our policy certainly doesn't forbid articles based on content that's appeared elsewhere. We just don't want identical content that's available elsewhere. Neither do the vast majority of readers who have voiced an opinion on this. Just because we live in the "instant age" doesn't mean that a collection of articles that come out every three months can't contain fresh and unique ideas. Often we have peer review from our readers, resulting in more discussion in the letters section or additional articles in future issues. The fact that our material is original makes these dialogues all the more interesting.*

**Dear 2600:**

First, thanks for the work you do! I've been a silent fan for a long time, but I just couldn't be silent anymore!

I'm writing in response to Micah Lee's advocacy of leaving your home network open without having your neighbors do any extra work.

I advise against that at every opportunity. Consider the case if one of your neighbors is secretly into child porn. Do you really want your home's IP address associated with those search requests? (And I've seen network logs from ISPs before... not all such queries run through Tor/VPNs.) While it's true that a case against you would have to include physi-

cal evidence from your hard drive(s), why even take the risk?

Further, keeping your access point open also opens you to having your online identity stolen. As an attacker, I'd much rather have someone else's IP take the blame for my hack. Also, considering that research has shown that the vast majority of people improperly configure their routers in the first place (such as not changing the admin password), this just argues more firmly: thumbing your nose at AT&T or Cox isn't worth the risk. Lock your router down.

**XeNO**

**Dear 2600:**

I have a couple of bones to pick with your article ("The Right to Know," 30:3). First of all, you conveniently failed to mention that Julian Assange did not seek asylum because anyone was after him for his WikiLeaks reveals. In fact, his cowardice was directly due to the U.K. government potentially extraditing him to Sweden to face accusations of sexual assault. Now, maybe there were others behind the scenes lining up to nail this chickenshit for providing Manning a forum, but that is not the immediate threat that caused him to run and hide.

In your column, you paint him as this great crusader out to expose every government secret that the public should have the right to know. Unfortunately, all you did was make it seem like sexual assault has no importance in the grand scheme of things when compared to exposing the goings-on of governments, especially the U.S. government. That being a potential sexual predator is OK as long as you are "sticking it to the man," so to speak. My BS flag is waving full force!

Snowden is another coward. If he had such an objection to the work that was being done, all he had to do was quit. No one was holding a gun to his head making him do his job. He could have left any time he wanted to. But instead, he decided to violate every oath he signed his name to. There was nothing noble about that, especially in light of his running away like the little cowardly bitch that he is. His word means nothing and anyone or any other country that trusts his word from this point forward is foolish in the extreme.

Manning is the only one that comes out of this with any dignity. I do not condone what he did; again, he violated every oath he signed. However, at least he had the guts to face up to the consequences of his actions and, for that, he deserves recognition and my grudging admiration.

All I have for those other two slimy little weasels, Assange and Snowden, is contempt as should you.

**M. Piazza**

*We barely touched upon Assange in that editorial, simply making the point that the stories such journalists as he and Glen Greenwald reveal often get lost in character assassination. Your words help to prove that point.*

*We believe that any charges faced by Assange should be answered. But clearly, there is much more going on here than there would be for any-*



one else facing such charges. The presence of police surrounding the Ecuadorian Embassy in London around the clock has cost millions of dollars. Is this how someone wanted for questioning in another country, someone who didn't cause powerful governments so much grief would be treated? Meanwhile, the United States has steadfastly refused to give any guarantee that its forces would not grab Assange, either in England or in Sweden if he were to leave the embassy. With all we've learned and witnessed about our nation's behavior, whether it's drone attacks in foreign nations or invasion of its own citizens' privacy through the NSA, would anybody really be all that surprised if such an action against Assange were to be taken? With members of Congress calling for him to be hunted like a terrorist, we can almost see this as being expected and even seen by many as a good thing. We believe Assange would gladly go to Sweden, answer the charges, and even face prison if there was a guarantee that he would not be extradited to the United States. But it actually serves the interests of his detractors to have him remain isolated and seemingly ignoring the charges. Adding further evidence to this is the fact that Assange has said he wouldn't leave the embassy even if these charges are dropped because of the likelihood of the U.S. taking action against him. It's clear this is about a lot more than the criminal charges in Sweden. That is very different than saying those charges don't matter.

Calling Edward Snowden a coward makes absolutely no sense to us. What he did took tremendous conviction and he's made a huge sacrifice. To say he could have just quit misses the point entirely. He felt the world needed to know what the NSA, the United States government, and various corporations were doing. Maybe you believe that should have all remained a secret. Many people say the same thing. But what he did took a great amount of courage. It would have been so easy for him to walk away and let these things continue. But he didn't. And now we're all talking about it. If there's even going to be a chance of things changing in the years ahead, this is where that chance will have begun. And, if you look back through history at some of the greatest changes that have ever occurred, they often started with the courageous actions of a single person.

**Dear 2600:**

Dudest of the dudes....

You need to throw the 2600 Government Seal on a black hoodie so I can wear that shit every day. I've just about worn out all the 2600 shirts I own. Time to cover up the old with some new threads. It would be much appreciated!

**apocalyptic**

To the best of our recollection, that's the exact design of our very first sweatshirt, which is still quite popular. Perhaps you should look around store.2600.com in the clothing department?

**Statements**

**Dear 2600:**

Human rights trump freedom of religion any day!

**nealcamp**

Not really sure why you needed our letters section to make that point, but we're here to provide a forum and we're happy to oblige.

**Dear 2600:**

My address book was hacked. I did not write any message to you about my subscription. Thanks.

**Dan**

But you did write a letter that wound up in the magazine. These things happen for a reason.

**Dear 2600:**

Unofficially, NSA stands for Never Say Anything. Yet the public is told, "If you see something, say something."

**Potissimum Libertas**

**In Omnia Paratus**

**Justin**

Clearly, not everyone plays by the same rules. We have our own take on what the letters NSA stand for, insofar as what rights the people have granted them. See our new NSA shirt.

**Dear 2600:**

Just finished reading the Autumn issue (30:3) including the letter by the person who wanted clarification on the compensation for submissions and how article writers were getting less swag than they used to get from 2600.

I am a lifetime subscriber. In my opinion, people who write articles should get more than people who submit pictures. Writing coherent and well-constructed essays has become a lost art in our culture.

I am a reader, and I understand that not all people enjoy reading. What I don't understand is why people seem to go gaga whenever they see the numbers "2600" in an address, or on a street sign, or branded on a milk cow somewhere in middle America. And then they take a picture of it and send it in to 2600. And, for some reason, you publish them.

It reminds me of people who smoke marijuana (I am not knocking it) who always seem to get into a state of arousal whenever the number 420 is mentioned, or seen, or whatever.

I enjoy looking at the telephone pictures from far away places, but looking at them just reminds me that I can't afford to travel to Korea, or Zimbabwe, or wherever it is these exotic phones are discovered.

In closing, I think writing articles demands significantly more time, effort, organization, and mental focus than submitting a photograph. And therefore, I think that people who have articles printed should receive more swag than those who snap a picture, and then merely hit send.

Please excuse me now, it is time for our daily Two Minutes Hate meeting.

Thank you.

**Real Name**

**[please withhold my name]**

(That was a close call - we almost printed your real name since you signed it. For future reference,

*you can just omit your name before asking us to withhold it.) We understand your points, but we really don't want to be in the position of judging one item over another. Every article or photo takes varying degrees of time and skill and it would be a mistake to try and gauge how much actual effort each one took. That's not what we're about. We want to give back as much as we can and we'll be thrilled if we can give more in the future. Incidentally, we wholeheartedly agree on the need for coherent writers in our culture. That's why we're always so happy to get submissions from people who clearly enjoy writing.*

*Most importantly, is there any truth to our name being branded on a milk cow somewhere?*

**Dear 2600:**

It is not enough to lament the appalling misuse of the justice system that drove Aaron Swartz to his suicide. In all such cases, *identify* the assistant prosecutors, higher officials, and all who made the decisions, filed the scurrilous indictments, and exercised wrong and/or malicious judgment, to harass and destroy people like Aaron. If you don't *name and describe* the real culprits, they will continue to act with impunity in other cases like this.

**F.**

*We absolutely agree that the people behind malicious prosecutions should be identified and held responsible for their actions. That was certainly attempted in this case by many people, but, as expected, not by the ones making decisions. (We're not sure where you're going with wanting a description of these people, however.) Even if they are actually found to be accountable, it's not enough. There's a system at play which encourages this sort of dishonesty in prosecutions and that needs to be dismantled in addition, or the perpetrators will simply get better at protecting themselves and covering their tracks.*

## **On Meetings**

**Dear 2600:**

Hello, deeply kind and helpful 2600 administration. I am in the right time and place. First Friday, at a popular cafe in a popular university. 4 pm local time, as written at the magazine and online. I checked IRC around 3 pm - empty. They are surely rushing to be on time. Surely.

But no one else is here.

Please help me find the group. All I need is the Philippine organizer's email address.

Thank you, and I love your magazine.

**Lex**

*While giving up this information would prevent at least one of our readers from spending a lonely evening in a cafe all by himself, we have a far greater concern towards protecting the privacy of other readers. Of course, you could probably easily obtain this info on your own by talking to someone on the IRC channel you mentioned. You're as much an organizer of these meetings as anyone else, however. We suggest you make this an issue in your community so that people show up when they say*

*they're going to. The unpleasant reality is that we have to delist meetings with multiple reports of non-attendance.*

**Dear 2600:**

Yo. I finally went to a local 2600 meeting. I've wanted to for years, but the first Friday was always "busy" for me. Fuck that weak excuse. Went to Interlock in Rochester, New York and it was awesome. Quickest place I ever lost "new guy" feeling ever.

Did I feel dumb compared to most people in the room? Absolutely. Was that a problem? No. You are a hacker and you live to learn new things. Likely with a splash of really blunt or vulgar dialog, but that just means you love life.

Go to the meetings. You'll probably dig it.

**Pic00**

**Dear 2600:**

I have been a 2600 reader for about one and a half years, but have not considering meeting other hacker brethren until as of late. I used to have the option, when in Fargo, North Dakota, to attend meetings, but never saw through to it. After moving back to Minnesota, I have now got the urge to meet with my kin of the same interests. However, there are no listed 2600 meetings in Minnesota. If there are no such meetings, I would be willing to commit some time to helping organize and run a Minnesota local 2600 meeting in St. Paul (Twin Cities metropolitan area) every month. I already have a few that would be willing to attend, and I can determine a good location in the area that seems to fit everyone's travel needs. Is there anything on my end, or vice versa on yours, that is required to kick off monthly meetings and have you post the location and time in your quarterly issues? And just to make things clear, I obviously plan for the meetings to have no affiliations with any outside parties or groups. It will merely be a group of like-minded individuals with some common ground to share and further our abilities.

Excited to hear from you.

**B**

*You have the basic idea, so all that's left for you to do is come up with a good, centralized location that's open to everyone and let us know about it. We do require that we hear updates so that your meeting doesn't get delisted due to lack of attendance. It also can't hurt to have a website to help guide people to your meetings. We look forward to hearing how this turns out.*

**Dear 2600:**

This is a response to a letter I saw in a previous issue. A reader from Charleston, South Carolina said that he had been waiting for people to show up to the meetings, and no one ever did. This resulted in the listing for the meeting in this state being taken out. The meeting was supposed to take place in Northwoods Mall in North Charleston. I actually work about 500 feet from that mall in a locally owned computer repair store, and I can see the meeting spot from the back door. I have never been able to make it to the meetings, but I wanted to let that person (and the rest of South Carolina) know that there is

still a hacker community out here! I'd also like to invite that reader and any other hacker to stop by the store anytime to chat. Just walk in and tell whoever you see working that you're there to talk to Sea-biscuit - they'll know what you're talking about.

**Sebastian**

*It must have been awfully frustrating to be able to see the meeting spot from a computer repair shop and not be able to attend one yourself. Perhaps the throngs of people who will soon begin streaming through your doors to talk to you will be able to help establish a new meeting in the area. We hope you can attend this one and, if not, that it will at least be close enough to your store where you can communicate with each other.*

**Dear 2600:**

I've been a reader of 2600 since I was a teenager. I'm 31 now and been helping to host raves in this small city of mine for almost a decade. I want to host a tech rave with about 50 people, but I want to do it as a 2600 meeting as well. Do you think you can help me?

### III Protocol

*We'll help you with some advice. A meeting and a rave really aren't the same thing. If you try and mix them, they will probably each suffer. Plus, people who go to the meetings are notoriously different in background and interests, so getting everyone to groove to the same music would be close to impossible. We believe you should pursue each of these ideas, but separately.*

**Dear 2600:**

Greetings from Biloxi, Mississippi. I am interested in getting a group started here - to meet regularly, do some teaching, pick brains, learn new things, and co-mingle with like-minded people. I know you may be thinking *Biloxi, Mississippi? WTF is in Biloxi, Mississippi?* Well, the big 2600 readership here hails from Keesler Air Force Base, which is where the Air Force teaches the latest and greatest in cyberspace operations and defense. I work with and teach some great cyber minds and would like to create a place for us all to get together.

### TheCyberInstructor

*It may surprise you to know that we once had meetings in Biloxi, so we are confident that they can be restarted. Please keep us informed.*

**Dear 2600:**

In response to Curious in Philly from the Autumn 2013 issue, I'm here to report that the Philly meeting is alive and well. The location in the description should probably be updated to say that we currently meet in the food court outside Taco Bell (as opposed to the mini post office as it says now) which is about 50 feet from the old location. We list the time as 5 pm, but people usually show up between 5 and 6. Sometimes we trickle in at 4:45, sometimes the first person arrives at 6. Either way, I've never gone to a meeting and ended up the only one in attendance.

