

Volume Thirty-Six Number Four

DIGITAL EDITION Winter 2019-2020

2600

The Hacker Quarterly

Boomer

OK
Not OK

Boomer Search

Get Off Lawn

Unusual Payphones



South Korea. We thought this phone had a very unique design. It looks like someone crammed a cell phone into it, but we're assured that isn't actually the case. Spotted in Seoul.

Photo by Sam Pursglove



Sweden. Found on the island of North Koster (almost certainly the westernmost phone in this country), this is an example of the times changing. Once purported to house the only landline in the area, this booth is now dedicated to preserving ancient reading devices

Photo by miggedymax



France. Not actually a payphone, but it's definitely unusual. You've likely never come upon one of these, unless you're a French coal miner. This was seen at the Hély d'Oissel mine in Greasque.

Photo by Mike LINUX



Canada. Probably the most unusual of the bunch, these were found at Vancouver International Airport. When was the last time you saw three working phones next to each other that all took coins, cards, and codes?

They even have phone books! *Photo by Estragon*

Got foreign payphone photos for us? Email them to 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 (Do not send us links as photos must be previously unpublished.)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)

REALITIES

thank you elliot

From the Ashes	4
Industrial Control with Modbus	6
Ideas Behind Site Reliability Engineering	9
Cyberspelunking	10
TELECOM INFORMER	13
Steganographic Filesystems	15
Death of a Scene	18
Body Key-Logging	20
HACKER PERSPECTIVE	26
Rehabilitation Center - (Attacker's) Mission Complete	29
How to Get Free Wi-Fi Anywhere	30
What is Hacking?	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
Maximizing Privacy in a Digital World	47
Do-It-Yourself Cloudflare on a Budget	50
Book Review: Artificial Intelligence: A Very Short Introduction	51
CITIZEN ENGINEER	52
Reflections on Hackers	54
Pass the Cookie and Pivot to the Clouds	57
Fiction: Hacking the Naked Princess 0x18	59
HACKER HAPPENINGS	61
MARKETPLACE	62
Student Privacy by Practice - Not by Policy (fixing our mistake)	65
MEETINGS	66

From the Ashes

We've been here before. But it never gets old.

We're referring to the scenario we often find ourselves in, where things appear to be hopeless or doomed for one reason or another. Distributors have vanished owing us large sums of money that we need to survive. We've gotten sued by everyone from the entire motion picture industry to the Ford Motor Company, threatening our very existence. And we continue to see fellow writers and members of the hacker community unfairly prosecuted and faced with life-destroying actions by authorities with unlimited resources and no shame in pushing false narratives. But somehow, throughout all of that, we always manage to come back with renewed spirit and determination.

Of course, the "somehow" really isn't that much of a mystery. Simply put, it's the massive amount of support and positivity shown to us and many others by the people in the hacker community. Without this amazing collection of individuals, so much would be impossible. And that extends well beyond the challenges we're talking about here. The innovations and inventions that hackers are responsible for have helped to change just about everything in our world today, from tech companies to telephones to the manner in which we protect speech and freedom. We can't ever forget this, nor can we let these accomplishments be tarnished or subverted by those who either don't get it at all or who are in this for the wrong reasons.

2019 brought us numerous challenges that could have been really depressing had we not been so used to them - and emboldened by our support network.

Earlier in the year, we were told that our magazine couldn't be put on newsstands in the United Kingdom because it might attract

"negative publicity" and subject us to fines of over \$13,000 per complaint! This said a lot more about what's happened to the U.K. than anything having to do with us. Since we never profited from sending issues overseas in the first place, these developments didn't actually hurt us. But the story gave us much more visibility in that country and led to more people subscribing to both the printed and digital editions. Still, the whole thing remains unsettling for anyone who values freedom of the press, reading, democracy, etc.

More recently, Google has decreed that we are something called a "replica magazine" that they will no longer carry in the digital magazine section of their Google Play platform. Apparently, they intend to redefine what a magazine is and we don't qualify. Yes, it's somewhat priceless that a corporation like Google is telling *us* what a magazine is. But again, this didn't really hurt us since Google's terms were always pretty poor and they never attracted anywhere near the same amount of readers as the Kindle. Again, though, it's unsettling to see how publications are being manipulated by people without a clue who probably shouldn't be in this business to begin with.

And, of course, we almost lost the radio station that broadcasts *Off The Hook*, our hacker radio show that's been on the air since 1988. In October, a minority faction of the parent Pacifica Foundation shut down local broadcasting of WBAI-FM in New York City and replaced it with a piped-in feed from California. It seemed like we would be losing a vital outlet that had always welcomed the voice of hackers over the airwaves. Thanks to listener support and the court system, the station was restored and is now operating with renewed passion and energy. There are massive challenges at the station to overcome still, but at least

now the danger of what might be is so much clearer. And that has proven to be a great motivator.

Our biggest challenge, though, was the future of our HOPE conference. When our previous venue decided to triple their price, we were faced with a choice: either triple our admission cost or stop running one of the most popular hacker conferences in the world. We didn't much like either choice, so our community helped us come up with a third choice: find another way.

We were blown away by the hundreds of letters of support we received from attendees, readers, and even people who had never come to the conference but were well aware of its importance and significance. When we saw how much it continued to mean to so many, we knew we couldn't accept something that was wrong or just give up. And so we spent pretty much the entire summer looking for new venues. Some were comically terrible and others were hilariously expensive. But we never stopped looking, primarily because so many people kept asking for updates and encouraging us to continue the search. So instead of not knowing how we could possibly solve this problem, we *knew* we'd find a solution but didn't yet know what that was. The difference between those two perspectives was so much more significant than we ever knew.

We found what we believe to be not only a great location but a pivotal point in the history of HOPE. Instead of battling hotel bureaucracy and getting perpetually overcharged and overcrowded, we're now going to be in a university environment, where space abounds and the people appreciate our community and what we do. And we won't have to leave New York City to do this. While no longer in midtown Manhattan, we'll be at a venue that will be easier for many to get to and far less stressful to maneuver.

St. John's University in Queens will be the site for HOPE 2020 from July 31st to August 2nd, 2020. We'll have the same or bigger rooms for all of our talks, plus additional hangout space, and a huge outdoor area to introduce all kinds of new projects

and activities. On-site housing will be available, bringing elements of a hacker camp to New York for the first time. Off-site hotels with special rates will be close by. And for those who want to stay in Manhattan, it's a one-stop train ride away.

Of course, this kind of a change won't be easy. It'll require a significant amount of additional coordination on our part and we expect to make many mistakes as we adjust to this new way of doing things. But if we're able to pull this off, we believe it will turn the page into a new era of hacker history and allow us to make new dreams possible.

We've never been more confident that this community has what it takes to make this into a successful - and recurring - event. Info on all of these developments will be posted and updated frequently at www.hope.net and www.2600.com. Please help us get the word out!

2600 (ISSN 0749-3851, USPS # 003-176) 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 - \$29 individual, \$50 corporate (U.S. Funds)

Overseas - \$41 individual, \$65 corporate

BACK ISSUES:

1984-1999 are \$25 per year when available.

Individual issues for 1988-1999 are \$6.25 each when available.

2000-2018 are \$29 per year or \$7.25 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 © 2019, 2020;
2600 Enterprises Inc.

Industrial Control with Modbus

by Malvineous

With recent news articles about network attacks on power grids and other infrastructure, one may be forgiven for wondering how exactly a circuit breaker can be controlled over the Internet, and how one would even begin to look for such vulnerabilities.

To help provide some answers, this article hopes to be an overview of the Modbus protocol and how it is used to control such industrial devices. Some tips are also provided at the end for anyone wishing to find inexpensive Modbus devices they can use to further their understanding of how one can control real-world devices via simple computer programs. There are many such devices available, from temperature sensors to electricity meters to relay control boards that can switch power on and off to other devices.

But first, to put everything into context, a little history.

What is RS232?

Many readers will be familiar with RS232, the standard specifying the electrical signals used for the serial ports found on so many computers over the last few decades. Before USB, and even for quite some time afterwards, these ports were used for connecting peripherals such as dial-up modems. They are still commonly used for configuring industrial devices and as a fallback for some commercial Ethernet-connected devices, so they can still be accessed when the network is unavailable.

One limitation of RS232 is that it is a point-to-point connection, allowing communication between only two devices. Electrically, this is because the transmitters at each end of the connection are active at all times, even when no data is being sent. This means that should two transmitters be connected to the same wire, they will work about as well as listening to two people shouting at the same time - neither can be heard clearly, if at all, each drowning out the other.

A side effect of this is that RS232 must be full-duplex, allowing data to flow in both directions at the same time, because each end of the connection needs a dedicated wire to

transmit on. So for RS232, separate wires for transmitting and receiving are required.

What is RS485?