We shouldn't be hard to find - just look for the loud guys sharing a table full of tech and tacos, usually dressed in black. If there are any uncertainties,

we've hurtled into the 20th century with a website (philly2600.net), Twitter account (@philly2600), and trusty IRC channel (#philly2600). We're not too hard to get a hold of.

**Mike**

**Dear 2600:**

I'm either bored or am finally getting to the bottom of my to-do list. Dilemma: I would like to start building a group with regular meetings, its own page, the whole shpiel.

The problem is that Friday evening sundown begins Shabbos here in "The Holy Land." Since we follow the lunar calendar, the "day" actually begins the night before, so therefore Shabbos doesn't end until Saturday night. Most folks start to get ready hours in advance, so even in the summer, when Shabbos starts late, it would impact on attendance and focus.

Also, Friday and Saturday comprise the weekend, with the workweek starting Sunday. (It took a bit of getting used to, but it's kinda cool, especially if you want to work Fridays (until Shabbos), because no one else is in the office and you can actually get something done - but I digress.

Possible solutions for your consideration: (I teach my team not to bring me a problem without at least one possible solution (from the wisdom of Solomon), and cutting the baby in half has nothing to do with this, so here are some ideas to consider, and your guidance is appreciated.)

1. Provide us with a waiver for meetings on another day - Sunday?

2. Tell us it's too bad, and treat us like the Red Cross (research this - religion is not a part of their credo, but the Red Islam is OK, however, the Red Magen David is not accepted into the Red Cross so we go it alone).

3. Nuke us - the problem takes care of itself. Unless we Stuxnet it first.

4. Ignore us and maybe we'll go away. But with the largest per capita tech startup rate and other such billion dollar trivia, I think our know-how goes a long way.

So there's a bunch of options - you may have more or an even more preferable one. All I ask for is consideration and resolution of a conundrum that may have been overlooked in establishing the Friday evening meetings. Also, I'd like to offer up a distribution channel for the hardcopy mag and other items - after we get through this.

So, please advise how to proceed because I think these meetings will have a lot to offer.

**Dr. MG Cyb3rSM3**

*While we've always discouraged having our meetings on other days because we would lose the whole "first Friday" thing and because there's always going to be somebody who isn't able to make it, a culture where people generally aren't able to go out on Friday evenings is as good an excuse as we can imagine for an exception. Since your weekends are Friday and Saturday, we propose having your meetings on Thursday evening, just as meetings everywhere else come right before the weekend*

on Friday evenings. This keeps it simple, easy to remember, and somewhat consistent with the rest of the 2600 meetings.

## Free Advice

### Dear 2600:

You kick ass. I need a good domain (preferably one run by members of the h@cker community) where I can test my newbie skills. I need domain owners who allow me to perform H@rdcore D0SS-es on my own site. I don't mind paying extra for this kind of service. I just need people who will give me written consent. In addition, it would serve as a testing ground for perfecting SQL injection techniques.

Yes, poor grammar is essential. B!G Br0ther probably uses SEO techniques, but I only want to use my craft to better the world (at least mine).

### Truly, Madly, Deeply Yours

#### The Apostolic H@cker @ x86 Assembly of God

If you truly want to better your world, you'll stop with the @s and slashes in words, for starters. Archaeologists of the future will not look kindly on this period of our development. And while we may indeed "kick ass" on occasion, we know of no one who offers the services you're after for a fee. Why would you need to pay someone for the privilege of performing "H@rdcore D0SSes" on your own site? You could probably learn everything you needed by setting up your own internal network that's isolated from the Internet so nobody else would be affected if/when things spiral out of control. We hope you eventually come to realize that denial of service attacks are the last refuge for those with nothing to say who simply want to silence the opposition. We've seen them used for very noble causes, but there's just no getting away from this point. It's been our experience that actions equivalent to graffiti (i.e., website hacking) are far more effective and clever. Failing that, actually encouraging evil entities to speak their minds is often enough to turn most people against them.

### Dear 2600:

I had a close call in central Christchurch during the February 2011 earthquake (got out safely). I've recently been playing about with Bluetooth and an idea popped into my head.

If, during an earthquake, the building you are in collapses and you become trapped but you have access to your cell phone, try this:

Call police.

0) Remember you probably have a flashlight on your phone. Use it sparingly.

1) Use Facebook/Twitter (assuming you are a user) to get word out. Include your medical status, building name, and/or GPS location. Don't waste battery trying to phone anyone other than police unless things are dire - the phone network is likely jammed for at least an hour. The data network stayed up in Christchurch.

2) Set your phone's Bluetooth to discoverable (no timeout), and your device ID to "SOS trapped" "building name" "medical status"

If your battery is low, switch off your phone and leave on for five minutes an hour.

A USAR team or members of the public (if this catches on) would be able to scan for Bluetooth devices and use the WSSI signal strength to triangulate and locate you. Rescuers that pick up a signal like this can pair phones and communicate over Bluetooth.

anon

*These are truly some great ideas that everyone should consider and practice. They could easily save lives. We hope this catches on.*

### Dear 2600:

Hypothetical and for educational purposes only. Suppose I have permission to try and hack a Gmail account. I have that willing person's Gmail address. I will use some of the brute force tools on a laptop to target the email address. Here are my questions:

1) How do I avoid the laptop giving away its Wi-Fi card signature - or do I care, just use it and replace with a MXM type upgrade?

2) Should I buy a laptop online for this purpose or does this have pitfalls as now there is a record of who gets the laptop?

3) Should I buy a laptop on Craigslist where it is a cash transaction and already registered to another, use cash, and an intermediary?

4) Should I use an open Wi-Fi from a cafe to run programs against the target, then, once done, shut down and trash the Wi-Fi card, hard drive, or entire laptop? I guess here the question is, what other digital signature does a laptop give for tracing?

5) How will the Gmail service record this test?

6) Do we know of any internal hardware of the laptop that sends out signatures that can identify that laptop, thus making the cash purchase a wise choice?

7) How should I download an OS like Linux? Should I use a CD? Does downloading that OS generate signatures specific to the place, IP, Internet provider, connection, etc.? Should I use a different medium to grab the OS to disk and then manually load it to the new laptop?

Besides sitting in an area where a person will not be seen, using an open Wi-Fi connection and a laptop bought using cash with no identification given to the seller, what other ways can a signature be traced? It seems almost impossible to do this without something tracing back to the person who is testing the tool on the account.

Thanks for your anticipated and learned response.

dILLHole

*And you say you all of these precautions would be used when you already had permission to hack this Gmail account? We can only wonder how many questions you'd have if you didn't have permission! First of all, it's a damn Gmail account, not root at WOPR. It's very unlikely anyone will even notice, unless you actually get in and do something that draws attention. (Just getting in itself might be noticeable, as successful logins are visible to the user. Gmail, however, doesn't allow users to see unsuccessful attempts and it has no limit on how many*



times someone can try to login, making brute force attacks possible.)

If you are, in fact, trying to get into something really sensitive, you're asking a lot of good questions. The one thing to remember is that if powerful people really want to find you, they will. That's why calling attention to yourself in any way would be a bad idea. Even trying to protect your identity could raise suspicions if done improperly. Paying cash and not identifying yourself is smart, but will be remembered by someone you buy a laptop from, which could come back to haunt you if there's some sort of investigation. You can easily get lost in the noise if you don't do too much at once, draw attention to yourself, or act in a predictable manner. That means don't act like everyone else, but also don't act the same way as yourself each time you do something, as that makes it easier to find you if you act in a unique way. Keep in mind also that any time you do something in a public space, there's likely a video of you being stored someplace which could easily be called up if an inquiry ensues.

Those of you reading this in horror thinking that we're plotting all sorts of crimes should consider learning how to think in this manner. Knowing how and when you could be identified is always something to be aware of. The day may come in some part of the world where such knowledge can save your life. And, if that day doesn't arrive, there is never any harm in learning how the massive brain of surveillance works.

## Horror Story from Hell

Dear 2600:

I'd like to ask for advice with a problem that nobody else has been able to fix in more than a year and a half: how to remove a rootkit that stores self-extracting copies of itself in the hard drive, memory RAM disks, and BIOS?

You cannot load/install/run anything from the optical drive because the system loads a "virtual CD on the hard drive" instead. USB drives are either blocked or bypassed as well, since the hardware interrupts and system calls are changed at every reboot (using ACPI, among other things). As a result, the OS "thinks" there are twice as many USB drives as there really are, the CD/DVD drive becomes a "partition" of the hard disk, and everything else, including power supply, appears different from what it really is.

You cannot access the Internet because the malware changes the network settings. That blocks access to any and all online virus removal tools. Downloading the latter (or rescue CDs, or BIOS editors) somewhere else is pointless, because then it has to be saved on media of some kind - which the infected computer will not read or load.

Any attempt to reinstall the OS (Windows, Linux, or DOS) will load the malware version of the corresponding operating system. In the case of Windows, it looks like some kind of a stripped-down Windows NT 2008 server running nothing but

BitTorrent, which I have no control over. (Well, I can remove all the wireless network cards and never plug in the Ethernet cable, but that's all.) Instead of Linux of any flavor - I've tried more than I can remember: Ubuntu, OpenSUSE, Fedora, PCLinux OS, etc. - I get the same thing named ISOLINUX. Among other things, it changes all disk drives from "directories" into write-protected bitstreams. The DOS part I found last, when I tried to load FreeDOS. That worked once, so I used "debug" to reset the CMOS:

-o 70 10

-o 71 said

-q

This corrupts the checksum-protected area of CMOS, forcing it to reset. That was the most useful suggestion I have found on the Internet so far, and it came from Wikipedia. Every technical article, blog, or forum on the topic of flashing BIOS and/or rootkit removal comes down to "go to this website, download this great tool, and run it" - from the OS or by booting from a disk. This totally does not work if the OS is infected (actually, replaced by something that only looks like it) and nothing can be read from a disk of any kind.

There is an exception, and this is how I was able to use debug from FreeDOS to begin with: the system would boot from a CD that it had never encountered before, but only once. Some of the Linux distros and this FreeDOS CD I had burned at a library computer did load one time. However, the rootkit has a utility that reads the ID off every optical disk, records it, and never lets it run again. I have seen the program that does that while digging through the files in the "ISOLINUX" in search of a way to break into my own computer. Besides storing the info that would recognize the disk in the future, it also copies and modifies the file that runs at the startup. So the next time the CD is used, it shows a menu that looks similar to the original, but the option selected will either do nothing or... load the malware.

When I used debug as described above and the message that CMOS had been reset appeared on the screen, that was the first hope I had in a very long time. I restarted the computer and, when it came back on, there were 26 RAM drives - one for each letter of the English alphabet - present in the system, each with a corrupted version of FreeDOS and a bunch of directories filled with duplicate reinstall-on-deletion files - exactly like what I'd seen happen to Windows much earlier.

The autoexec.bat (one of them, anyway) had pages and pages of simple "for" and "case" blocks writing the same things into 26 different locations. It also had a comment:

*"Dear Life, When I said 'How things could possibly get any worse?' that was not meant as a challenge."*

That was yesterday. It is the second half of September 2013 now. The way this started: sometime in March of last year, I noticed that my computer was running something I had not installed. I removed it. When it reappeared, I removed it again. And again.

When Add/Remove Programs in the Control Panel of Windows stopped working, I manually deleted the files that weren't supposed to be there.

I was going to grad school online, so I needed to turn in homework at least twice a week - over the Internet - so there was no time to take the computer somewhere and wait until it was fixed. I could only count on myself. And since I had not worked in years because of a disability, nor left home much for that matter, I did not have a whole lot of other places to use a computer.

So I ran System Restore, closed the ports that weren't supposed to be opened, installed a firewall beyond the one in Windows, got a new security software package, and deleted what I didn't absolutely need. It worked. For a few days, I stopped whoever had turned my computer into a bot from breaking back in.

Apparently, I also made them very angry. When he (she, it) got back in, everything on the hard drive was wiped out and I had something less than a dumb terminal: a chunk of metal and plastic that was using my Internet connection to run the BitTorrent and media streaming while I could not go online.

I have no idea how much money I spent on "computer repair" at different places over the next few months. They all did the same thing: formatted the disk, reinstalled the OS, charged me around \$100, and got angry when I told them the computer stopped working within two hours after I booted it up. A lot of people ask me why I didn't buy a new computer. I did. I bought six new computers. I returned four and got stuck with the other two, in addition to my old laptop. Every single one of them was hijacked as soon as I went online. Well, two hours after, since that's how long it takes to incrementally wipe out the original OS and replace it with that BitTorrent-R-Us.

The one time I borrowed a friend's computer to turn in the damn homework, it got hijacked, too. She had an ancient Dell laptop with Windows XP and dial-up Internet. Two hours after I dialed up, it was exactly like mine. Apparently, "no one has ever heard of anything like it."

Hijacking my computer - and any other I tried to get - hit my life worse than if my house burned down. Actually, a fire, a bad car accident, an assault, and a robbery all put together would not be half as bad as what I've been going through.

#### **Morgan**

*This is a nightmare scenario like none we've ever seen. We'll throw this out to our readers to see if anyone has some suggestions. Perhaps the instigator is out there somewhere too and can chime in. This sounds like something out of a movie (and, if nothing else, you should get the rights to it, as it's an incredible story) and we can only wonder what would happen if such a scenario played out within a school, corporation, or government system. Regardless of how this develops, you (and anyone involved in some sort of technological craziness like this) need to tell your story, keep a good sense of humor, and not give up, hard as that may be. Technologi-*

*cal advances are terrific, but they can also crumble for unknown reasons and we'll crumble right along with them if we have no life outside of that world. There always needs to be a backup method of accomplishing a task should every bit of technology suddenly stop working. And it doesn't hurt to possess a rudimentary understanding of the technology itself, so you can analyze what's taking place. You seem to have that part of it covered.*

*We found one thing to be particularly interesting in this horror tale. The fact that multiple computers were infected rather quickly tells us that there's something about the setup that's lending itself to this. This could be a valuable clue as to the source. What did all of these computers have in common, other than being in your possession? Did they all connect to the net in the same method? Was the same web page visited on each of them? Whatever it is that links these machines together is likely the gateway to the evil that has visited you.*

#### **Future Plans**

##### **Dear 2600:**

I first got to know about your magazine in the early 1990s while I lived in the United States. Since then, I moved abroad and I missed reading the printed version of your magazine dearly for a few years since I left, but to my surprise I found that I can purchase individual copies of the current publications in the Kindle format from amazon.com and, to say the least, I am thrilled. I was also excited about your digests that included older publications that I have missed. I still have fun reading the older publications and the old emails that you used to get (from the book *Dear Hacker*) and ponder about the great strides and advances in technology from those days till today. Please keep up the good work that you have always done. I hope that all the older publications can be found in the Kindle format for purchase soon, and I look forward to getting all the upcoming editions. I hope one day I can purchase the printed edition as well. Thanks for a great publication that, in my humble opinion, is timeless and a classic publication.

#### **Sam**

*Thanks for the kind words. We certainly do want to digitize our entire back catalog, but this is by no means a trivial endeavor. As is the case far too frequently in the digital world, the systems we initially used for those early issues were allowed to become obsolete and the digital files have long since become incompatible and ultimately nonexistent. So the scanning, OCRing, proofreading, and layout actually are more work than putting out brand new issues. This is why it takes the time that it does and why it's so important that people support these efforts by buying the digests as they become available, as this is a tremendous investment, but one that is necessary if we are to preserve our history.*

## Appreciation

### Dear 2600:

I wanted to write you and say how much I appreciate 2600. I have always been interested in computers. My first computer was a Tandy. Thinking back, it is kind of funny how excited I was over a 300 baud modem. I always figured I would work with computers either in IT or as a programmer, but for one reason or another life happens. For the last 12 years, I have been studying chemistry, which could possibly be considered a form of hacking in the loosest sense of the word. However, my interest in computers never waned and I always had 2600 to keep my interest satiated. Just recently, my boss informed me that the IT supervisor was retiring and, knowing my interest, asked if I would like to take his place. The only obstacle that stood in my way was the CompTIA Security+ exam. In preparing for the exam, I was surprised that I had a pretty good foundation just from reading 2600. In short, I passed and I am very excited to finally work in IT. I owe a big part of that to you; thank you.

Gazza

*It's letters like these that keep us going as well, so thanks for that.*

### Dear 2600:

I just wanted to thank you guys (and the author!) for publishing the article "Dev'ing an OS" by Shikhin Sethi in 30:1. This kind of low-level technical content is exactly why I got my lifetime subscription many years ago!

The article provided, in my opinion, the perfect level of detail and explanation to pique a reader's interest. It also managed to avoid turning into a dry textbook-like introduction. Thanks so much for publishing articles of this type and quality - I feel a proper understanding of the systems around us really requires familiarity with its lowest-level components and processes.

Great work, and keep it up!

Ian

### Dear 2600:

I'm sorry it took so long to get around to this. I am an on-call tech and sometimes work a ridiculous schedule. But today is a chance to catch up on things. I very much appreciate the calendar even though it does not actually get used for reference on a daily basis. The quality of physical production, photography, and topics/captioning make them collectible as far as I am concerned. And I find all of the historical references extremely interesting. Perhaps someday I can be of use/service to you and several other worthy organizations I try and support, but for now all I can do is collect a few bucks here and there for contributions to the "tip jar" in appreciation for your efforts. A couple of weeks ago, I did manage to pass my exams and am now Amateur Extra AC2LS. Haven't had a ham license in almost 20 years and am dying to get back on the air, but for the present time I am all dressed up with no place to go. Have a pile of equipment to select from and lots of space for a great antenna, but no time to set something up yet.

Hope to do so before the cold sets in. Please keep up the great work and stay optimistic! I'm trying to.

J.

### Dear 2600:

After reading "U-verse Networking" by Uriah Christensen in 30:3, I have to say it is the best article I've seen in 2600 in a while that explains some real life, actual benefits of hacking. This is a must read for all IT or networking personnel. Even I learned something and I've been networking and programming since 1993. This is just another example of nicely written, informative, and useful articles we can expect from the 2600 crowd to keep our thirst for knowledge quenched. Keep 'em coming, everyone!

RAMGarden

### Dear 2600:

This is an amends letter. I stole 2600 when I was very down and out. I am sending what is the beginning of paying you back. I am sorry. I promise to repay the debt. And, not to justify, but reading 2600 did offer me quite a bit of comfort. Thanks and sorry.

P.S. You guys rock.

Anonymous

*This is a really nice gesture (we've now received two envelopes with \$50 each), but we don't want people to feel guilty for such misdeeds of the past. For anyone out there torturing themselves because you shoplifted our magazine in the past, getting a lifetime subscription would help alleviate the pain since it's the same amount you would have paid had you gotten it in the past, and you would have received the stolen issues anyway as part of the deal. We always appreciate honesty, even when it's delayed.*

## Digital Divide

### Dear 2600:

I had a letter published a year or so ago about the disappearing Kindle issues. I can't say which issue it was published in because, again, I have lost all of my back issues. I can back up John's letter in the Autumn issue 100 percent. I could have written that letter nearly word for word.

The credit card associated with my Kindle account expired. I wasn't aware of that until I received an email from them. By that time, it was too late. I had lost all of my back issues again. I called them and asked for my back issues to be reinstated. I was told that there was nothing that they could do. The Amazon rep was very nice, so I tried to reason with her. I put it this way. If my credit card had expired while I was receiving my magazine in the mail, would you be able to walk into my house and take them off of my coffee table? No? OK, so how can you go into my tablet or phone and take back the electronic copies? I own them and I want them back. I don't care if the credit card expired. The magazines were paid for and they were mine to keep as long as I wanted to.

I was offered a refund, just as John was. I was a little stubborn. I told her that I didn't want that. I

paid for those magazines, just as I would have if I had bought them in a store. They were my property and I wanted them back. I explained that I was really concerned and worried about buying anything from Amazon at this point. I asked her how I could be sure that they wouldn't go into my tablet and start taking back books that I had purchased. I asked to talk to a supervisor. I couldn't understand why they couldn't just send me copies of back issues for free since they do sell them on the site, but no, they wouldn't do that either. On my next credit card statement, there was an entire page of \$1.00 credits.

Clicking "Keep this issue" doesn't work if your credit card expires or the number changes and you don't change it on your Kindle account before they try to bill you for the month. If they are unable to bill your credit card for any reason, all of your issues disappear. If, for some reason, you decide to not continue with your subscription, all of your issues disappear. This was not a mistake on the part of the rep that John spoke with. The supervisor explained to me that it is their policy. I told them that they were wrong and explained again that they couldn't take back printed magazines from my house. I know that we are paying less for the Kindle subscription, but it doesn't have to be printed and shipped to a store either.

I'm going to try to back up my magazines with Calibre. I live in a really tiny house and, if it weren't for Kindle, there would be so many books in this place I wouldn't be able to move. I hope that this can be straightened out because I love the convenience and the extra storage space.

**June**

*This bothers us as much as anybody because when they give you that refund, it's really us that's giving it to you without even being asked. This really sounds like some kind of programming deficiency because the policy makes no sense whatsoever. We will continue to get on their case about fixing this. Hopefully, we'll get somewhere.*

**Dear 2600:**

Tried to find you browsing in the Barnes and Noble store on my Nook but couldn't find you under any categories including technology and computing or whatever they had. Found you at bn.com, though. Just thought I'd mention it. Some people less persistent than I might have given up.

**Jota**

*Every outlet where we're available poses its own challenges. Thanks for letting us know about this one. We will investigate.*

## **HOPE-X Tickets**

**Dear 2600:**

I was wondering why, when I had tickets in my cart, put my credit card info through (took me less than one minute), and then hit submit, I was told that this item was no longer available. You need a better system of how this is done. If they are in your cart, someone else should not be able to purchase them out from under you.

This whole race for tickets is the reason we stopped going to Shmocon.

**Lynn**

*First off, this wasn't our whole ticket batch, but a small number of half-priced tickets. When there's a limited number, not everyone is going to get them. We had a huge amount of people competing for this and the entire batch was gone in just over a minute. If you didn't get our second batch at a slightly higher price, then there's our far more mellow preregistration process, which is open now. It's still cheaper than the door price and far cheaper than any other conference of its caliber. We did discover a little trick, which we'll share here. When limited items are made available, the challenge is getting all the way through the process before others do. That means selecting your item(s), entering your name and address, and finally putting in your credit card info. It's that final button click that determines whether or not you made it in time. But if you're already in the process of placing an order at the moment when the limited availability item becomes available and have already entered your name and address, you can simply hit the "keep shopping" button (or even the "back" button on your browser), select your new item, and quickly check out, having already entered most of your info. We're not trying to get you to buy more stuff as a means of getting things that are highly sought after. But it would be a nice way of thanking us for sharing this little tip.*

**Dear 2600:**

Hey! Will there be more tickets for sale because I missed the half price sale? I sure hope so. It will be my first HOPE event.

**Ether 9ine**

*Yes, tickets should be available as you read this at x.hope.net. We do encourage people to get them early, as it gives us more money to work with to pay for the conference and there's also the slight chance that somebody really famous will tweet about it and have us sell out the whole place immediately.*

**Dear 2600:**

The time of the sale is unfair for me who is at work at that time with no Internet access. Is it possible to make the sale later in the evening or on the weekend when most people are available, please? Thank you HOPE in advance!

**Greg**

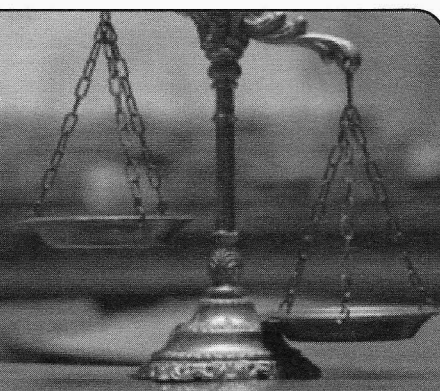
*We did weekend sales for HOPE Number Nine and had the same complaints from people who weren't around then. Eventually, we'll do a 3:00 am sale so night owls will stop being angry at us.*



# BLACK AND WHITE



## THE GROWING SCHISM BETWEEN HACKERS AND THE LAW



by Scott Arciszewski

About two years ago, I was a computer engineering undergraduate at UCF, hoping to eventually go to graduate school and eventually earn a Ph.D. One day, my curiosity got the best of me. I went to [infragardtampabay.org](http://infragardtampabay.org) and decided, "This website is used by the FBI, another Infragard site just got hacked by LulzSec. I'm no skilled hacker, so if I just looked around it should be harmless enough. I probably won't find anything." How many 2600 readers told themselves that before?

Before trying anything too obvious and noisy (SQLI), I decided to view the page source and see what software they used. This is what I saw on June 21, 2011:

```
<!-- DotNetNuke - http://www.
dotnetnuke.com -->
<!-- Copyright (c) 2002-2008 -->
<!-- by DotNetNuke Corporation
-->
```

"Strange," I thought. "2011 is half gone. Why would a website used by federal law enforcement show 2008 in their credits?" So I did the obvious thing: I typed "DotNetNuke vulnerability" into Google and found this page: <http://www.exploit-db.com/exploits/12700/>

The total "intrusion" lasted only 23 minutes, according to court documents.

Stricken with horror and disbelief of having found a published vulnerability in a website used by federal law enforcement (and having been unable to locate their webmasters' email address), I decided to blow the whistle on Twitter, various forums, and my personal website. Many experienced 2600 readers will realize this as a classic "completely stupid

move" (runner up: not using Tor, an overseas VPN, or an SSH tunnel when I knew how). I agree.

One month later, at the height of the LulzSec media frenzy, the FBI raided my dorm room and questioned me on every detail of the incident. I was then arrested, thus making me miss my scheduled exam in Discrete Structures. When I was released that evening, my face was all over the news.

I had juxtaposed my face over the "Lame Pun Coon" background, as an inside joke with my friends, and added the flavor text "How dare you accuse me... of PUNditory?!" and many media outlets chose to crop it to "How dare you accuse me," apparently for comic relief. My home town, however, opted to take the yellow brick road:

```
http://www.winknews.com/Local-
Florida/2011-07-20/What-is-
North-Fort-Myers-alleged-
hacker-accused-of-doing
```

(A full day after, they somehow thought I had a botnet and DDoSed Infragard to get in. Despite being criticized by many people, they never corrected their mistake.)

Before anything got resolved by the courts, UCF held a student conduct hearing. When a hearing happens, you have two choices: an administrative hearing, where one adult UCF employee hears your case and decides your fate; or a peer hearing, where two UCF employees and two students decide your fate. I chose the latter, thinking that the student body would realize how benign (although admittedly reckless and stupid) my actions were in the grand scheme of things.

One of the employees was a narcissist who told the receptionist he was there for "the admin-

istrative hearing” and was evidently butthurt that he didn’t have all the power throughout the hearing. The two students were meek and ineffectual. My public defender was not notified and was, in fact, not allowed to be present. As usual, the game was rigged, and I lost: two year suspension (on top of whatever sanctions the court decided), and I had to write a five-page apology paper.