To address some of the limitations in RS232, RS485 was created. Like RS232, all devices must still select a common baud rate to operate at, although RS485 can go all the way up to 10 Mbps. RS485 also requires that the transmitters be switched off when no data is being sent, allowing multiple transmitters to share the same wire. As a consequence, all receivers need to listen on the same wire as well, making RS485 half-duplex. Although this is a small drawback, it is greatly outweighed by the benefits of being able to connect many devices to the same wire run. (There are also some schemes that run two RS485 buses in parallel to achieve a kind of full duplex, so it's not really that much of a drawback anyway.)

This may appear to be a bit like a rudimentary Ethernet network, for those readers who remember the days of 10 Mbps thin Ethernet with its coax cables, allowing multiple computers to be connected to a single cable run. In fact, RS485 shares a number of similarities with thin Ethernet, but in some regards offers more flexibility.

While thin Ethernet required both ends of the cable to have terminating resistors installed in order to operate, with RS485 these are only needed for high speed operation. At lower speeds the terminators can be omitted, and a reduced speed also allows the maximum length of the cable run to be far longer - over ten times longer than Ethernet's 100 metre/300 foot maximum. (As a side note, the early parallel SCSI interface used many RS485 lines in parallel to make up the 50-pin SCSI bus. This is also why sometimes these old SCSI buses would appear to work on short cable runs even when the termination wasn't set up properly.)

Unlike Ethernet, RS485 only deals with getting bytes from one device to all the others. It does not have MAC addresses, collision detection, a concept of data packets, or any of the other features of Ethernet. With RS485, all this must be done in software by a higher level protocol, just as it did with RS232. All you get from the RS485 interface is a stream of bytes,

and it's up to you to decide what these bytes should represent, and indeed if they are even correct, since significant noise on the line can corrupt the data.

This means when using RS485, you must define the set of rules used by all devices on the bus. If two devices transmit at the same time, the result will be garbled, so you need to come up with some protocol to prevent this from happening in the first place.

What is Modbus?

With RS232, ascribing meaning to the bytes traveling over the wire was often done with higher level protocols such as SLIP and PPP. With RS485, a very common protocol that does the same is Modbus. Originating in 1979, Modbus is an early protocol and is very simple by today's standards. However, with that simplicity comes robustness, and many modern industrial devices still use Modbus for control today. Modbus is also effectively an open standard, while many of the competing (and often superior) standards such as BACnet cannot be obtained without payment, preventing them from fully replacing Modbus.

To prevent collisions on the wire, Modbus works in a master-slave arrangement. There is only one master device on the RS485 bus, and it requests data from up to 247 slave devices (although practically speaking, RS485 maxes out at around 32 devices per bus). After the master initiates a request from one of the slave devices, that slave is allowed to transmit its response. This arrangement ensures only one device is ever transmitting at a time, avoiding collisions. A CRC code in each message guards against any corruption from noise on the line.

Conceptually, Modbus devices are based on numbered registers, each of which can hold a numeric value. The Modbus master sends messages such as "read register X" or "write X to register Y", with the device returning an appropriate response. For an electricity meter, one register may contain the current mains voltage, while a different register may contain the current rate of power consumption in watts. Since the registers are addressed only by numbers, it is crucial to have a register map for the device you are working with, so that you can find out which register contains the information you are seeking, and which registers must be written in order to trigger the action you need.

There are 65,536 possible registers in each category, and there are three categories. The first category is called "coils," so named as they were originally used to turn the coils in relays on and off in order to control devices like heaters and air conditioning compressors. These registers are only a single bit wide so are not commonly used now, with the other two categories being preferred as each of those registers is 16 bits wide. Sadly, there is no standard about the endianness of each register value (endianness is the direction of the bits within a byte - do they come in as 12345678 with the 1 first, or 87654321 with the 1 last), so some devices will supply their 16-bit register value in little endian order and others in big endian, and again the register map must be consulted to discover which order a particular device uses.

Often two registers will be combined to store a 32-bit or 64-bit value (either as an integer or a floating point), however, like the endian issue, here care must also be taken to discover in which order the two registers are combined. Generally speaking, registers are mapped directly into the memory of the microcontroller on the device, so little endian values in each register should mean registers are combined in little endian order to read any 32- or 64-bit values. However, it is unfortunate that sometimes devices are encountered that combine registers together in one endian order, but return each register value within as a different endian order, which certainly creates a headache for the programmer!

How Do I Speak Modbus?

There are many cheap USB-to-RS485 adapters available from the usual places, costing as little as a dollar including postage from China. These devices appear as standard USB serial ports, so they don't need any additional drivers to operate, appearing as "/dev/ttyUSB0", "COM1:", or similar depending on your OS.

In the network connected world, there are many Modbus gateways that can provide an interface between the RS485 bus and a TCP/IP network. Typically, these will listen on TCP port 502 and, once connected, the bytes sent and received over the TCP connection are identical to those sent over the RS485 bus. For this reason, most Modbus utilities will let you specify either a serial port or an IP address

when using them for communication.

There are a huge number of devices that speak Modbus, however, as many of them are industrial, they tend to be on the expensive side. Searching for “(rs485,modbus) -usb” on eBay or similar will give you an idea of what is available (this will match anything containing “rs485” or “modbus”, but ignore anything containing “usb” so that all the USB-to-RS485 adapters don’t clutter the search results). You will find things like humidity sensors and relay boards, however, bear in mind that this is less likely to show industrial devices such as variable-frequency motor drives as those are assumed to have Modbus or equivalent interfaces, so this isn’t usually highlighted and you need to go digging in the specs to find out.

Before purchasing any Modbus device, make sure it either comes with a register map or that you can find one online, as without this it will be very difficult to figure out which register values mean what.

How Do I Use Modbus?

As Modbus is a relatively non-descriptive protocol (i.e., there is no hint what a register might be for unless you consult documents that are not part of the protocol), there are limited utilities available for working with it. There are programs specific to certain devices, like NUT (Network UPS Tools) that can only speak to specific models of backup power supply via Modbus, and there are general programs like “mbpoll” that are mainly useful to perform raw reads and writes on Modbus devices to confirm you are reading the register map correctly.

To actually do anything useful with your device, you will likely have to write your own program to provide an interface between the Modbus registers and the system you want to connect the device to. For example, I have written a program that queries an electricity meter connected to my computers, and if the power drops below a certain threshold, it means the monitors on all the PCs have gone into sleep mode, implying that everyone must have left the room. The program then writes to a couple of registers on a relay board which shuts off power to the sound system and the lights. The data is also logged to a time-series database, which is useful for displaying dashboards. In my case I am displaying the temperature and humidity in different rooms read from Modbus sensors located in each one, as well as the predicted cost of my next electricity

bill based on my power use so far in the current billing period.

While this is far from any form of industrial control, it has at least allowed me to put my “play” devices to some use now that I have learned a great deal from them.

How Do I Hack a Power Grid?

While Modbus is one of the protocols used in SCADA systems, there are a number of others such as PROFIBUS and BACnet. BACnet in particular provides much more information about what each data point means and controls, but it is still far from self explanatory. In short, it means that remotely exploring SCADA infrastructure is not an easy task, and will likely start with an unrelated compromise in order to gain access to schematics, network architecture, and other documentation. Without this, figuring out how a network of Modbus devices are arranged, what they do, and the implications of sending them control messages would be exceedingly difficult to discover.

The remote network would also almost certainly need to be compromised, as most organizations are now at least aware that these devices have no support for any kind of security. They are typically placed on an isolated VLAN, not even accessible from the rest of the corporate network. Gaining access to this restricted VLAN is likely to be quite difficult, involving the compromise of an accessible device that has access to the restricted VLAN, such as a reporting interface or a PC used for managing the SCADA systems.

It would appear that some of the recent attacks making headlines were able to get malware onto the PCs controlling the SCADA systems, making the accomplishment even more impressive as this suggests that the attackers had no access to the target network. How they managed to figure out what IP addresses things were listening on, what protocols to use, which registers to write to and the correct values to write is amazing if all they had to work with was a simulated environment built around stolen schematics. Apparently, the attack on Ukraine’s power grid was foiled because at the last moment the commands were sent to the wrong IP address, so maybe a device was replaced or moved at some point and the attackers were working off older documents? Or perhaps forgetting to update the documentation isn’t always bad....

Ideas Behind Site Reliability Engineering

by kingcoyote

As the software industry grows and matures, the systems that run all around us grow in size and complexity. Users' demand for reliability combined with this growth has produced a new specialization: the site reliability engineer (SRE). While the role relies on a mixture of sysadmin and software development skills and overlaps with infrastructure engineering, it is made unique by the mindset that it brings to bear on the problem. I want to share what I know about working like this because it's a relatively unknown specialty and because it soothes my heart to know that humanity isn't one error away from turning the world into a *Mad Max*-like desert.