The final decision to suspend me through Fall 2013 came right after my final exam grades were posted (I got a C in computer science 1 and a D in Physics 3; not great, but I was dealing with a lot). That didn’t matter to UCF though. My last semester was erased (which screwed up my taxes for the next year and is probably illegal).

Eventually, my public defender advised me that the best option would be to plead guilty to avoid prison. On an initial filing from Infragard’s hosting and cybersecurity company (which I found out about in the presentence report), Sylint Corporation ([usinfosec.com](http://usinfosec.com)) claimed damages from June 16-24 totaling over \$32,000 (which meant prison and an overwhelming restitution). When I pointed out that I don’t own a time machine and couldn’t have hacked them at any time before June 21, they amended their claim: \$9,370 in damages (45 man-hours) from the 21st through the 27th.

All this for being a greenhorn with no knowledge of the laws or ethics surrounding computers. For being a curious and stupid kid. For the digital equivalent of knocking on someone’s front door, it swinging ajar, looking in, seeing nobody home, going on my way, and then being put on house arrest for six months (and probation for five years) and told to pay the homeowner \$9,370 plus \$100 in special assessment fees. For the equivalent of a full disclosure without notifying the vendor ahead of time. I’m still amazed that they can operate while paying their employees over \$200 an hour. Nepotism pays, I guess.

That was my story. Since I began reading 2600, I’ve heard similar elements from many other people less fortunate than myself (my heart goes out to anyone locked up in prison for out-mathing or out-logging the developers who produced a “protected system”).

There is a lesson to be learned from all this, and this is what I would like to emphasize: *Do not be a good guy*. It never pays off.

Let’s look at another example. The same year I was arrested, I read news stories about a

young man in the U.K. who hacked Facebook, and was arrested while writing his vulnerability assessment report for their whitehat challenge (<https://facebook.com/whitehat>). He had previously been rewarded for finding flaws in Yahoo and other large companies’ websites (and was publicly acknowledged for doing so), and when the authorities interrogated him, he referred them to a Cambridge lecture on computer science. Ring any bells? I can’t find the story anymore.

I won’t even get into Weev’s story, because everyone knows it and this article is long enough. (Look up “weev ipad” in Google if you’re curious.)

Are you seeing the pattern? Well-meaning folk are being prosecuted left and right, while the people who are causing the real damage are either on their payroll (usually as informants) or scot-free. And we wonder why our country’s cyber-readiness is ranked three out of 10 by the NSA. In the words of Mercedes Haefer, in response to Keith Alexander’s comment about how hackers are just what this country needs: “*Then stop arresting us!*”

That won’t happen. Government employees are overworked or lazy (depending on your perspective) and will always opt for the lowest hanging fruit. That’s why HackForums blocks Tor exit nodes and known proxies. (And can you even count the number of Groups and Crews who conduct their membership interviews over Skype without causing an integer overflow? Probably not!)

The time for the white hat is over. Unless you have a solid contract and previous working relationship, helping a company or government agency is just opening the door to being used and abused. A white hat is like a condom - you’re either useful or disposable.

If your good nature won’t let you abandon the white hat path, let me make a friendly recommendation: don’t help companies, don’t help schools, don’t help the government. Only help people and, even then, only do so safely and anonymously. Being anonymous should be your first priority. You can’t trust anyone. Tor and proper OPSEC (see also [grugq.github.io](https://grugq.github.io)) are your essentials.

The law is black and white. You’re either a criminal or not. (Most likely you are.) While most of the hackers I’ve met are varying shades of gray, I think everyone could do well by taking a phrase out of the FBI’s dictionary and “go dark.”

# Netcam: Basics and Vulnerabilities

by John Thibault

An Internet Protocol (IP) camera or “netcam” is a digital video camera used for surveillance to send and receive data via a computer network. Unlike analog closed circuit television (CCTV), IP cameras can send information via the Internet. Most cameras that do this are commonly known as webcams. The term netcam is typically applied only to those used for surveillance. Netcams are available at resolutions ranging from 0.3 to 29 megapixels while newer systems operate and capture video in high definition, e.g. 720p or 1080i and 16:9 widescreen format. There are two different types of netcams.

1) *Centralized IP Cameras*: Requires a central network video recorder (NVR) to handle the recording, video, and alarm system.

2) *Decentralized IP Cameras*: Does not require a central NVR, since the cameras typically have a built-in recording function and can record digitally to local storage media, such as flash drives and HD drives or even to standard network attached storage.

Netcams are commonly used for security, due to their ease of accessibility from any computer, as well as from many smartphones and other devices such as an iPad or tablet. Some cameras can be moved anywhere on an IP network (including wireless). They can also be equipped with “distributed intelligence” allowing scalability in analytic solutions to ensure coherency of agents of a surrounding area such as motion detection, as well as two-way audio which allows users to communicate with what they are seeing. They can be programmed to determine when an object or individual moves to a specific zone or area. Commands for pan, tilt, and zoom (PTZ) are accessible via a single network cable or connection and can also be operated via any computer or accessible device.

Most netcams are assigned a temporary IP address (four numbers ranging from 0 to 255 that are separated by periods) by the router. This is how you find the camera(s) you wish to access. Turning the router or camera(s) off changes the IP address. For users who are less “computer savvy,” the cameras can be set with a fixed address, which means the IP address of the camera does not change and the user can always locate it with ease. The cameras are accessible

using a local area network (LAN) which can only start with 192.168 or 10... but to access the camera(s) remotely, you will need to know the wide area network (WAN) address provided by the Internet service provider (ISP). Most netcams are powered via PoE protocol. “Power over Ethernet” simply means the cameras receive their power via the Ethernet cable they are connected to.

When installing multiple network cameras, it is wise to use a centralized network camera, which requires a network video recorder (NVR). An NVR is a program that can store video from network cameras and allow for viewing of multiple cameras at once. It is similar to a digital video recorder (DVR), but while a traditional DVR is responsible for encoding and processing video from component cameras, NVR depends on the cameras to encode their video, simply storing it and allowing for centralized remote viewing. Netcams offer secure data transmission through encryption and authentication methods such as WEP, WPA, WPA2, TKIP, and AES. But we all know a network is only as secure as the individual creating it. If you plan to record and store footage, you will also need a dedicated NVR or a PC to install NVR software on, as discussed earlier.

In 2012, research showed that 21.57 percent of users utilizing netcams used the default passwords, either out of laziness or simply a lack of knowledge of the importance of having a strong, unique, and secure password. The most common default combination is admin/admin with more than 30 percent of all manufacturers using it. As we can see, nearly a quarter of all netcams used are set to their default passwords and are never changed or altered. It is even common for a business to alter the password so slightly that it is still pretty easy to figure out.

Here is a list of common netcam default passwords:

- ACTi: admin/123456 or Admin/123456
- Arecont Vision: none
- Avigilon: admin/admin
- Axis: root/pass, new Axis cameras require password creation during first login
- Basler: admin/admin
- Bosch Dinion: none
- Brickcom: admin/admin
- Cisco: No default password, requires

creation during first login

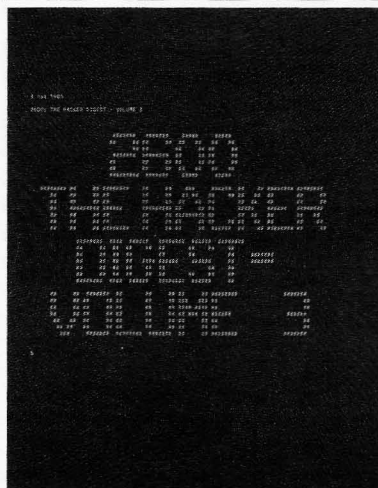
- Dahua: admin/admin
- Edimax: admin/1234
- Grandstream: admin/admin
- Hikvision: admin/12345
- Honeywell: administrator/1234
- IQinVision: root/system
- IPX-DDK: root/admin or root/  
Admin
- Mobotix: admin/meinsm
- Panasonic: admin/12345
- Pelco Sarix: admin/admin
- Pixord: admin/admin
- Samsung Electronics: root/root or  
admin/4321
- Samsung Techwin (old): admin/1111111
- Samsung Techwin (new): admin/4321
- Sanyo: admin/admin
- Scallop: admin/password
- Sony: admin/admin
- Stardot: admin/admin
- Starvedia: admin/<blank>
- Trendnet: admin/admin
- Toshiba: root/ikwd
- VideoIQ: supervisor/supervisor
- Vivotek: root/<blank>
- Ubiquiti: ubnt/ubnt

For example: Sony's netcam default password is: admin/admin. Other than using default passwords, some would be shocked at how many businesses set their access information to something as simple as the name of the business, or street number of the address where the secured location can be found. I recently worked for a company who set up a surveillance system and used admin/2600 for the login infor-

mation - "2600" being the street address where the business was located (of course, I changed this for the purpose of confidentiality). Almost anyone with basic hacking skills could, eventually, figure it out.

Let's say, for instance, there is a company called "Bob's Shack." I wouldn't put it past them to set up their netcam to be admin/bobsshack. It's easy to remember, right? But it's also pretty easy to figure out with a little bit of trial and error.

I would advise anyone with only basic knowledge to consult a professional security technician when installing and setting up security surveillance. It is critical that proper precautions are taken to secure all networks, IP addresses, and VPNs. If your passwords and protocol are weak, it is easy for almost anyone willing to put in the time to figure out how to penetrate your IP cameras and use them to their advantage. Safety and security should not be taken lightly and should be of the utmost highest priority. You never know who will try to exploit a security loophole, especially when it comes to something accessible via an Internet connection. If you know someone who is thinking about installing a netcam security system, tell them to read this first. Hopefully, this article will bring the vulnerabilities and importance of proper use and setup of high-tech security systems to light. It doesn't matter how much (or how little) you spend on a security system if the passwords can be figured out with only the smallest effort. If you install a camera system to feel "safe," you must first be sure that the system and its data are also safe from possible intruders.

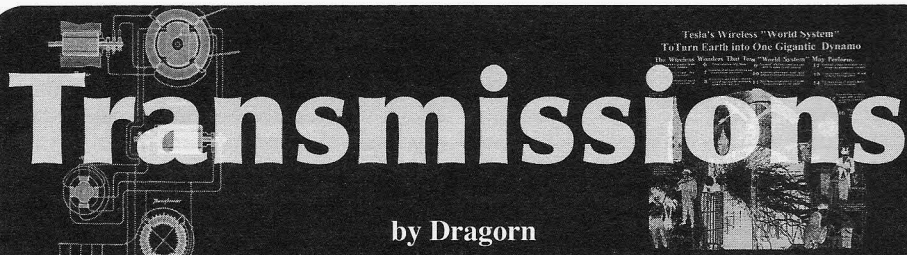


## VOLUME 3 of The Hacker Digest is Now Out!

Comprising articles, letters, illustrations, and data from our third and final year in the old newsletter format. It may have been 1986, but our pages were filled with news about the NSA, military secrets, and all sorts of mischief that inspired everyone from teenagers to filmmakers. Now available digitally in all its restored splendor.

Get the PDF at [store.2600.com](http://store.2600.com) or visit [digital.2600.com](http://digital.2600.com) to see all of the digital options





# Transmissions

by Dragorn

## Location Spying, Not Just for Governments Anymore!

Every time you leave the house, you're tracked - and with more precision than you might guess. What city you're in, what street you're on, what store you've gone in, how long you spend in it, and even what aisles you visit. How long you spent looking at personal hygiene products.

How is such universal tracking done? There are several tricks the government uses to keep track of people (in the United States, anyhow - likely similar methods are used worldwide):

1. *License plate scanners.* Increasingly common in large cities, license plate scanners are good enough to monitor every car entering or exiting an area, as well as tracking what streets you drive on once inside the city.

Major metropolises like New York City routinely scan all cars entering and exiting the island, as well as tracking movement to specific areas. "Exclusive" communities in California have started scanning all vehicles in and out of public neighborhoods in a thinly veiled threat to keep out "undesirables" - remember, we're always watching you.

Optical character recognition systems are more than fast enough to do real-time recognition of cars passing through control points such as toll booths or low-mounted cameras on police or unmarked vehicles, which scan every car parked on a street they drive down.

Despite numerous protests, there is little case law dictating the use of automatic plate capture. Several cases have arisen where authorities are accused of racial or religious profiling by logging plates around mosques, churches, and protests.

2. *Voluntary digital tracking devices, like the "E-Z Pass" system.* For readers unfamiliar, the E-Z Pass is similar to an RFID tag system, which is mounted in a car and used to pay road tolls. E-Z Pass tags use an internal battery to boost transmission to the toll readers. Similar technology is used in other regions, under names like FasTrak, TollPass or, in Europe,

systems like eToll, autoPASS, or ENC. Often, toll authorities offer a discount for using the automated system.

Originally, the E-Z Pass was pitched as short-range - it worked in normal toll booths at low speeds. Then it was expanded to high-speed toll lanes where it could be scanned at highway speeds. The maximum range for reading an E-Z Pass tag is unknown.

Of course, every time you pass through a tag reader, it photographs your license plate in case there is a problem issuing the toll electronically.

In the United States, it is currently illegal to use the electronic tag systems, or to use the toll booth systems, to enforce maximum average speeds. In the U.K., average speed cameras have been automatically logging license plates and issuing fines for years. As municipalities become more and more cash strapped, it seems only likely that this tracking will extend to the U.S.

More unsettling is that recently, "Puking Monkey" revealed at DefCon how he modified an E-Z Pass tag to light up an LED every time it was triggered by a reader, and discovered that in New York City, tag readers are placed throughout the metropolis, tracking cars well away from expected toll booths. The DOT states that the data collected from mid-city readers is used for traffic flow analysis but, once data is created, there's little limit on what it can be applied to.