At its core is the belief that as systems grow, they become less legible. No longer can we look at a UML diagram and predict all its behaviors. When we had to take care of ten or 20 hosts or a simple web application, it was possible for a single person, usually the senior engineer, to understand the system and keep it in a stable state. But when the number of hosts grows and the application becomes distributed and has dozens or hundreds of engineers changing it every day, it becomes a murky pool of statistical probability where something somewhere is always failing. Disks are dying, network links are going down, and processes are exhausting the available resources. Hiring more people doesn't work for two reasons: it's really expensive and it increases the communication overhead (Brooks's law). How do SREs attack this problem? By learning from the broader engineering community how to deal with complex systems like aircraft.

The foundation of this approach is observability. The system has to continuously report its state so that the engineering team knows whether it's working, broken, or becoming broken. This pushes the existing practices into overdrive because we want to get and store all the metrics we can get our hands on. Some examples here are host-level metrics like CPU, disk, network, and memory utilization; service-level metrics like rate, type, and latency of incoming and outgoing requests; and every log line the service produces. Not

only should these all be gathered and stored, but they should be easily accessible and searchable by everyone on the team. Having these, we can, over time, single out those that provide us the strongest signal about how well things are working. We will be able to go back and study the state of the system closely and investigate all the dimensions in which it deteriorated when things were broken. We will also be able to build some automation on top of them to fix certain recurring problems automatically. Any system will experience a steady flow of problems, like disks dying or hosts getting into a weird configuration state, but time is precious for us, so we want the system to react to these events on its own. We want to take as many humans out of the equation as possible.

Knowing how the system is behaving every second, we can automate away a good chunk of senseless toil that happens whenever we change it. The biggest contributor here is the stream of new features and bug fixes. Having service-level metrics means that once a change has been reviewed by a human, it can be deployed automatically because we trust the system to detect a problem, revert the change to the last known good state, and notify someone. This is a great thing to have for a couple of reasons. Our users will appreciate that even if something is broken, it's likely to get fixed within minutes or even seconds. The people making these changes will appreciate it because they will be getting quick feedback about their code while it's still fresh in their minds. Finally, exercising this flow gives us confidence that we can make changes quickly, which is pretty handy when we need to get a fix out ASAP.

The second source of toil is usually managing the configuration of all the hosts. Instead of crafting artisanal coconut milk configs by hand for each of them, we can roll out a uniform, self-enforcing set of configuration everywhere. Whenever a host deviates from this golden standard, it can be automatically reimaged and reconfigured without a single person taking action. This view is summed up as "treat your hosts like cattle, not pets." This setup leaves us with more

time to focus on anomalies that need a human to investigate. It also speeds up our reaction time considerably. Imagine if the primary data center goes down. Now imagine how much stress, sweat, and coffee all this automation would save us if all we had to do was point it at a set of blank machines in a new location and wait an hour for everything to go back to normal.

In my experience, the most important piece in all of this is how the engineering team handles failures. It's organizational, not technical, in nature. First, all production incidents should be investigated and discussed at a post-mortem meeting with all affected present. The goal isn't to dish out blame and punishment, it's to build a shared understanding of how the system entered a bad state. Trust is essential in order to bring up all the little details and go through as many follow-ups as feasible to prevent the problem from happening again. Without trust, people will hesitate to report incidents or their details for fear of punishment. Think of it as a group learning process. It's important to note that some incidents may be the result of how the work is organized, so managers should be a part of this, too.

Second, there's the on-call process, where a rotating member of the team is notified whenever something is broken and has to fix it. It's familiar to many, but to make it truly work, all

technical team members should be part of the rotation. This puts equal pressure on everyone to keep reliability in mind as no one likes to be woken up at 2 am. It directs everyone on the team toward the same set of goals. The opposite approach is why ops and security teams used to fail in the past - the "feature team" doesn't understand that security or reliability is part of the product and introduces bug after bug, vulnerability after vulnerability, while the ops and security teams take up drinking because it's the only way to handle a dysfunctional relationship like that.

None of these practices are new, they just needed to be discovered and put into practice by the right people in the right place. I imagine we, as both users and builders of systems, will reap more benefits of these practices as they gain popularity.

For those interested in learning more, here are some reading materials:

- *The Field Guide to Understanding Human Error* by Sidney Dekker,
- *Debriefing Facilitation Guide* by John Allspaw, Morgan Evans, Daniel Schauenberg
- *Site Reliability Engineering* by Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy
- *An Introduction to General Systems Thinking* by Gerald M. Weinberg

Cyberspelunking A 2600 Guide to Exploring the Internet

by //dug0ut

We have a term for the weekend curiosities known to hackers. Instead of spending too much time going into the details of what we actually did (in a way that only we ourselves really understood), we would simply smile and say that we went "cyberspelunking." We knew that we each had our own definition for it, and that we didn't fully understand the others', but we knew that it meant that the other was deep in thought chasing some curious itch down repeated rabbit holes for nothing other than the joy of learning something new. Sometimes it was code. Sometimes it was a new or really old operating system. Sometimes it was a network. Sometimes it was a boat, school bus, crock-pot, radio, television, or any other oddity that

caught someone's interest to an unhealthy degree.

We called it cyberspelunking because people got uncomfortable when they overheard the word "hacking," or would join in with a mocking tone. Cyberspelunking seems to be an accurate way of conveying the same curiosities with a positive connotation or, at the very least, with a word that society has not yet twisted. The phrase was coined by a former boss of mine who would ask what we did over the weekend but, not being as technical as the rest of us, would quickly get bored or lose interest. It was never rude, and he enjoyed our excitement. Around this time, he was planning his retirement adventures. One day, he was reading a magazine about spelunking, called me over, and giggled while asking me what

I did for the weekend. Before I had a chance to answer, he asked “Did you do some cyber-spelunking?!” and continued to chuckle to himself.

He retired shortly after, began his adventures with his wife, but sadly passed away a few months later.

I thought the phrase was perfect, and that small encounter plays in my head quite often.

No Set of Steps - Go Explore

Spelunking is the act of cave exploration, and cyber is the buzzword of choice for the Internet. Cyberspelunking is simply the act of exploring the Internet in a non-malicious manner. There is just as much to learn from Open Source INTelligence as there is from trespassing and exploitation. I like to discover and explore the infrastructure of other countries. Everyone experiences the Internet differently and I like to try to imagine how someone from a foreign country would experience the Internet.

What is Belize Like?

Let’s take a look at the infrastructure of Belize. It isn’t a place I know much about, other than that it is small and it is a popular

tourist location at the moment. I like to start with Wikipedia for a quick summary. You’ll often find information about population size, telecom providers, brief history, and sometimes top level domains (TLDs) or links to government sites for that country. The official Belize Wikipedia entry is all we are after here.

A brief review of the wiki entry provides some useful information for us to get started with. The population size is right around 400,000 people, which is pretty damn small. There are multiple languages spoken, and multiple ethnicities living throughout the country. It appears that there are two primary telecom providers: Belize Telemedia Limited and Speednet. Speednet was created to attempt to break the monopoly of BTL. There are official wiki entries for both companies, each linking to their official domains.

There appear to be over a dozen colleges/universities in Belize. The .bz TLD is the official TLD for Belize, and it is maintained by the University of Belize. The other official TLDs are .com.bz, .edu.bz, .gov.bz, .net.bz, and .org.bz, but it appears that standard .net, .com, .org, and also .biz are common for Belizians. It looks like the “Telecommunications in Belize” wiki entry has done a lot of legwork for me.

Internet [edit]

- Top-level domain: .bz,^[1] administered by the Belize Network Information Center at the University of Belize.
- Internet users: 81,930 users, 171st in the world; 25.0% of the population, 138th in the world (2012).^{[3][4]}
- Fixed broadband: 10,077 subscriptions, 148th in the world; 3.1% of the population, 115th in the world (2012).^{[3][5]}
- Wireless broadband: 419 subscriptions, 147th in the world; 0.1% of the population, 146th in the world (2012).^[6]
- Internet hosts: 3,392 hosts, 152nd in the world (2012).^[1]
- IPv4: 61,952 addresses allocated, less than 0.05% of the world total, 189.0 addresses per 1000 people (2012).^{[7][8]}
- Internet Service Providers: There are several ISPs in Belize: BTL, Speed Net, and others.^[citation needed]

It appears that most of these stats come from 2012. I doubt this is still accurate, as I’m sure more IPv4 addresses have been allocated since then. I’m also sure there are more hosts online, and the number of Internet users increased. This still seems like a manageable amount for us to dig through.

Belize Internet Routes - BGP ASN FTW LOL

I’m not that awesome at routing. It is something that I’ve always planned on studying harder, but instead I just pick up more tidbits here and there. I am familiar with BGP Sink-hole attacks (yay - something else for you to

search), which is enough for me to know that the Border Gateway Protocol used by most larger entities will be broadcasting the routes for BTL and Speednet as well as any other large provider.

In order to find the routes, first we have to find the ASN (Autonomous System Number) registered to the telecom providers. MX ToolBox has always been reliable and has been online for a while now. If it is down, there are plenty of other BGP ASN search tools. I’ve gone ahead and provided the ASNs and the netblocks they’re advertising now.

AS10269 - Belize Telemedia Limited

```
170.0.180.0/22 170.0.182.0/24
➔ 179.42.192.0/18 179.42.192.0/18
➔ 190.197.0.0/17 190.197.0.0/20
➔ 190.197.17.0/24 190.197.18.0/23
➔ 190.197.20.0/22 190.197.24.0/21
➔ 190.197.32.0/20 190.197.48.0/22
➔ 190.197.51.0/24 190.197.53.0/24
➔ 190.197.56.0/22 190.197.58.0/24
➔ 190.197.60.0/22 190.197.64.0/19
➔ 190.197.96.0/22 190.197.96.0/24
➔ 190.197.100.0/22 190.197.104.0/24
➔ 190.197.104.0/21 190.197.110.0/24
➔ 190.197.112.0/22 190.197.115.0/24
➔ 190.197.116.0/22 190.197.120.0/21
➔ 200.32.192.0/24 200.32.192.0/19
➔ 200.32.192.0/18 200.32.195.0/24
➔ 200.32.198.0/24 200.32.205.0/24
➔ 200.32.213.0/24 200.32.218.0/24
➔ 200.32.221.0/24 200.32.222.0/23
➔ 200.32.224.0/22 200.32.228.0/24
➔ 200.32.228.0/22 200.32.232.0/21
➔ 200.32.240.0/20 200.32.253.0/24
```

AS262239 -

Speednet Communications Limited

```
186.65.88.0/22 196.52.81.0/24
➔ 196.55.4.0/24
```

AS266762 -

Smart Com (Belize) Limited

```
45.234.88.0/22
```

A Quick Dive

Throughout this process, I saw plenty more AS numbers. I will leave those for you to find. AS266762 was downstream of AS262239, so I went ahead and included it. There were quite a few downstream of BTL. Those downstream addresses are likely to be small ISP resellers. Let's check out AS266762 because it is only advertising a small number of address ranges.

I like to start with `censys.io` to check address ranges for open ports, while other people like Shodan. I say use both. For those that are unfamiliar, Censys and Shodan are Internet search engines which constantly scan ports instead of crawling web pages like traditional search engines. Searching for the address ranges listed under AS266762, I found a surprising amount of telnet and ssh ports open, and plenty of web services. Let's do our scan for common web ports and then use aquatone to connect up and screenshot them all.

```
>$ nmap -Pn -n -sT -vv -T 5
➔ --open -p 80,81,82,443,8080,
➔ 8180,8181,8888,8443,9443,8000,
```

```
➔ 1080,3128 45.234.88.0/22 -oA
➔ smartbz- webports
>$ cat smart-bz-webports.xml |
➔ ./aquatone -nmap
```

Aquatone will go through every open port found in the nmap scan and attempt to take a screenshot of the landing page. In the directory that you ran aquatone from, there will be multiple folders and a report.html. View the report in your web browser, and you'll see the screenshots grouped together based on similar services found. In my case, I found quite a few firewalls, a few VPNs, some webcams, and some electrical boxes.

I don't crack accounts, but I'll try logging in with default credentials. Especially if it is a system I have never encountered before. When doing this, I never make any changes or interact with anything that could potentially cause a change. I like to check logs to see who else has been here. I like to look through configs and see where else they lead me.

One "smart electric meter" I found contained default credentials (found with a quick Google search). Upon logging in, I was greeted with a large warning screen which stated that real electrical systems were being maintained by this device, and that dumb changes have the potential for physical damage or harm. I was prompted to change the password, but was given the option to skip. Always skip. (How dumb is that though? An admin set this up. Why were they not forced to change it then? Horrible practice for them, but it works out for us.) Looking through the logs showed that someone else had been there before us by a few weeks. The device was sending reports via email, and showed the Yahoo account which was receiving the reports. The more malicious individuals may change the SMTP server setting to a server they control and capture the email creds, but I chose to do some quick OSINT over the address instead.

A quick Google search immediately took me to a Facebook page of a small electrician contractor in Belize. Interesting, and makes sense based off how we found the address. Maybe send a quick email and let them know their system is open. There isn't too much more to do on the device, so it's time to move on.

I'll leave the rest of the exploration to you.
Happy Hacking!
Safe Spelunking!



TELECOM INFORMER

by The Prophet



Hello, and greetings from the Central Office! Today, I am writing to you from the opposite side of the Indian Ocean from The Seychelles. I'm on Christmas Island. Although it's technically part of Australia, you have to pass through Australian Customs and Immigration to get here. In fact, Christmas Island is so remote that it has its own famous .cx top level domain!

Although Christmas Island is practically a stone's throw from Bali (about 650 miles), there aren't any direct flights. There are two regularly scheduled flights a week to Perth, Australia, which is about 1600 miles away. There are also charter flights to Jakarta, which usually run once a week. They're really expensive, running around USD \$500 round trip from Jakarta and over \$750 round trip from Perth (which, in and of itself, is a \$300 flight away from Sydney). As locations go, it's about as close to the middle of *some-where* that you can be while remaining in the middle of *nowhere*.

In addition to it being complicated for people to get to Christmas Island, it's also tough to get cargo on and off the island. Phosphate is pretty much the only export, and specialized transport ships and conveyors are used. For sea cargo, there is a crane. The harbor is poorly sheltered, though, so loading can only happen when the seas aren't rough. They're often rough. Right now, large waves are slamming into the rocky coast, sending spray almost as high as the cab of the cranes, so I'm fortunate that the piece of equipment I'm here to provision was offloaded from a cargo ship yesterday (during a relatively calm period) and is sitting safely in a container on shore.

If you think getting here is expensive, the costs of living on the island are even higher. Nearly everything must be imported

from the Australian mainland, and the cost of transportation is very high. Gasoline is \$6 per gallon. A head of lettuce costs \$13.50. And Internet is similarly expensive. Basic satellite connectivity (through the satellite Internet provider Speedcast) costs residents over AUD \$100 per month. Like all satellite Internet, it's strictly metered and very slow. Residents ration their Internet usage, jealously guard the security of their Wi-Fi access points (lots of them are named "Get Your Own WiFi" or something similar), and limit their video streams to 720p.

It's not just Internet that comes via satellite. Everything does. Television and radio transmissions are received from the Australian mainland via satellite dishes (one each for two TV stations and the radio), but these don't always work reliably. Satellite transmissions can be impeded by heavy rain and storms, and the island often has both. On top of this, Telstra, the local telephone and GSM provider, uses satellite. They have only a single satellite dish for connectivity to the rest of the world and it goes down frequently, at least once a month for a few hours. Speaking of mobile connectivity, it's GSM only - and only voice and text. It's like a time warp to the 1990s.

Christmas Islanders are, however, a hardy and creative bunch and they have a solution to their telecommunications problems: blackboards! There is a town square of sorts with a roundabout in the middle. The buildings there are covered in blackboards and these are used for community-wide news and notifications. The islanders are avid users of Facebook as well, but the on-island blackboards are treated as the "source of truth" and can be updated when electronic communications are unavailable.

So, given this context, you can prob-

ably imagine the excitement of the island's residents that a fiber-optic cable has finally landed on the island. It promises faster, less expensive, and possibly even unmetered Internet access, maybe even at speeds up to 20 Mbps. The cable is here, and packets are flowing. However, progress has been slower than anyone would like in deploying the infrastructure for most of the islanders to use it. The "last mile" infrastructure in place largely isn't suitable for high-speed broadband, so a lot of work (and working out the costs) needs to be done before residents can enjoy the benefits. The first customer is the Australian government.

The Australian government's interest in this part of the world is strategic, and the region is growing in strategic importance. You can draw your own conclusions about what this means for the future. The first facilities that have been brought online are the Australian government's offices, police station, school, recreation center, airport, and hospital. Subsequent facilities to be brought online are likely to be, as you can imagine, ones that the Australian government considers strategically important. So, for no particular reason, I'm here to install a *thing* in a *place* for a *client*. Based on their confidentiality requirements, I hope you understand that I won't be going into details.

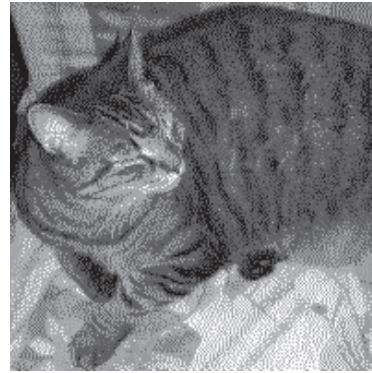
There's only one problem. *Crabs*. It was just my luck to arrive at the beginning of the red crab migration season, and the island is absolutely swarming with them. Christmas Island is inhabited by millions of land crabs, and they all spawn at the same time each year. This means that the land turns into a river of red. It's an absolutely astonishing spectacle: every surface is covered with them. They are everywhere and get into everything. You have to put towels under the door to keep them from crawling underneath (or mobbing the door every time you open it) and coming into your living space! Making matters even more complicated, these are a protected species. You can't run them over and kill them (and the islanders also consider it bad luck), so you have to push them out of the way. The island more or less shuts down while red crab migration is underway and this can take *over two weeks*.