3. *Cell phones.* There is no more perfect spy in your pocket than a device which constantly updates where it is located.

To route a phone call or an SMS message to a phone, the cell phone company must know what tower it has most recently connected to. To fulfill E911 requirements, it must be able to locate a phone geographically.

Case law in the U.S. has already established that this tracking data is not considered private, despite several legal challenges, allowing the government unfettered access to location records without a warrant.

\*\*\*

Unfortunately, it's not just the government getting in on the game. Stores want to know where you are in the store, how long you spend somewhere, and match that to what you buy.

To get high-precision tracking within a store, cell tower precision location is insufficient, and a store would have to pay the cell carrier for the data, anyhow. The solution: Tracking Bluetooth and Wi-Fi.

Bluetooth tracking came first, and originally was used for interactive ads embedded in kiosk stands or posters, which didn't see a lot of popularity. For Bluetooth monitoring to work easily, the device must be in discoverable mode - for various technical reasons, sniffing Bluetooth devices which are not discoverable is difficult and expensive, putting it outside the price point companies are looking for when building store-wide tracking networks.

A discoverable Bluetooth device responds to inquiry packets; the most basic of scanning systems simply needs to constantly issue a "scan for new devices" request and log everything seen. Since Bluetooth is short-range - locating a device within a store becomes as simple as installing as many sensors as are needed.

Fortunately, most (though not all, by any means) devices default to non-discoverable, in part exactly because of these privacy concerns. Unfortunately, then we come to Wi-Fi.

When a Wi-Fi device is turned on, it expects to connect to a network. To try to connect to a network, it sends "probe request" packets. Each of these packets contains the name of the network the device is looking for, and the unique MAC address of the Wi-Fi radio in the device. Anything in reception range (tens or hundreds of feet) can receive these packets.

Whenever a device's Wi-Fi is turned on, it is regularly sending these packets. It may often send multiple packets - one for each network in the saved list of preferred networks.

Private companies now have all that is needed to track user movements throughout a store using nothing but the Wi-Fi radio in smart phones. Additionally, these companies can share and correlate such data - since the packet is meant as a public, broadcast request

for a network to join, it could be argued there is no expectation of privacy.

Of course, once data is collected, there's no telling what it could be used for - or who could use it. Cell phone location data was originally tracked simply for technical reasons: The network needs to know what tower to send a message to. Now, private companies are being compelled (or volunteering) to collect tracking data. There is no reason to think this won't be the same story again.

Nothing limits this tracking to inside stores, either. Several companies have begun to offer outdoor pole-mounted tracking systems, under the auspices of traffic data collection (sound familiar?). Some of the collection systems are run by law enforcement agencies, some are run by private companies.

Think data collected by a private company isn't a means of tracking you? Depending on the location resolution of the tracking system, it's possible to correlate the locations in the store, the products in those locations, and the purchase records of that time period, and map a MAC address of a Wi-Fi device to the credit card information used to pay. Consider also the other companies which have similar data. For instance, Apple or Google know the user ID of a device and the MAC address (used in backups, etc.). While it may have been possible to assume that data collection agencies weren't collating these records in the past, it seems naive to think so given recent revelations. If the same system can collate number plate recognition or toll tag recognition with Wi-Fi detection, it would be similarly possible to identify a user... maybe not with a single read event, but with multiple events over several locations.

Not all is lost. Privacy in movement is rapidly eroding, but some methods can be avoided. The simplest way to avoid Wi-Fi tracking? Turn off Wi-Fi when not at home. When turned off, the device is no longer looking for networks, and no longer sending probe requests. Either make it part of your daily habit or use various helper tools. On Android, event tools like Locale or Tasker can be used, or dedicated tools like Smarter Wi-Fi Manager (disclaimer, written by yours truly) can be used to control the radios based on cell tower location - using the automatic location data from the cell network to *increase* your privacy for a change.

# All I Want is Total Freedom

by lifeguard

When men like John Adams and Benjamin Franklin were hammering out the USA's Bill of Rights, it was possible for them to have a private conversation. They could simply walk into the middle of an empty field and talk quietly to each other, all the while observing if another person came close enough to hear them. Today the government has the ability to see and hear through walls! There is also total integration of state and corporate data collection. This article is about how to get back some privacy. But be warned: taking these steps could be characterized as "trade craft" and raise suspicions.

First, I got rid of the snitch on my PC by using Linux. Next, I got rid of the snitch in my browser by using two different browser applications side by side. By only logging into my Google account in Chrome and doing all my other web surfing in a modified Firefox browser, I made it much more difficult for the Googleplex to correlate all my map, YouTube, and web searches. I use Adblock Edge to block a lot of third party social networking content that also correlates my surfing. For most searches, I use [duckduckgo.com](http://duckduckgo.com) to anonymize Google web searches. I installed Torbutton for when I wanted to randomize the IP address my traffic is emanating from. I got rid of the snitch in my email by setting up a free email account at a company based in Switzerland. Almost any "second tier" webmail provider in a non-U.S./British Commonwealth country reduces automated or warrantless data collection. If I need a preexisting email account to activate service, I use [mailinator.com](http://mailinator.com).

Next, I turned my attention to the snitch in my pocket, my smartphone. I dumped my Android phone and put an old expired cell phone (battery stored outside phone) in my car for emergencies - 911 will still work even if a phone is not on an active account. Then I purchased the cheapest prepaid phone possible to reduce the remote attack surface area of my phone OS. I got two GSM-based phones and multiple SIM cards. I swap cards in and out to reduce traffic analysis. I only store phone data on SIM and micro SD cards so they can be quickly removed. Remember, "destruction of evidence" is a crime. To activate my prepaid phone, I used Tor and Mailinator with a pseudonym. I provided a zip code from a different town. I made sure to be in a public place when I turned the phone on for the first time. When I want to have a private face-to-face conversation, I remove the battery from my phone and request the people I am speaking with do the same. This is due to the fact that phone mics and cameras can be remotely activated.

Then I looked at the snitches in my wallet. I have customer loyalty "club" cards for several stores. Why should I use the same card year after year when they are free? So every few months, I lose my card and get a new one. Next, I thought about my bank card. It produces a time stamped list of where I shop and what I buy. So now, I go to my bank's ATM and withdraw \$100 cash at a time and make all of my purchases with cash. Some businesses ask for a credit card number as a form of deposit. So I purchased a cheap debit card and activated it the same way as my cell phone. This is not always accepted, but often it is. Then I looked at my driver's license and wondered why I use it for identification? It is a license to drive. So instead, I use my passport for ID because it does not have my home address on it. If I show a passport to a police officer while walking down the street, he is not able to pull my DMV and other records with just the passport number. It does not show my state and city of residence. To improve privacy of my phone calls, I also purchased two prepaid long distance phone cards. If I call card number 2's access number with card number 1, it obfuscates Caller ID. I can also use them to make calls on payphones and courtesy phones that block toll calls. When a card gets down to a few dollars, I abandon it near a payphone so another person can use it and dirty up my data.

Finally, I thought about the ways I am a snitch on myself. I decided to make a 3x3 grid of keywords. Next, I wrote three code words (names) down the side and another three code words across the top:

	Jones	King	Smith
Alvin	YES	NO	UNKNOWN
Bob	MY HOUSE	THE MINIMART	YOUR WORK
Charles	BEER	CIGARS	2600 MAGAZINE

I provided a copy of this to my partner so we could have an easy code to obscure details of what we are discussing. So I could send this message: "Do you want to hang out with Charles King or Charles Jones?" And my partner decodes it as: "Do you want beer or cigars?" She could then reply: "Let's meet CJ at Bob King's house." I would understand that she wants to get beer at the minimart. So I would reply: "I am talking to Alvin J, see you in a bit!" She understands that I said yes to her. On a regular basis, we change the code words and, if we need to, we update the keywords to be relevant to our interests. It is a good idea to have a unique first letter for each code word.

# *Dev Manny, Information Technology Private Investigator “Hacking the Naked Princess”*

by Andy Kaiser

## **Chapter 0x7**

“So what do you want, anyway?” Lynx pushed away from the table and shoved a headset in his ear.

I liked the straightforward question. It meant I could give equally straightforward responses. If everyone in the world was like this, conversations would actually be worth the effort.

“I’m an Information Technology Private Investigator.”

“Wow. I have no idea what that is.”

“I get that a lot. I’m investigating a problem. There’s a file in the hacker community, a secret archive. It’s called the ‘Dante collection.’ It’s connected to the AnonIT hacking competition.”

While I talked, he’d been fiddling with his headset and poking at his cell phone. He stopped, and looked at me with narrowed eyes.

“It’s not really ‘hacker’ these days,” he said. “A hacker is a person interested in how things work, someone who loves taking things apart. I mean, if you’re talking about script-kiddies or crackers, even social engineers -”

“Semantics aside, I need to find more about this Dante collection. I need help from people who have it, or know people who have it. It’s important - it’s about a missing person.”

He considered, then nodded to himself. He pointed with his cell phone.

“Let’s talk outside.”

We weren’t far from my office. Close enough that I’d walked. Not that I wanted exercise or anything. More like the walk would do my car good. The heap of rusted alloy was already on life support, and every use pushed it closer to its automotive flatline.

I wasn’t a big outdoors guy. I appreciated it when I was forced to, like when the power was out, or when there was a gas leak. I stared around as we walked, waiting for Lynx to speak. I took in Nature’s special effects: nice frame rate and resolution. The moon hung low and pale, like a gigantic low-watt LED bulb. The wind forced me to shiver and dig my chin a little deeper into my coat collar.

Lynx was again poking at his cell phone. I saw he was playing a port of Nethack. I gave him a look of polite expectation. He caught my eyebrow-initiated cue.

“I don’t want anyone else to hear. What we’re talking about isn’t exactly legal.”

He kept his voice low. I couldn’t tell if he was being secretive, or if he really was one of those naturally shy people. His next sentence cleared up any confusion.

“I tried the AnonIT competition. Failed it hard. But I know one of the winners, *Minotaur*. He showed me the Dante Collection.”

Just what I needed. If this kid had access to someone with the Dante Collection, I could figure out how it related to P@nic, the missing hacker, and maybe learn where she’d gone, why she was missing. Then her infatuated friend Oober would be happy because his love interest would be returned. I’d be happy, because I’d have brought a very unique girl back into the hacking community. Maybe I could even figure out a way to get paid.

So far, I was lucky - this was a pretty straightforward case. No surprises. Just the way I like it.

Lynx’s thumb paused over his cell phone screen, and his eyes unfocused. He leaned closer to me. He didn’t make eye contact. His cheeks burned an embarrassed red.

“Hey. Just so we get this out of the way now... In the Dante Collection...”

He took a shaky breath before continuing. The kid had tears in his eyes.

“I’ve seen the naked princess.”

## **Chapter 0x8**

A lot of my success isn’t about knowing anything (though it makes things easier). It’s not about having the right tool for the job (though I never go anywhere without my Leatherman multitool).

Success comes from the right reaction to a given situation.

*I’ve seen the naked princess*, Lynx had said.

I had no clue what that meant, so I used my standard exception handler.

I nodded knowingly.



"Yeah," I said. "The naked princess. Keep talking."

Lynx looked at me like I was crazy.

"If you knew anything about it, you wouldn't say that."

"Why?"

Now his look turned suspicious. He moved a step away from me.

"You better tell me why you want to know."

Generally I don't give out the names of my clients. Not if I can help it. On the other hand, since I was the only Information Technology Private Investigator I was aware of, I got to make the rules, like the just-now-created Rule Seventeen: *An ITPI is allowed to share data in order to progress on a case.*

"I'm working for Oober. He brought me in because another hacker is missing. P@nic dropped completely off the grid."

Lynx blinked a couple times, then nodded to himself. He slipped his cell phone into his pocket and gave me his full attention.

"I don't know Oober. Never talked with P@nic, but I heard about him. The guy's a wizard. I'll tell you what I know."

Lynx's mental firewall had changed from no entry to all ports open. Just the mention of P@nic's name was enough to get him comfortable, though he didn't know P@nic well enough to know she was a girl.

"I bailed out early on the competition," Lynx said. "It was way over my head. Later, I tried to contact the winners, to see what they did. Chixor Zed wasn't real friendly. But Minotaur was pretty cool, and showed me what he did to break into the target. None of the others would talk."

His mention of Chixor Zed and Minotaur confirmed my theory about the list Oober had given me. The names listed under the "*dante connection*" header were a list of winners, or other competitors.

"How did he win?"

I'd said the words casually, though the question was anything but. This was one of the reasons I'd started my own ITPI practice, why I didn't have a job that paid better and had benefits beyond the strange smell in my office. I was interested in how things worked, what made things succeed and fail, and being an ITPI was a great way to experience this. While I needed to periodically afford dinner and rent, I needed more in life: The best reward for solving a case was the opportunity to solve another.

Here, I had the chance to learn about elite-

level hacking, and what it took to be in that select group. Here I had an express elevator to the top mental floor.

"It was a nasty one," Lynx said. "You know anything about this year's AnonIt?"

"I know that the goal of the competition was to get the Dante Collection."

"Right. The Dante Collection is a file archive. The archive was located on a secured, limited-access, fully-protected storage array of a multinational corporation."

Then he said the company name. You and I and several billion earthlings would certainly recognize the name and logo.

My mouth dropped open slightly.

"Yeah, I know," Lynx said. "Getting in wasn't easy. And since it was -" he spoke the company name again, preceded by a culturally-overused but appropriate expletive, "- they know security, obviously, so anyone trying to hack them better be elite, or they'd get Mitnicked awful fast."

"What was the hack?"