I don't have time to wait, obviously. And movement can still happen during the red crab migration, albeit carefully and deliberately. To get around during the red crab migration, islanders drive very slowly. Their vehicles are improvised for the local conditions, and someone literally hangs off the front of the vehicle with a rake to move crabs out of the way. Or, in the case of baby crabs when they're migrating the other direction, *leaf blowers*! It took me two hours to get into town from the airport yesterday, and I have twice as far to go today. And that's *round trip*, which means that most of my day will be spent just getting to the job. Once I'm there, I'll need to go through mandatory training, and be escorted everywhere, so I have to hope that the person who is supposed to train me and the person who is supposed to escort me were able to make it to work (fortunately, they commute by bus and it's pretty well organized, so I'm pretty confident it will happen).

Everything is - allegedly - in place for me to do the job. We shipped the equipment I'll need, and also a spare (they'll need one on the island anyway, and I'll want to have it available in case of a bad part). While transportation hadn't been sorted out before I arrived, the locals have a typical problem-solving Australian attitude which is refreshing compared to some of the nearby locales I work in. We have some sort of golf cart with a snowplow-like attachment, a couple of guys with long rakes, and a giant truck that is ordinarily used for phosphate mining operations (the island is host to a large mine). The equipment is on the dock. Everything else I need is at the site. Even if we need to come back for a spare, I'm confident I'll make my flight back to Perth in a few days.

And with that, I'll sign off from Christmas Island! This time, it's a short visit to a tropical island, and I don't have any excuses to stay longer than planned. However, I'll be making the most of it before I leave. Have a safe winter in whatever frozen tundra where you're currently shivering, and I'll have a Bundaberg for you on the beach!

STEGANOGRAPHIC FILESYSTEMS



by Chimera Manicore

People are worrying a lot about data privacy and security these days. The use of strong encryption is one popular method to ensure private data stays that way.

Encryption is not always the best way to protect data. One can imagine many scenarios where the existence of encrypted files might be considered compromising by a third party.

According to some, the level of plausible deniability is diminished when you encrypt a file - after all, why would one bother unless one has something to hide? Or at least so the argument goes. Grand Inquisitor Torquemada would likely be unimpressed with your assurances that the encrypted file is really a picture of your grandmother, and so might coerce you to decrypt the file. A plain old subpoena might have a similar effect.

This is where steganography comes in. Steganography refers to the art of hiding in plain sight, which in this context is the practice of concealing private data of some sort inside public data of some other sort, thereby evading the attention of snooping eyes. For example, a message could be hidden inside an image, or an image could be hidden inside an audio clip, or encoded in a blog or broadcast. The trick is to make the envelope appear as normal and innocuous as possible.

It turns out that's a nontrivial task. Regardless of the types of envelope and payloads one chooses, the fact that we're embedding a file within another will introduce anomalies that can be detected by an analyst. In other words, we have a cat and mouse game between steganographers and steganalysts similar to that between cryptographers and cryptanalysts. The moves of that game are often very complex and beyond the scope of this article,

but suffice it to say the strongest methods often result in relatively low bandwidth in terms of letter-to-envelope size ratios. That in itself can be a problem. After all, how many pictures of your grandmother can you have without arousing suspicion? And why do all your Bach cantatas sound a bit off? Another similarity with cryptography is that if the analyst figures out how to extract the message from the envelope, there's no longer a question of plausible deniability.

The game is over.

Encryption and steganography used in isolation are indirect proof that someone has tried to hide something. Worse, if somebody coerces the legitimate owner to reveal the cryptographic key or a steganographic algorithm, the cat is out of the box. This is the core problem that a steganographic file system addresses.

The basic idea is to embed encrypted data inside a very large volume of random data in such a way that it's impossible to determine what data (if indeed any!) has been embedded. In addition, it should provide a method to extract individual pieces of embedded data without revealing if there is additional embedded data. Since random data is by definition random, the concept of an anomaly evaporates, and an analyst has no reference point from where to begin to unravel the mystery. The analyst would see a large amount of random data, but won't be able to determine what if anything at all has been embedded. When confronted with waterboards, rubber hoses, or court orders, the legitimate owner of the data can choose to reveal some of it, while keeping the balance secret and yet maintain plausible deniability. For example, when coerced as described above, the owner could choose to reveal the nuclear launch codes while still keeping the

video of that embarrassing karaoke night at the Singapore Metropole from the public eye.

By now the reader is likely thinking “I really need one of those!” Fair enough. Let’s build a proof-of-concept steganographic file system from scratch.

The first thing we need is a very large volume of random data. In a production strength system, this would likely be an entire disk partition filled with random data, but for the purposes of this article a large file will do. On a Linux system, you can very easily create a large file of random data using the `dd` command. At your option, you can also just as easily overwrite your system with random data and turn it into a fancy doorstop which might not be what you desired, so the preferred method is to create the file on removable media such as a USB drive.

Assuming the USB drive is mounted as `/media/x/y` you simply run:

```
dd if=/dev/urandom of=/media/x/y
  ➔ /bigfile bs=1M
```

When the command completes, you have a huge file of random data taking up all the free space on the USB drive. We are now ready to direct our attention to Listing 1. The entry point to the program is indicated around line 86. The first thing we need to do is calculate the number of blocks we have available using the actual size of the file and a fixed block size.

We also indicate the file we want to embed and a secret key associated with that file. The next step is to add the file we want to embed to the file system.

The algorithm for doing that is implemented in the function `writfsys()`. Here’s a high level summary:

First, we calculate the ID of the starting block by calculating the SHA256 hash of the secret key and the file name modulo the number of available blocks. We then encrypt the first block of data and write it to the block. Our encryption algorithm is a simple-as-spit XOR operation with the key. In a production grade system, we’d more likely use something like AES. We then calculate the ID of the next block by calculating the SHA256 hash of the previous block, and then encrypting and writing the data. And so on with the next block, and the next. The net effect of this is that the encrypted data is randomly distributed over the entire file system, and unless one knows the secret key and the file name, there’s no reason-

able way to collect it. We can embed multiple files in the same file system simply by calling `writfsys()` again with a different file name and secret key, the only requirement being that the combination of file name and key are unique.

When we want to retrieve the file, we simply run the process in reverse, using the function `readfsys()`. We calculate the ID of the starting block using the key and filename just like before. Then we read that block and decrypt it. Like before, the hash of the SHA256 hash will give us the next ID and so on. The uniqueness of secret key and file name guarantees that the extraction of one file does not reveal any of the other files or even show their existence.

The proof-of-concept can only store individual files, but it’s trivial to extend it to support other common features of file systems such as directory trees, symbolic links, and inodes.

The demo code has one problem that has to do with the nature of hashing. Multiple entries can have the same hash value, and this would result in collisions where later entries will overwrite data already stored. Similar to a birthday paradox, this is more likely than one would naively guess. A solution to this issue is to store each encrypted datum in multiple blocks along with a validity checksum using several different hash values. When extracting files, we would only consider blocks that have a valid checksum. This scheme will naturally reduce the number of files that can be stored, but will protect the integrity of the data. The demo code does not have this feature for reasons of clarity.

Although this is an emerging field, there are currently several public implementations of steganographic file systems. A popular choice is StegFS. This is a user-space file system for Linux based on FUSE written in C and offers the robustness and performance that our demo’s 100 lines of Python can’t hope to match. (See github.com/albinoloverats/stegfs for details.) Another interesting architecture is Mnemosyne, a peer-to-peer distributed steganographic file system. (The white paper is at www.cl.cam.ac.uk/research/srg/netos/papers/2002-mnemosyne-iptps.pdf.)