"He installed a covert WAP in the lobby of the building where one cluster of the hosting servers was located. He used that to remotely access the wired network. Then he installed keyloggers on a few PCs and damaged a few things to get admins to sign on and fix what he did. He used those logged admin credentials to break through an internal DMZ to get to the target storage array. Then he just FTP'd the Dante Collection to his own server."

"Nice kung-fu."

Lynx stood a little straighter. "Minotaur got in with a mixture of physical access, social engineering, and hacking. This was way beyond kung-fu. This was MMA."

Hearing stories of massive hacks was either fascinating or a disappointment. Sometimes I was let down, like when you guessed a magician's trick in the middle of a performance. But this hack was definitely in the first camp. It required guts, confidence, planning, luck, and a very solid skillset.

"He told me that from surveillance to traveling onsite to monitoring and hacking, the whole process took about a month."

"Seriously?" I was even more impressed. "That's really fast."

"Minotaur is really sick."

"So, he got the Dante Collection," I said, trying to parse the logistics. "But how did the AnonIT judges know he really did what he said he did?"

"They have a mole inside the company. They knew something more about the collection, about what files the Dante archive contained. There was one file unique to the collection. One file, that, if you owned it, it meant you had access to the Dante collection archive. That file is a picture. Once you see it, you know why it's kept so secure."

"This picture is the 'naked princess'?"

He swallowed and nodded.

"It's... probably the freakiest thing I've ever seen. I wish I'd never even looked."

"What is it? Porn? Violence? Republican talking points?"

"I don't even want to think about it."

My attempt at defusing the tension had failed. His eyes were haunted. He actually looked ill. I figured I had only seconds before he'd either refuse to talk, or he'd vomit. Either action would end the conversation in a way I'd not prefer.

"Come on, one picture can't be that bad," I said. "You can tell me. I've been dealing with nasty, ugly stuff for years. You ever had to work on Windows machines with pre-loaded OEM software?"

His eyes snapped back to mine. He almost snarled.

"You have no idea how horrible the picture is. Someone did some really bad stuff, and then decided to brag about it. Whoever did it - whoever took that picture - should be shot. I'm serious. They should be shot and killed."

He turned and walked away. He spoke his last words over his shoulder.

"If you ever get the chance to see the 'naked princess'... Just don't. Don't look at it, because you'll regret it the rest of your life."

## Chapter 0x9

Back in my office, I checked out the AnonIT results: P@nic had won the competition, too. Her name wasn't on Oober's list, but she was listed by the AnonIT channel's IRC bot. She was also the most recent winner - hers was the most recent hack attempt claimed and confirmed by the AnonIT judges. She probably hadn't included her name on Oober's list because, well, she'd written it herself.

That gave me the total list of winners: *patient zero*, *agent\_from\_harm*, *dragon\_bawls*, *minotaur*, and *chixor zed*. I added p@nic to the list.

I had a feeling that the people representing the names on this list were very dangerous.

Luckily for me, I might have an in with Minotaur. Lynx had told me how he'd made contact, and I'd do the same.

Time to introduce myself.

After a brief IRC chat, I'd scheduled a meeting with a guy who knew an IP who knew a bot who knew a compromised LAMP server who knew Minotaur. Later that hour we made the connection:

Minotaur: *who's knocking? name/id*

Me: *Dev Manny. ITPI. Friendly human.*

Minotaur: *means zero. tell me yr innermost thoughts*

Me: *The AnonIT competition. I have questions.*

Minotaur: *<sigh> ah more adoring fans. ok switch to webcam. vid /voice*

Me: *Sure. Protocol? Security?*

Minotaur: *doesn't matter don't care good luck i'm behind 7 proxies*

I lit up my webcam, and saw Minotaur.

A man sat on a couch, and that was a polite way of putting it.

If my office was homely, this guy's room was royalty-inbreeding-for-generations-mutated.

My first sight was that of trash. Boxes and food wrappers, bags and hardware. It almost looked as if the man never moved from his well-indented position on the stained middle cushion, and just dropped around him whatever he'd been recently eating and using.

Multitudes of shelves crowded the space and held piles of equipment, all using a Dr. Seuss-inspired stacking scheme. I saw old computers and their guts of circuit boards, memory sticks, and interface cards. Piles of books showed a spectrum of titles ranging from database architectural design to Amiga assembly programming. The walls were a study in New Age artwork, all with weird phrases that could be either motivational or pornographic. One poster behind the man was a tilted-perspective shot of a grimacing outdoorsy guy riding a jet-powered kayak up a waterfall. The caption read, *'Too real to feel the shocker'*.

Minotaur was way older than most hackers, probably in his early 70s. The remainder of his thin white hair had retreated to the back of his head in a final sad stand against male pattern baldness. He wore an old camouflage jacket that failed to hide its many stains. It was unzipped, and partially covered a dark shirt draped over a skeleton-thin body. His lower half wore thin, faded jeans that had been through a few thousand washings. His feet were bare, and their

deep tan matched that of his face and hands.

"That's better," the guy said as we studied each other. His voice was raspy, like he had to strain to push words from his throat. He had a trace of a Slavic accent, maybe Polish. "I've had a lot of wonderings and verbal permutations lately. Call me old-school, but video chat rocks. I want to see who I talk to. Get to know souls, not scripts."

Out of curiosity, I traced his connection. I assumed he'd already done the same to me.

His signal originated out of Chicago, USA. If his proxy comment was true, my trace meant nothing in terms of tracking him down. Given the generous helping of liver spots peeking through his heavy tan, Chicago was not his home turf.

Other indicators of his approximate global position were the thick curtains behind his couch. They were closed, but their edges glowed bright from outside sunlight. Wherever *Minotaur* was, at my time of night he had the luxury of midday sun and tropical weather.

"Dev Manny, Information Technology Private Investigator," he said. "We've never communed before."

"Never too late to start. I'm checking out what's happened to -"

"I know your intent. You are working to unravel the minds of the Fates and the AnonIT competition. You've fooled yourself into thinking my thoughts can raise yours to a new level, where you will light a candle in darkness and chase out a dragon."

This called for a shift in mental gears. I doubted I could respond with a similar insane-poet's response, so I tried the direct approach.

"Tell me why you entered the AnonIT competition."

Psychiatrist mode should give me information, and time to plan an appropriate follow-up.

"Because I knew I could win."

He looked at me carefully, suspicious now. So much for buying some time.

"You knew of me," he said. "You talked to entropy, and the chaos coalesced into this conversation. You really didn't expect that?"

I didn't answer because I didn't understand the question. I reassessed my position.

I wasn't sure if he was even picking up who I was or what I represented. I'd need a good justification to poke my electronic nose so far into his business. I shuffled through plausible reasons for contacting him, semi-truthful ploys that might get me information I wanted.

"I will open my mind to you. I will tell you what I know," he said.

This would be a pleasant surprise if it didn't make me immediately suspicious.

"That's very nice of you. My job doesn't usually come with free information."

He leaned towards his camera. I got a dermatologist-level view of his sun-damaged, sagging wrinkles. He looked disappointed, like there was an obvious, deep, metaphysical point I'd missed.

"Information wants to be free. This is the point of contests like AnonIT. That's my intent. I unearth information that's hidden by others."

"What information?"

"Doesn't matter. Actual bytes are meaningless. Trapped data needs to be freed. Otherwise, we craft political shackles, life stagnates, civilization grows cold. Freedom, change, and progress are the natural states of things."

I'd heard this argument before, and my natural skepticism rolled its eyes.

"If all information is free," I said, "Wouldn't that, you know, *destroy society*? Empty bank accounts? Unlock every piece of private property? No home would be safe. Every car would be stolen. Nation-controlled bioweapons and nukes would be free to anyone with the ability to make them. You want complete informational freedom, but you hide behind your seven proxies. It seems like the price of exposing all information... is anarchy."

He grinned at me, a smile containing dark, receding gums and mostly original teeth.

"I'm also a realist. Let's just say I don't support any major political party."

Cute. I'd never before met a militant hippie altruistic anarchist hacker.

"So, what happens now?" I said. "You scratch my back, then empty my Bitcoin wallet?"

"Nah," he waved me away. "You and I, we are solid. I have no desire to destroy society or people. I focus all of my mana on the one thing I do really, really well. Like -"

"Like... Freeing information from the confines of those who would keep it locked away from the natural order."

Saying that sentence exercised brain muscles I rarely used. I didn't know how this guy did it.

"Yeah," his smile was beatific. "You understand."

"Thanks. And I'll take whatever you're willing to tell me."

He did. It was a little more ethereal and symbolic than I needed, but he told me about the hack, and what he did to break in. He told me about the Dante Collection.

First was the name itself.

The "Dante collection" was an informal name, but was derived from the server names where the file collection was stored. Named after the "nine circles of Hell" as written by the 14th century author Dante Alighieri, the network had systems called GREED, GLUTTONY, FRAUD, ANGER, and LUST. With one possible exception, this server farm didn't sound very fun.

Minotaur described the Dante collection as mostly financial reports, credit reports, accounting and payroll databases, customer billing data, and all the usual stuff that any sensible company needs to keep hidden.

The collection was physically located inside of a demilitarized zone designed to provide an extra layer of security for whatever needed protecting. Entrance into the DMZ was via three-factor authentication, with an environment that booted a custom, limited-access virtual machine that was built on-demand and destroyed after each use. The Dante collection was very, very secure.

Minotaur got in, however. Few people would understand the incredible effort he'd gone through to get his result. As Lynx had implied, this ran the spectrum from physical trespass to social engineering to straight up black-hat hacking.

It made me wonder about P@nic. She was good, certainly. But was she *this* good? She was only fifteen. Did she really have the ability, money, time, and freedom necessary to hack like this? I didn't know. I'd have to ask her.

So I'd better find her.

"Hackers today," Minotaur was saying, "are mostly tourists clustered around a few truly talented beings. The tourists have no vision, no end game, no goal beyond that of exploration. Sometimes that's wonderful, but not with AnonIT. Get far enough, and no mistakes are allowed. Any permutation outside of winning will put you in the same place as the information you're trying to free: You'll be locked up. Every step must be a recursive gameboard eval to find the best of all possible actions. I told P@nic this, too."

Theory was fascinating, but not what I wanted to discuss at the moment. Particularly after he mentioned P@nic.

"Just watch out, okay?" I said. "With your mantra of 'information wants to be free,' you could still hurt people, or have people come after you."

"I observe, then think, then act. I am very careful. I don't need laws to mandate my actions. Not if I'm moral. Unlike the rest of this broken world, I am aware of my impact. I'm responsible."

"That's a fancy way of saying, '*I know what I'm doing.*' Famous last words."

"My results speak louder than this conversation."

"How did you help P@nic?"

He shrugged. "I gave him knowledge, enlightened him with technique and method."

As with Lynx, Minotaur had no clue that P@nic was a girl.

"Information wants to be free," I said. "Did you give P@nic the Dante Collection?"

He chuckled. "I tried, but he refused. He wanted to earn it!"

"P@nic completed the AnonIT challenge, and has the Dante Collection. Or had it."

Minotaur's head tilted slowly to the side.

"Good. I'm happy to have edified. But what do you mean, he 'had' it?"

"You didn't run a video chat with P@nic, did you?"

He grinned. "No. He insisted on text. It misses the human element, but is efficient in the right hands."

"P@nic is a fifteen-year-old-girl. Now she's disappeared."

His grin dropped, along with his saintly bravado.

"A girl... She's just a child? I didn't know she was so young. We only chatted. I can send you all the logs."

"Thanks. I'm working for someone who'd like to find her."

"Who?" He leaned forward again, an almost crazed look of interest on his face. "Tell me. Now."

"I'm not like you," I said, realizing that even with his assurances, I didn't trust him as much as Lynx. "Sometimes, it's safer to keep things hidden. Like the name of my client. I can't break that -"

He lunged towards the camera and the video image seized.

"Tell me!"

The shout overloaded his webcam's cheap microphone, and his voice came sheathed in static, complementing his twisted face.



"We'll agree to disagree," I said. "But I'll contact you when this is over. After I've figured out what happened to P@nic. Call it my thanks to you for getting me this far."

He sat back and looked thoughtful. The emotion purged so quickly, I didn't know if he'd really meant the anger, or if it was just a cheap attempt at intimidation.

"You can't imagine what you're getting involved with," he said.

"All part of the fun," I said. "For example, I know about the 'naked princess.'"

His skin paled under his tan, making him look suddenly frail and sickly.

"You've *seen* the naked princess?"

"No. But I've heard about it."

"Then you know nothing. Keep it that way."

"Come on," I smiled. "What about information wanting to be free? Can't you -"

"Shut up and listen." His voice was lower,

his Slavic accent stronger. "Some things should not be known. By anyone. Some actions should never be taken. This is one of those things. If you hear anything from anyone about the naked princess, get away. Immediately."

"What about P@nic?" I said. "She has the Dante Collection. She might've seen the picture."

He sat back, his posture more relaxed, but his eyes were still intense.

"I didn't say anything about it to her. It lives in the collection, but it's only a few megs tarballed among terabytes. But whether or not she's seen it, if she's got the Dante Collection, she's got the naked princess. I'm telling you, drop her. You don't want to get involved."

"I know what I'm doing. Some of your own philosophy applies to me: I'm aware of my actions. I'm responsible."

He looked at me with scorn and pity.

"You are wrong, kid. Way wrong."

## HOPE-X PREREGISTRATION IS OPEN!

Announcing the newest Hackers On Planet Earth conference, to be held at the recently rescued Hotel Pennsylvania in New York City, July 18, 19, and 20, 2014

Preregistration is easy! Just visit [store.2600.com](http://store.2600.com) and order your tickets. You'll get an email confirmation and you'll be set. Thanks to the hard work of so many great people, we're able to continue to keep the price extremely low for a conference of this kind in the middle of one of the busiest places in the world. (Check [x.hope.net](http://x.hope.net) for deals on hotel rooms for conference attendees.)

We will once again have in excess of 100 speakers and talks, break-out sessions, workshops, concerts, all sorts of villages (hackerspace, lockpicking, hardware hacking, and the like), Segway rides, art displays, contests, retro computing, and new things still being developed!

Interested in speaking? HOPE-X wants to hear from you! Just email [speakers@hope.net](mailto:speakers@hope.net) and let us know in a few paragraphs what you want to address, who you are, and other relevant info. Guidelines are at [x.hope.net](http://x.hope.net).

None of this would be possible without the hundreds of volunteers who pitch in to make it all happen. If you want to be a part of that, send an email to [volunteers@hope.net](mailto:volunteers@hope.net) and let us know if there's something specific you can do or if you're able to simply be sent where you're needed.

Finally, our biggest challenge as always remains getting the word out. We don't have a big PR team, just a magazine, radio show, website, and lots of friends. But we would be thrilled to have the word spread before the conference so that more new people get to experience this and not simply read all the amazing press we get after it's all over. If you can help, email [press@hope.net](mailto:press@hope.net) and give us your ideas.

HOPE-X is our 10th conference, the 20th anniversary of our first conference, and the 30th anniversary of 2600! It's all lining up so perfectly. We hope to see you there.

[xxx.xxxxxxxxxxxxxxxxxxxx.xxx](http://xxx.xxxxxxxxxxxxxxxxxxxx.xxx) (likely the coolest domain name EVER)

or [x.hope.net](http://x.hope.net) (for those who can't or won't visit the .xxx domain)

# HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under \$150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, *email us* at [happenings@2600.com](mailto:happenings@2600.com) or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA**. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

January 17-19

**ShmooCon**

Washington Hilton Hotel  
Washington DC  
[www.shmoocon.org](http://www.shmoocon.org)

June 5-6

**RVasec**

Commonwealth Ballroom  
Virginia Commonwealth University Campus  
Richmond, Virginia  
[rvasec.com](http://rvasec.com)

January 18-19

**Maker Faire Oslo**

The Norwegian Museum of Science and Technology  
Oslo, Norway  
[makerfaireoslo.no](http://makerfaireoslo.no)

June 13-15

**CircleCityCon**

Hyatt Regency Indianapolis  
Indianapolis, Indiana  
[circlecitcitycon.com](http://circlecitcitycon.com)

April 10-13

**Notacon 11**

Cleveland Marriott East  
Warrensville Heights, Ohio  
[www.notacon.org](http://www.notacon.org)

July 9-13

**ToorCamp 2014**

Hobuck Beach Resort  
Neah Bay, Makah Indian Reservation, Washington  
[toorcamp.org](http://toorcamp.org)

April 17-21

**Easterhegg 2014**

Kulturhaus Arena  
Stuttgart, Germany  
[eh14.easterhegg.eu](http://eh14.easterhegg.eu)

July 18-20

**HOPE X**

Hotel Pennsylvania  
New York, New York  
[x.hope.net](http://x.hope.net)

April 26-27

**Maker Faire UK**

Centre for Life  
Newcastle, England  
[www.makerfaireuk.com](http://www.makerfaireuk.com)

August 7-10

**DEF CON 22**

Rio Hotel and Casino  
Las Vegas, Nevada  
[www.defcon.org](http://www.defcon.org)

May 16-18

**CarolinaCon 10**

North Raleigh Hilton  
Raleigh, North Carolina  
[www.carolinacon.org](http://www.carolinacon.org)

September 20-21

**World Maker Faire New York**

New York Hall of Science  
Queens, New York  
[www.makerfaire.com](http://www.makerfaire.com)

May 17-18

**Maker Faire Bay Area**

San Mateo Event Center  
San Mateo, California  
[www.makerfaire.com](http://www.makerfaire.com)

*Please send us your feedback on any events you attend and let us know if they should/should not be listed here.*

# Marketplace

## Events

**HOPE X. 2600** presents the tenth Hackers On Planet Earth conference at New York City's Hotel Pennsylvania July 18-20, 2014. Visit [xxx.xxxxxxxxxxxxxxxxxxxx.xxx](http://xxx.xxxxxxxxxxxxxxxxxxxx.xxx) or [x.hope.net](http://x.hope.net) for the latest news, travel info, special hotel rates, etc. Speakers wanted: email [speakers@hope.net](mailto:speakers@hope.net). Volunteers wanted: email [volunteers@hope.net](mailto:volunteers@hope.net). Vendors wanted: email [vendors@hope.net](mailto:vendors@hope.net). Projects wanted: email [projects@hope.net](mailto:projects@hope.net). You get the idea. You can help define what HOPE X focuses on and be a real part of hacker history, right in the middle of midtown Manhattan, across the street from the busiest train station in America. You can also join our announcement mailing list from the main page of our websites. Call (212) PENnsylvania 6-5000 for the special conference room rate.

## For Sale

**FINAL CHANCE FOR THE 2014 HACKER CALENDAR.** As you may know, 2014 has already begun, so don't let another day go by without this amazing calendar. Learn what happened in hacker history for every day of the year and see some amazing payphone photography for every month of the year. Email [calendar@2600.com](mailto:calendar@2600.com) or visit [store.2600.com](http://store.2600.com) while supplies last.

**BLUETOOTH SEARCH FOR ANDROID** searches for nearby discoverable Bluetooth devices. Runs in background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download @ <http://tinyurl.com/btscan>.

**CLUB-MATE** is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Now available in two quantities: \$36.99 per 12 pack or \$53.99 per 18 pack of half liter bottles plus shipping. Bulk discounts for hacker spaces are quite significant. Write to [contact@club-mate.us](mailto:contact@club-mate.us) or order directly from [store.2600.com](http://store.2600.com).

**A TOOL TO TALK TO CHIPS.** It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only \$30 including world wide shipping. Check out this open source project and more at [DangerousPrototypes.com](http://DangerousPrototypes.com)

**TV-B-GONE.** Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! 2600 readers get the keychains for 10% discount by using coupon code: 2600REAL. [www.TVBGone.com](http://www.TVBGone.com)

## Announcements

**WHISTLEBLOWER EDWARD SNOWDEN** is currently in Russia where he has been granted temporary asylum. The United States government is exerting substantial pressure on Russia and other countries in an attempt to force Mr. Snowden to the United States where he will face decades in prison or worse. Mr. Snowden's legal defense and its associated public campaign will be a long and expensive journey which will only be overcome with your financial help. Support the right to know. Support Edward Snowden. <https://wikileaks.org/freesnowden> Donation methods include online credit card or PayPal. Checks can be mailed to Derek Rothera & Company, Chartered Accountants, Units 15 & 16, 7 Wenlock Road, London N1 7SL, United Kingdom. Bitcoins can be sent to 1snowqQP5VmZgU47i5AWwz9fsgHQg94Fa.

## Help Wanted

**ARTIST AND PHOTOSHOP NINJA NEEDED.** Small ebook publisher needs a Photoshop ninja/graphic artist/true artist to create 5 book covers during the next 5 months, and a further 15 covers during the following 18 months. We are not a big, greedy multinational publisher, so we will pay a reasonable amount, we will treat you with respect, and we will give you the credit you deserve. Our owners are longtime friends of 2600 and HOPE. Send contact info and portfolio samples, if any, to: [librosfirst@gmail.com](mailto:librosfirst@gmail.com).  
**NEED HELP IN DECRYPTING A WINZIP DATA FILE,** password was lost! Also, want any or all Facebook, LinkedIn, or social data with name, email, and/or photos. Contact Joe: [soldato13@yahoo.com](mailto:soldato13@yahoo.com)

## Wanted

**INTRODUCING GSCSI** - Global Strategic Cyber Studies Institute: We are a startup with solid senior leadership and a mission that calls for change to the current mentality regarding the negative connotations associated with the term "Hacker". We are all hackers in one way or another and we want to put forward and proudly carry the wisdom behind some incredibly talented individuals. In fact, we don't hire anyone who "doesn't get it". We need help to grow and develop a revenue stream, and are seeking volunteers for positions in curriculum development, instructional design,

instructors (virtual and classroom). We also are looking for any interested candidates to serve on our Advisory Board. Also, if you are interested in public speaking at Cyber events and are willing to travel the globe, let us know. Please send any questions or expressions of interest to 2600team@gscsi.org. Please help us reshape the cyber world and thinking one mind at a time, if need be.

**AUTHOR WILL PAY UP TO \$1,000 FOR TECHNICAL CONSULTANT** re: current technical methods and tactics used to hack voice mail accounts, i.e. England, U.S., and elsewhere. cdg (dot) book (at) yahoo (dot) com

## Services

**THOUSANDS OF GOVERNMENT DOCUMENTS** are published at GovernmentAttic.org. New material available each week. Click on the Documents homepage link to start.

**WANT SOMEONE'S FBI FILE?** Check out GetGrandpasFBIfile.com, a site that shows you how to get the FBI files for any dead person. Or use GetMyFBIfile.com, the site that shows you how to get your own FBI file. **GET YOUR HAM RADIO LICENSE!** KB6NU's "No-Nonsense" Study Guides make it easy to get your Technician Class or General Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from [www.kb6nu.com/tech-manual](http://www.kb6nu.com/tech-manual). E-mail [cwgeek@kb6nu.com](mailto:cwgeek@kb6nu.com) for more information.

**DIGITAL FORENSICS FOR THE DEFENSE!** Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or email us at [sensei@senseient.com](mailto:sensei@senseient.com).

**INTELLIGENT HACKERS UNIX SHELL:** Reverse. Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from \$5/month, with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon Code: Save2600. <http://www.reverse.net/>

**NO PAY CLASSIFIEDS.COM** - Free advertising - 50 countries! Free business directory, classified ads (6 free photos) with link to your website to help you expand your business and improve search engine placement. Search over 35 million classified ads (mostly USA) to help you find what you want. Thank you for being part of our online audience!

**SECURE UNIX SHELLS & HOSTING SINCE 1999.** JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular \*nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCd, and web sites w/SQL. 2600 readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) adds free WHOIS privacy to all domains registered or transferred in!

**BASEMENT TECHIE AND THE DYSTONAUT:** Two great tastes that taste great together! Better than a kick in the ass with a steel toe boot! DIY - Dystopias - Poor Hackers playing with Electronics and RF - Living Outside The System - by Ticom - <http://www.oberonsrest.net/>

## Personal

**NO JUSTICE NO PEACE FOR GHOST EXODUS.** Former ETA and Anonymous /h/ (Scientonymously aka 74K71X, 4chan, 94chan) member looking for anyone willing to help me tell the story about my case and broadcast it out behind these prison walls to reach the masses, and hopefully gain the attention and legal aid I deserve, but can't afford (EFF?). Get a Google Voice # with my local 409 area code, then write me at the address below. Let me explain via telephone (while you record it) in detail how far the DoJ went to manufacture fictitious, unsubstantiated "facts" in order to bury me with a historic conviction to send a message to other hackers. Jesse McGraw, #38690-177, PO Box 26020, Beaumont, TX 77720.

**CURRENT WEB-HOSTING PROVIDER** looking for your help in this new digital age. I am currently locked up in the B.O.P., but I am due for release this October. I am currently accepting new applicants who have any knowledge of any of the following: domain registration, web hosting, IRC.ircd hosting, SHOUTcast hosting, Ventrilo hosting, TeamSpeak hosting, VoIP hosting, cloud-based services, networking, server management, and more! This list goes on and on but will give more details on request. This opportunity will not last as we are limited on this great offer. For those of you who have written me a letter and have not heard from me, I apologize. A lot of letters don't reach me for some odd reason. I am willing to write to anybody even if it's not regarding this ad. A pen pal is nice once in a while. I reply to all letters received. Chris Douglas 14329-298, Big Spring FCI, 1900 Sim ler Ave., Big Spring, TX 79720. All mail is welcome. Write me as much as you like! Email is available, but I need your email address first.

## 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. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to [subs@2600.com](mailto:subs@2600.com).

**Deadline for Spring issue: 2/21/14.**



# NOBODY SAW THIS COMING. **TWO BRAND NEW 2600 SHIRTS RELEASED AT THE SAME TIME!**

Our 30th anniversary shirt shows a pictorial progression of our history from floppy to CD to flash drive, the contents of which have consistently caused panic for those in power at the time. On the back is a collection of our headlines from each of our 30 years, done up in traditional 2600 style.



But wait! There's more. You didn't think we could just let all of this NSA business go by and only write about it in these pages? Well, now we're also writing about it on clothing! On the front of our new NSA shirt is a forbidden image of the NSA headquarters (our staffers were detained minutes after capturing it), along with our interpretation of what their acronym really stands for. On the back is a leaked image of the now infamous PRISM program, along with some very good advice for those who want to hold onto their privacy.



Shirts are black with blue & white writing (30th anniversary) and red & white writing (NSA) \$20 each in sizes from S to XXXL. (Add \$5.25 per shirt for overseas orders)

Visit [store.2600.com](http://store.2600.com) for special deals.