Shouts to John and Kirk.


```

import os
from hashlib import sha256
''' Calculate the block id and hash '''
def calcblock(bts,numblocks):
    hsh=sha256(bts)
    block=int.from_bytes(hsh.digest(),byteorder='little',
        signed=False)%numblocks
    return block, bytes(hsh.hexdigest(),"utf-8")

''' does what the name says '''
def encryptdata(value,pwd,blocksize):
    ''' SHA256 hash of the password will always be 32 bytes '''
    pwsh=sha256(bytes(pwd,"utf-8")).digest()
    if(len(value)<blocksize):
        ''' If too short pad with spaces '''
        val=value.decode("utf-8").ljust(blocksize)
        value=bytes(val,"utf-8")
    return bytes(a ^ b for a, b in zip(value, pwsh))

''' does what the name says '''
def decryptdata(value,pwd,blocksize):
    ''' SHA256 hash of the password will always be 32 bytes '''
    pwsh=sha256(bytes(pwd,"utf-8")).digest()
    if(len(value)<blocksize):
        ''' If too short pad with spaces '''
        val=value.decode("utf-8").ljust(blocksize)
        value=bytes(val,"utf-8")

    try:
        val=bytes(a ^ b for a, b in zip(value, pwsh)).decode("utf-8")
    except:
        val="End of message"
    return val

def writefsys(fsys,fname,pwd,blocksize,numblocks):
    ''' Calculate the first block as the hash of filename+passphrase '''
    block, hshval=calcblock(bytes(pwd+fname,'utf-8'),numblocks)
    outf=open(fsys,"r+b")
    with open(fname, "rb") as inf:
        while True:
            value = inf.read(blocksize)
            if value == b'':
                break # end of file
            #print("Writing to block "+str(block))
            #print(value.decode("utf-8"))
            byts=encryptdata(value,pwd,blocksize)
            outf.seek(block*blocksize)
            outf.write(byts)
            ''' the next block is based on hash of
            ➡ this block's hash '''
            block, hshval=calcblock(hshval,numblocks)
        ''' This is just a bespoke end of file marker '''
        value=bytes("End of message".ljust(blocksize),"utf-8")
        #print("Writing to block "+str(block))
        #print(value.decode("utf-8"))
        byts=encryptdata(value,pwd,blocksize)
        outf.write(byts)
        inf.close()
        outf.close()

def readfsys(fsys,fname,pwd,blocksize,numblocks):
    value=""
    rc=""
    ''' Calculate the first block as the hash of filename+passphrase '''
    block, hshval=calcblock(bytes(pwd+fname,'utf-8'),numblocks)
    with open(fsys, "rb") as inf:
        while True:
            #print("Reading from block "+str(block))
            inf.seek(block*blocksize)
            binarydata=inf.read(blocksize)
            value=decryptdata(binarydata,pwd,blocksize)
            if value.startswith("End of message"):

```

```

                                break
                                rc+=value
                                ''' the next block is based on hash of
                                └─ this block's hash '''
                                block, hshval=calcblock(hshval,numblocks)

inf.close()
return rc

''' Entry point to program '''
if __name__ == '__main__':
    ''' The file which contains the file system '''
    fsys="/media/x/y/bigfile"
    ''' A file with the message that must remain secret '''
    fname="./secretmessage.txt"
    ''' A secret passphrase '''
    pwd="To Heloise"
    ''' The block size we're using (bytes) '''
    bsz=32
    ''' Size of the fsys file '''
    fsz=os.path.getsize(fsys)
    ''' number of blocks in the file system '''
    blknum=int(fsz/bsz)-1
    ''' Write the file contents to the file system '''
    writefsys(fsys,fname,pwd,bsz,blknum)
    ''' Read it back '''
    msg=readfsys(fsys,fname,pwd,bsz,blknum)
    ''' Display the message '''
    print(msg)

```

Heloise,

Could I have imagined that a letter not written to yourself could have fallen into your hands, I had been more cautious not to have inserted anything in it which might awaken the memory of our past misfortunes. I described with boldness the series of my disgraces to a friend, in order to make him less sensible of the loss he had sustained. If by this well meaning artifice I have disturbed you, I purpose here to dry up those tears which the sad description occasioned you to shed: I intend to mix my grief with yours, and pour out my heart before you; in short, to lay open before your eyes all my trouble, and the secrets of my soul, which my vanity has hitherto made me conceal from the rest of the world, and which you now force from me, in spite of my resolutions to the contrary.

DEATH OF A SCENE

7B

|

7C

by NervousYoungInhuman

It was the fall of 2014. I was a college freshman, still so excited and intimidated by higher education. I finally was meeting like-minded peers who blew my mind with their tales of hacking exploits and further digital mischief. I soon found myself comfortably nestled in a social scene of hackers, artists, anarchists, and various other misfits. We spent most evenings chatting, playing video games, pulling pranks, and watching our favorite

movies from my significant collection on a portable hard drive. One night, we wanted to watch *Blade Runner*, but I only had the theatrical cut.

My first thought on where to get the final cut was a torrent, but the campus blocked traffic to my favorite sites, and if I had the money for a VPN, I wouldn't need to worry about downloading it. Before I could even consider other options, "L," one of my upperclassman friends asked, "Why don't we check the Hub?"

Intrigued, I asked about the Hub. It turned

out, given that we were a tech school and all, there was a private file sharing network on campus. I was told it was pretty exclusive. To get access, you needed to share five gigs of stuff, and it couldn't duplicate something already present on the network. And it was *fast*. By the time it was explained to me, L had already downloaded the Final Cut of *Blade Runner* in 1080p.

I was fascinated and I knew, as a media junkie, I had to get in! I eventually weaseled the server address from L, and presented the admin with the "Despecialized" edition of the original *Star Wars* trilogy.

And there it was. More media than I knew what to do with. Dozens of users online at a time, with most offering 10 to 20 gigs, but there were a few giants who had terabytes of data. These icons had standard stuff, like the latest movies and video games, but they also had strange things, like the phone numbers for the campus elevators and ancient CIA instructional manuals for various nefarious purposes, along with countless iterations of *The Anarchist Cookbook*.

I was absolutely hooked. Every day, I would scour the Hub for anything I could ever need. I watched entire directors' filmographies, became an expert in underground music, and read dozens of books, all for free. And every time I found something somewhere else that I thought would be enjoyed, I shared it back with the community. It seemed like I would never have to look far for media ever again. While some users disappeared at the end of the semester due to graduation, dropping out, or other reasons, new users would take their place when classes started up again.

But then Junior Year came, and I noticed the number of users had dropped from about 50 to maybe two dozen, with even some of the giants going quiet. For once, I couldn't find something I wanted once in a while. I partially blame this on the fact that the cable company and my school reached an agreement with HBO to provide an HBO Go account to every student. Who needed to download *Game of Thrones* or *The Wire* anymore? Every year, legal streaming services became more popular and accessible. The "must-watch" shows weren't on prestige cable networks, they were made by Netflix or Hulu. If you already had access, why would you need to pirate? *Stranger Things* and *Master of None* were

already freely available to subscribers, or close friends and family of subscribers. And if you had Spotify Premium for Students, then you had Hulu, too!

In the end, the private and exclusive nature of the Hub also somewhat led to its downfall. Sure, requiring exclusive and plentiful content from users led to quality content for all, but it also deterred people. VPNs also got cheaper and more user-friendly, so more people were able to safely torrent again. Why go to the trouble of finding the server address and then find something that nobody else has when you can just login to a VPN and go to your favorite tracker? Sure, the quality might not be as good, and it might be a slower download, but at least it was easy.

Slowly, over time, the scene sort of destroyed itself. The smaller shares disappeared one by one, leaving only the giants. I hung on as long as I could, but once I left campus housing for my own place, I lost access as well. I no longer needed to worry about the limitations of campus Wi-Fi, so I could once again torrent as I wanted.

About a year after the last time I used the Hub, I decided to log on again during a visit to campus. Where the sidebar was once filled with countless handles, promising total entertainment forever, there were a mere four names, all with terabytes of content. The few that remained seemingly traded only with each other. But even these giants would not last forever. The pinned message in the chat was a farewell from gh0st, the largest share on the network. He announced that he would be graduating and, as a result, the small brotherhood remaining would become just a little smaller in his absence. He thanked everybody for sharing, and closed it with a simple, yet poignant message.

"I know that this place won't last much longer, and that by leaving I bring us a little closer to the end. But if you're reading this, you were here, you stayed to the end, and you were part of something very special. Never forget that. Keep sharing, and goodbye."

One week later, another member left without a word. To quote the movie that led me to the Hub, *"It's too bad she won't live."* But it will live on in my love for all the media I would not have discovered without it.

BODY KEY-LOGGING

by Paz Hameiri
keylogger@gmail.com

Cyber criminals and security researchers have employed different approaches to capture keystrokes on keyboards and keypads. Devices used to capture keystrokes are known as key-loggers. While the common numeric keypads used in safes and electronic door locks may offer an attacker immediate entry, that person needs intimate knowledge of the architecture of the device's hardware and software in order to build a customized key-logger. Deployment of a key-logger is difficult since manufacturers build the devices so that only trained personnel know how to access the circuits without damaging the device or tripping the tamper alarm.

In this article, I propose a new approach to key-logging. Since common keyboards and keypads have rigid user interfaces, it is possible to detect keystrokes by tracking the user's body movements and crossing that information with the layout of the keypad. Body tracking technology is commercially available and already in use for gesture recognition and computer vision.

The aim of this article is to alert users to the risks of body tracking technology for the purpose of key-logging. To explore these risks, I designed and built a body key-logging "proof-of-concept" device from commercially available components and demonstrated its functionality on the keypad of a commercially available safe.

Malicious Key-Loggers

Malicious key-loggers' most fundamental requirement is to track keystrokes of an unsuspecting user in order to reveal the data to the person who planted the key-logger. Researchers, including Olzak¹ and Creutzburg², divide key-loggers into two main categories: software-based and hardware-based. Software-based key-loggers are installed on the victim's device or on a device which is connected to the victim's device. Hardware-based key-loggers are based on dedicated hardware, whose main purpose is to act like a key-logger. Hardware-based devices are either

connected to the victim's device or installed close to the victim's device to monitor various physical emissions. Simple hardware key-loggers are physically connected to keyboards and are able to extract keystrokes using the keyboard interface. More sophisticated key-loggers track measurable physical properties of the keyboard, like electrical properties, acoustics, electromagnetic emissions, and more. Another approach to hardware-based key logging is to use a well-placed surveillance camera to recover keystrokes from captured images, as demonstrated by snopes.com³ and Maggi et al⁴.

When deploying a hardware-based key-logger, the attacker is required to connect the hardware to the victim's device or place it near the device. This is done by either physically accessing the device or by installing it close enough for the key-logger to track the data. When deploying a camera-based key-logger, installation locations are limited by the conditions needed for successful data extraction. The attacker needs to take into account the location of the keys, the location of the fingers, the camera angle, the light conditions, and any other factor that might limit the image processing algorithms to recover the data from the captured images.

Numeric Keypads Under Attack

A numeric keypad is a set of buttons arranged in a block which mostly bear digits. Numeric keypads are found on devices such as ATMs, safes, combination locks, and digital door locks. When using these devices, the user is required to enter an access code to access locked products, money, or information. Since the access code is the key to an immediate profit, the keypad is a natural candidate for a key-logging attack. But planting a key-logger on such a device is hardly easy for the following reasons:

- In many cases, the hardware and software are embedded (e.g. Oke Alice et al⁵ and Lawan et al⁶). In order to design a dedicated hardware key-logger or a dedicated software key-logger, the attacker needs to be familiar with the device's circuitry and code.

- Device designers are aware that the circuits and the keypad are the key to locked goods and make an effort to stop unauthorized personnel from accessing the device's control unit (e.g. Sargent and Greenleaf Inc.⁷ and Nortek Security and Control⁸).

Plore⁹ demonstrated an electronic safe lock attack by analyzing the current consumption of the device. This attack did not use a key-logger by definition, but it resembles a key-logger attack in the sense that it measured and analyzed the electrical properties of the device. This attack is done by tampering with the device. Such an operation on a public device will draw much attention to the attacker and most likely will leave evidence that the safe has been tampered with.

Camera-based key-loggers exploit the interaction between the victim's fingers and the device keypad. This approach is harder to detect since the compromised device is not tampered with. The greater the distance between a disguised key-logger and a compromised device, the harder it is to link the two and expose the attack. The attacker does not need to be familiar with the device's circuitry or software, making it easier to focus on the development of the key-logger. Since a camera-based key-logger relies on image processing, it entails requirements for sensors, algorithms, processing power, and battery usage. It is also limited by the limitations of photography, such as the need for a clear line of sight and sufficient lighting - a keypad would be hard to photograph if the victim stood close to the keypad and blocked either the view of it or the light.

Body Key-Logging

When a user presses the keys on a keypad, an interaction is taking place between the user and the device. On one side of the interaction there's the device: the hardware, the software, and the mechanics. On the other side of the interaction is the user: mind, senses, limbs, and fingers. In the middle, there's the interaction: the keys of the keypad are pressed one at a time and, in some cases, there's physical feedback to the user, indicating a successful key press (either visible or audible). Most key-loggers target the device side of the interaction. A camera-based key-logger targets the interaction between the user and the device from a viewpoint. Martinovic et al¹⁰ conducted

experiments whose goal was to extract PIN numbers from the victim's brain. I propose a method to target the interaction between the user and the device from the user's side of the interaction.

Each keypad has a defined layout and dimensions. Therefore, the user is forced to press keys that have a well-defined position in space. This can be a vulnerability, since eventually the user will press these positions in space in order to enter a code. A well-positioned key-logger based on a 3D camera (a camera with an ability to record spatial information) will be able to record the user's movements. Since the keypad's layout and dimensions are rigid and known to the attacker (either in advance or upon key-logger deployment), an algorithm may be found to link the finger positions and the keypad layout in order to detect the code. This link can be based on the absolute position of the keys (coordinates of each key in space) or on a relative position of the keys (by following the distance between each key press and using one of the keys for spatial registration). If the device has a user feedback mechanism which the key-logger can track, the 3D problem can be reduced to a 2D problem since the pressing event can be detected by other means.

Time-of-Flight (ToF) Sensors

An optical time-of-flight sensor measures the distance between the sensor and an object. It is based on the time difference between the emission of light and its return to the sensor after being reflected by an object. Some sensors emit a short pulse towards the object and measure the time it takes for the light to return. Others emit modulated light toward the object and measure the phase delay of the returning light. Simple time-of-flight sensors are comprised of a laser source and a single receiver. More sophisticated sensors are comprised of an array of receivers and are considered as 3D time-of-flight cameras. Arrays of 320x240 pixels are commercially available while products having bigger arrays (e.g. Teledyne e2v¹¹) and higher depth resolution (e.g. Li et al¹²) are being developed.

Body Key-Logger "Proof-of-Concept"

To explore the body key-logging approach, I built a body key-logger. The target device I chose was a safe with a keypad (Yale YSV/200/

DB1 Electronic Safe, EAN: 5010609182200). The safe's keypad is shown in Figure 1. To open the safe using the keypad, a user is required to perform the following tasks:

- Enter the numeric code, digit by digit, by pressing the numeric keys of the keypad. Upon each successful keystroke, the device makes a noticeable sound and lights an indicator to indicate a numeric keypress.
- Press one of two “code entered” keys - either the “Enter” key or the “Key” key. Upon a successful keystroke, the device makes a noticeable sound and lights an indicator to indicate a successful or unsuccessful code entry.
- Rotate and pull a handle to open the safe door (assuming the code entry was successful).



Figure 1: Safe's Keypad

The vulnerabilities I decided to exploit in the user-device interface were:

- Each key has a fixed position.
- Each key has a fixed function.
- Audio feedback indicates a successful key press.
- After entering a personal code, the user is forced to press either the “Enter” key or the “Key” key.

The circuit I designed is shown in Figure 2. It is comprised of a line of optical time-of-flight sensors. When scanned periodically, the line of sensors creates a detection plane that is used to track the horizontal movement of the key-pressing finger in front of the keypad. The design assumes that the user is pressing each key with a single finger and that the remainder of the fingers are held in a fist which does not change from one key press to another. Two properties are read from each sensor:

the measured distance to the user's finger and return signal rate.



Figure 2: Body key-logger circuit

The circuit is also comprised of a microphone which is sampled periodically to detect successful key press events. Other major components are an STM32F303K8T6 microcontroller, an ambient light sensor and an IR LED. The microcontroller executes the body key-logger software. To save on battery power, it is assumed that the safe is not exposed to light when it's not in use (e.g. the safe is installed in a drawer or a closet). The ambient light sensor is used to detect the decrease in ambient light (keypad not in use) or its increase (keypad in use) and to set the power consumption mode of the key-logger accordingly. The IR LED is used to transmit the logged key presses to an external terminal, upon request, using IR light.

The key-logger device was designed to be disguised as a magnet or a sticker, as shown in Figure 3. It could have been designed to be deployed in other forms (e.g. placed on a wall next to the safe).

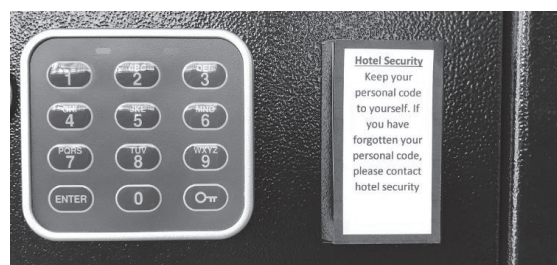


Figure 3: Body key-logger deployment

When not in sleep mode, the software scans the time-of-flight sensors waiting for object detection. When the victim's finger enters the detection plane, the software stores detection data records in a buffer until a "successful key press" audio event is detected. When the audio event is detected, the software stores the data records in the key press buffer. These records comprise the information derived from the user's finger position at the time of the "successful key press" audio event. When the attacker requests code extraction, the software performs the following steps for each key press event:

1. Finds the last data record before the audio event
2. Selects the readings with the highest return signal rate
3. Estimates the object's position on the sensors' axis using the following average:

$$\bar{X} = \sum_{i=1}^m \hat{p}_i x_i$$

\bar{X} is the average position

\hat{p}_i is the return signal rate of sensor i

x_i is the position of sensor i .

4. Calculates the range to the object by doing a linear interpolation on the range data of the two sensors closest to the estimated object position.

The software then determines if the last key pressed was the "Enter" key or the "Key" key:

- If a key pressed was to the right of the last pressed key and the range from the last pressed key was larger than two thirds of the keypad key column margin, then the last pressed key most likely was the lower left key, or the "Enter" key.
- Otherwise, if a key pressed was to the left of the last pressed key, and the range from the last pressed key was larger than two thirds of the keypad key column margin, then the last pressed key most likely was the lower right key, or the "Key" key.
- Otherwise, if the last pressed key range was beyond the distance between the detectors and the middle column of the keypad, then the last pressed key most likely was the lower left key (the "Enter" key).
- Otherwise, most likely the lower right key was pressed (the "Key" key).