2600  
PO Box 752  
Middle Island, NY 11953 USA  
+1 631 751 2600

*"If we can't understand the policies and the programs of our government,  
we cannot grant our consent in regulating them." - Edward Snowden*

**Editor-In-Chief**  
Emmanuel Goldstein

**S** **Infrastructure**  
flyko

**Associate Editor**  
Bob Hardy

**T** **Network Operations**  
phiber

**Layout and Design**  
Skram

**A** **Broadcast Coordinator**  
Juintz

**Cover**  
Dabu Ch'wald

**F** **IRC Admins**  
beave, koz, r0d3nt

**Office Manager**  
Tampruf

**F**

**Inspirational Music:** Tele:Funken, Ryan Latham, Electric Light Orchestra, Penetration, Shanneyganock, Los Aterciopelados, Mindless Self Indulgence, Klaatu, Yann Tiersen, Cat Power, Kalyanji & Anandji, Donner Party, Buckethead, Phaeleh & I-Mitri, Juno Reactor, Bassnectar

**Shout Outs:** Miles, Olssy, Soma, Sean\*4, Drew, Sherry Huss, NYC Resistor

**Welcome:** Hudson

**Thank You:** Banksy

**2600 is written by members of the global hacker community.**

**You can be a part of this by sending your submissions to  
articles@2600.com or the postal address below.**

.....  
**2600** (ISSN 0749-3851, USPS # 003-176);  
*Winter 2013-2014, Volume 30 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. & Canada - \$27 individual,  
\$50 corporate (U.S. Funds)  
Overseas - \$38 individual, \$65 corporate

**BACK ISSUES:**

1984-1999 are \$25 per year when available.  
Individual issues for 1988-1999  
are \$6.25 each when available.  
2000-2013 are \$27 per year or \$6.95 each.  
Shipping added to overseas orders.

**LETTERS AND ARTICLE  
SUBMISSIONS:**

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

**2600 Office/Fax Line: +1 631 751 2600**

Copyright © 2013-2014; 2600 Enterprises Inc.

**ARGENTINA**  
Buenos Aires: Bar El Sitio,  
Av de Mayo 1354.

**AUSTRALIA**  
Melbourne: Level 2 food court,  
Melbourne Central Dome.  
Sydney: The Crystal Palace  
Hotel, 789 George St. 6 pm

**AUSTRIA**  
Graz: Cafe Haltestelle  
on Jakominiplatz.

**BELGIUM**  
Antwerp: Central Station, top of  
the stairs in the main hall. 7 pm

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

**CANADA**  
Alberta

Calgary: Food court of Eau  
Claire Market. 6 pm  
Edmonton: Elephant & Castle  
Pub, 10314 Whyte Ave., near  
big red telephone box. 6 pm

**British Columbia**  
Kamloops: Student St in Old Main in  
front of Tim Horton's, TRU campus.

**Vancouver ( Surrey )**: Central  
City Shopping Centre food  
court by Orange Julius.

**Manitoba**  
Winnipeg: St. Vital Shopping  
Centre, food court by HMV.

**New Brunswick**  
Moncton: Champlain Mall  
food court, near KFC. 7 pm

**Newfoundland**  
St. John's: Memorial University  
Center Food Court (in front  
of the Dairy Queen).

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

**Toronto**: Free Times Cafe,  
College and Spadina.

**Windsor**: Sandy's, 7120  
Wyandotte St E. 6 pm

**Quebec**  
Montreal: Bell Amphitheatre,  
1000, rue de la Gauchetiere  
near the Dunkin Donuts in the  
glass paneled area with tables.

**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

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

**Leeds**: The Brewery Tap Leeds. 7 pm  
**London**: Trocadero Shopping  
Center (near Piccadilly Circus),  
lowest level. 6:30 pm

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

**Norwich**: Entrance to Chapelfield  
Mall, under the big screen TV. 6 pm

**FINLAND**  
Helsinki: Fennia-kortelli food  
court (Vuorikatu 14).

**FRANCE**  
Cannes: Palais des Festivals & des  
Congres la Croisette on the left side.  
Grenoble: EVE performance  
hall on the campus of Saint  
Martin d'Heres. 6 pm

**Lille**: Grand-Place (Place Charles  
de Gaulle) in front of the Furet  
at Nord bookstore. 7:30 pm

**Paris**: Quick Restaurant, Place  
de la Republique. 6 pm

**Rennes**: Bar le Golden Gate, Rue  
St Georges a Rennes. 8 pm

**Rouen**: Place de la Cathedrale,  
benches to the right. 8 pm  
**Toulouse**: Place du Capitole by

the benches near the fast food and  
the Capitole wall. 7:30 pm

**GREECE**  
Athens: Outside the bookstore  
Papasotiropi on the corner of  
Patission and Stourmari. 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**  
Kagoshima: Amu Plaza next to  
the central railway station in  
the basement food court (Food  
Cube) near Doutor Coffee.

**Tokyo**: Mixing Bar near  
Shinjuku Station, 2 blocks  
east of east exit. 6:30 pm

**MEXICO**  
Chetumal: Food Court at La Plaza de  
Americas, right front near Italian food.

**Mexico City**: "Zocalo" Subway  
Station (Line 2 of the "METRO"  
subway, the blue one). At the  
"Departamento del Distrito Federal"

exit, near the payphones and the  
candy shop, at the beginning of the  
"Zocalo-Pino Suarez" tunnel.

**NETHERLANDS**  
Utrecht: In front of the Burger King  
at Utrecht Central Station. 7 pm

**NORWAY**  
Oslo: Sentral Train Station  
at the "meeting point" area  
in the main hall. 7 pm

**Tromsø**: The upper floor at Bla  
Rock Cafe, Strandgata 14. 6 pm

**Tromsheim**: Rick's Cafe  
in Nordgate. 6 pm

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

**Trujillo**: Starbucks, Mall  
Aventura Plaza. 6 pm

**PHILIPPINES**  
Quezon City: Chocolate Kiss ground  
floor, Bahay ng Alumni, University  
of the Philippines Diliman. 4 pm

**SWEDEN**  
Stockholm: Central Station,  
second floor, inside the exit to  
Klarabergsviadukten above main hall.

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

**WALES**  
Ewloer: St. David's Hotel.

**UNITED STATES**  
Alabama

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

**Huntsville**: Newk's, 4925  
University Dr. 6 pm

**Arizona**  
Phoenix: Cartel Coffee Lab. 6 pm  
Prescott: Method Coffee, 3180  
Willow Creek Rd. 6 pm

**Arkansas**  
Ft. Smith: River City Deli at  
7320 Rogers Ave. 6 pm

**California**  
Los Angeles: Union Station,  
inside main entrance (Alameda  
St side) between Union Bagel  
and the Traxx Bar.

**Monterey**: East Village  
Coffee Lounge. 5:30 pm  
Sacramento: Hacker Lab, 1715 I St.

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

**San Francisco**: 4 Embarcadero Center  
near street level fountains. 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**  
Colorado Springs: The Enclave  
Coop, 2121 Academy Circle. 7 pm

**Loveland**: Starbucks at Centerra  
(next to Bonifelli Grill). 7 pm

**Connecticut**  
Newington: Panera Bread,  
3120 Berlin Tpke. 6 pm

**District of Columbia**  
Arlington: Champs Pentagon,  
1201 S Joyce St (in Pentagon  
Row on the courtyard). 7 pm

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

**Jacksonville**: O'Brothers Irish  
Pub, 1521 Margaret St. 6:30 pm

**Melbourne**: Matt's Casbah, 801  
E New Haven Ave. 5:30 pm

**Sebring**: Lakeshore Mall food  
court, next to payphones. 6 pm

**Titusville**: Krystal Hamburgers,  
2914 S Washington Ave (US 1).

**Georgia**  
Atlanta: Lenox Mall food court. 7 pm

**Hawaii**  
Hilo: Prince Kuhio Plaza food  
court, 111 East Puainako St.

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

**Pocatello**: Flipside Lounge,  
117 S Main St. 6 pm

**Illinois**  
Chicago: Golden Apple, 2971  
N. Lincoln Ave. 6 pm

**Peoria**: Starbucks, 1200 West Main St.

**Indiana**  
Evansville: Barnes & Noble cafe  
at 624 S Green River Rd.

**Indianapolis**: Tomlinson Tap Room in  
City Market, 222 E Market St. 6 pm

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

**Davenport**: Co-Lab, 1033 E 53rd St.

**Kansas**  
Kansas City (Overland Park):  
Barnes & Noble cafe, Oak Park Mall.

**Wichita**: Riverside Perk,  
1144 Biting Ave.

**Louisiana**  
New Orleans: Z'otz Coffee House  
uptown, 8210 Oak St. 6 pm

**Maine**  
Portland: Maine Mall by the bench  
at the food court door. 6 pm

**Maryland**  
Baltimore: Barnes & Noble  
cafe at the Inner Harbor.

**Massachusetts**  
Boston: Stratton Student Center  
(Building W20) at MIT in the  
2nd floor lounge area. 7 pm

**Worcester**: TESLA space  
- 97D Webster St.

**Michigan**  
Ann Arbor: Starbucks in The  
Galleria on S University. 7 pm

**Missouri**  
St. Louis: Arch Reactor Hacker  
Space, 2400 S Jefferson Ave.

**Montana**  
Helena: Hall beside OX  
at Lundy Center.

**Nebraska**  
Omaha: Westroads Mall food  
court near south entrance,  
100th and Dodge. 7 pm

**Nevada**  
Elko: Uber Games and Technology,  
1071 Idaho St. 6 pm

**Reno**: Barnes & Noble Starbucks  
5555 S. Virginia St.

**New Mexico**  
Albuquerque: Quelab Hacker/  
MakersSpace, 1112 2nd St NW. 6 pm

**New York**  
Albany: SUNY Albany Transfer  
& Commuter Lounge, first  
floor, Campus Center. 6 pm

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

**Rochester**: Interlock Rochester, 1115  
E Main St, Door #7, Suite 200. 7 pm

**North Carolina**  
Charlotte: Panera Bread, 9321 JW Clay  
Blvd (near UNC Charlotte). 6:30 pm  
**Greensboro**: Caribou Coffee, 3109  
Northline Ave (Friendly Center).  
**Raleigh**: Royal Bean Coffee Shop,  
3801 Hillsborough St (next to the  
Playmakers Sports Bar and across  
from Meredith College). 7 pm

**North Dakota**  
Fargo: West Acres Mall food court.

**Ohio**  
Cincinnati: Hive13, 2929  
Spring Grove Ave. 7 pm

**Cleveland (Warrensville Heights)**:  
Panera Bread, 4103 Richmond Rd. 7 pm

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

**Dayton**: Marions Pizza ver.  
2.0, 8919 Kingsridge Dr., behind  
the Dayton Mall off SR-741.

**Youngstown (Niles)**: Panera Bread,  
5675 Youngstown Warren Rd.

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

**Oregon**  
Portland: Theo's, 121  
NW 5th Ave. 7 pm

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

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

**Philadelphia**: 30th St Station,  
food court outside Taco Bell.

**Pittsburgh**: Tazz D'Oro, 1125  
North Highland Ave at round  
table by front window.

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

**Puerto Rico**  
San Juan: Plaza Las  
Americas on first floor.

**Trujillo Alto**: The Office  
Irrish Pub. 7:30 pm

**South Dakota**  
Sioux Falls: Empire Mall,  
by Burger King.

**Tennessee**  
Knoxville: West Town  
Mall food court. 6 pm

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

**Nashville**: J&J's Market &  
Cafe, 1912 Broadway. 6 pm

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

**Dallas**: Wild Turkey, 2470  
Walnut Hill Lane, outside porch  
near the entrance. 7:30 pm

**Houston**: Ninja's Express seating  
area, Galleria IV. 6 pm

**Vermont**  
Burlington: The Burlington Town  
Center Mall food court under the stairs.

**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

**Richmond**: HackRVA 1600  
Rosenath Rd. 6 pm

**Virginia Beach**: Pembroke  
Mall food court. 6 pm

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

**Spokane**: The Service Station,  
9315 N Nevada (North Spokane).

**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.



# Payphones of the World



**Croatia.** This phone is completely operational, and it can be found on the ferry from the city of Split to the island of Vis. The phone carries the initials of a now defunct company (Hrvatska Pošta i Telekomunikacije), which hasn't existed since the 1990s.

*Photo by Bojan Paduh*



**Australia.** A truly remote phone, found in a place called Winning Pool on the North West Coastal Highway around 150 miles from any people. The coin mechanism has been completely removed, ostensibly to save the phone company the 300 mile trip to empty it.

*Photo by Astrant Photographic*



**Barbados.** Seen in Bridgetown, this phone carries the familiar logo of parent company Cable and Wireless to the left of the BarTel name, a very familiar sight throughout the Caribbean.

*Photo by Kristyn Rose*



**Uganda.** Spotted in Mukono, this phone is operated by Mobile Telephone Networks, a company based in South Africa that has expanded its operations to over 20 countries in Africa and the Middle East.

*Photo by TC Johnson*

Visit <http://www.2600.com/phones/> to see our foreign payphone photos!  
(Or turn to the inside front cover to see more right now.)



# The Back Cover Photos

November 25, 1977

Baby Boy

( )

Service	Fees Charged
Partial Reimbursement on Maternity Care	\$1,221.00
Average Cost per Infant (attached)	\$ 659.00
Partial Social Service Fee for Adoption	\$ 500.00
Estimated Costs of Legal Proceedings for Termination of Parental Rights	\$ <u>220.00</u>
Total Reimbursement	\$2,600.00

So **momentumdave** was going through some old papers concerning his adoption and discovered that he was worth exactly \$2600 at the time. How cool is *that*? Incidentally, we can't help but wonder if the actual infant was the attachment referred to in "Average Cost per Infant (attached)."



Now this is something we find ourselves wanting more than anything - a true hacker radio, as discovered by **sarx** in Scotland. Had this company only stayed in business another 30 years or so, this would have been the perfect gift for *Off The Hook* listeners.

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](mailto: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) or a 2600 t-shirt of your choice.