The last two steps solve the ambiguity problem in the case where the code is limited to a single keypad column. The two steps assume that the distance between the key-logger and the middle column of the keypad

is known. A different approach can be taken by recovering keys pressed twice - once for the left column and once for the right column. In this case, the attacker's interrogation will yield two recovered codes instead of one. One of the recovered codes will be correct.

After choosing the role of the last key pressed, the software performs the following steps:

1. Finds the closest key grid to the detection grid (closeness defined as the sum of the minimum distances).
2. Determines the numeric value of each pressed key by finding the closest distance to a key at the closest key grid.
3. Transmits an encoded message via the IR LED (that is attached to the attacker's reading device).

Proof-of-Concept Tests Results

The "proof-of-concept" tests were mostly conducted with the key-logger placed one inch to the right of the keypad. The pointer finger was used to press the keys while the rest of the fingers were clenched. The tests were performed using both left and right hands and similar results were obtained. An example of key position recovery is shown in Figure 4.

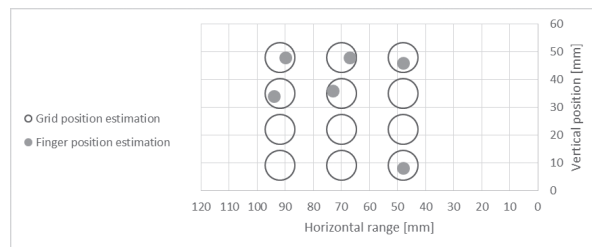


Figure 4: Finger position estimation example for "1-2-3-4-5-Key" code

An example of key position recovery and matching return signal rate is shown in Figure 5 and Figure 6.

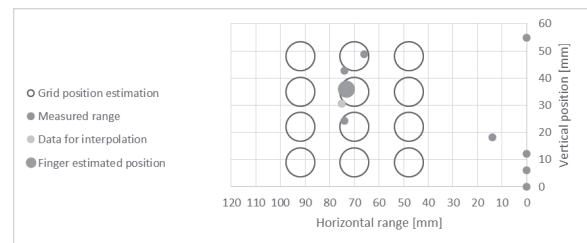


Figure 5: An example of finger position estimates for the "5" key

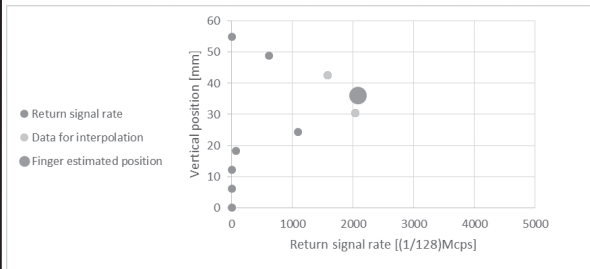


Figure 6: An example of return signal rate for the “5” key

Each sensor used in the device was comprised of a light source with a 25 degree illumination cone. To avoid the keypad’s frame detection, the sensors were tilted, as shown in Figure 7. The wide illumination cone causes side detections in the horizontal plane which are shown in Figure 5 and Figure 6. Since only a single key is pressed at a time, it is relatively easy to recover the physical location of the finger. On the vertical plane, the wide illumination cone influences the ability to detect the pointing finger. When the finger is short or when the finger is not perpendicular to the keypad, the side detections reflect the side view of the fist. By blocking the upper and lower parts of the lens of the light source, the angle of the illumination cone was reduced and the probability of successful detection was improved.

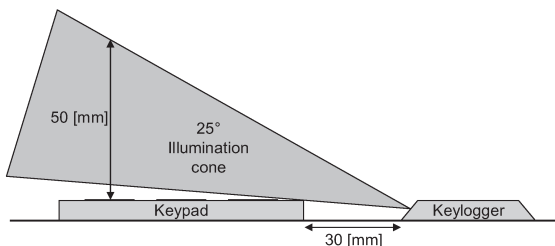


Figure 7: Time-of-flight illumination cone

I conducted tests to evaluate the probability of successful keystroke detection. The tests were performed by seven people, each entering the following codes: 1-2-3-4-5-Key and 1-2-3- 4-5-Enter, in an alternating manner. In every test, the codes were entered 25 times (a total of 150 key presses). The average probability of successful detection was 92 percent. Test results per subject can be seen at Table 1.

Subject Number	Hand	Successful detection probability [%]
1	Right	100
1	Left	100
2	Right	96
3	Right	93
4	Right	92
5	Right	86
6	Right	85
7	Left	83

Table 1: Successful probabilities of recovery test results

Battery Consumption

Based on the current consumption of the circuit, battery capacity, and circuit activity period per day, the battery time was calculated. Calculated battery time versus activity period per day is shown in Figure 8.

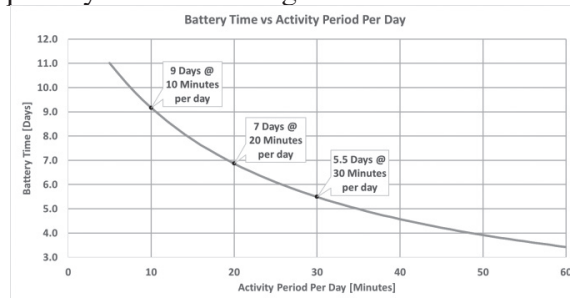


Figure 8: Battery time versus activity period per day

Discussion

Common keyboards and keypads have rigid user interfaces, making it easy to extract keystrokes by following the body movements of the user and correlating the data to the key layout. This would have been harder to do if the user interface was not rigid. Touch screens as well can be used to achieve this goal if at each iteration the layout changes. An example of an arbitrary keypad layout is shown in Figure 9.

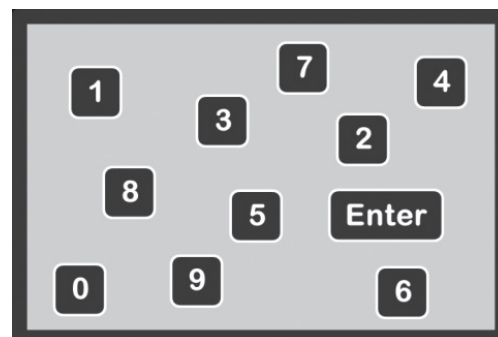


Figure 9: An example of an arbitrary keypad layout
Snyder et al¹³ show that skilled typists’

explicit knowledge of the key locations is incomplete and inaccurate. This emphasizes the importance of the key layout. To improve the user's ability to remember the code, I suggest that graphic signs other than numeric keypad keys be used. Intelligent Environments¹⁴ suggests replacing numeric PIN codes with emoji codes. Other graphic signs that could be used are colors, letters, icons, emoticons, etc.

Audio feedback is relatively easy to detect and exploit to improve the probability of key detection. It may be replaced with a narrow field of view visual sign that is visible only to the user.

Future Directions

The device used for the "proof-of-concept" can be improved in several ways. The sensor positioning and the data processing algorithm can be improved to reduce the device's physical dimensions. The tracking approach can also be changed. One approach could track the side view of the hand, instead of tracking the finger. A different approach can track the wrist or the forearm.

3D time-of-flight cameras should be explored as they offer a wider range of tracking options. They may also increase the physical range at which the key-logger is deployed.

Acknowledgments

I would like to thank my wife and our children for supporting my endeavor. I would also like to thank you, the reader, for your interest in my work.

References

1. T. Olzak, "Keystroke Logging (Keylogging)", 2008.
2. R. Creutzburg, "The strange world of keyloggers - an overview, Part I" *Electron. Imaging*, vol. 2017, no. 6, pp. 139–148, 2017.
3. Snopes.com, "ATM camera", www.snopes.com/fact-check/atm-camera/.
4. F. Maggi, A. Volpatto, S. Gasparini, B. Simone, G. Boracchi, S. Zanero, "A fast eavesdropping attack against touchscreens", 7th International Conference on Information Assurance and Security, IEEE, 2011.
5. O. Oke Alice, A. Adigun Adebisi, S. Falohun Adeleye, F.O. Alamu, "Development of a Programmable Electronic Digital Code lock system", *International Journal of Computer and Information Technology*, Volume 02– Issue 01, 2013.
6. M. B. Lawan, Y. A. Samaila, I. Tijjani, "Microcontroller Based Electronic Digital Lock with Security Notification", *Journal of Engineering Research and Reports*, Vol.: 2, Issue: 3, 2018.
7. Sargent and Greenleaf Inc, "Easy View/Tamper Resistant Keypad for Comptronic Locks Installation Instructions", Document part number: 630-614, Revised 04/13/2006.
8. Nortek Security and Control, "212iLW and 242iLW Standalone Keypad Installation and Programming Manual", Document number: 6-050700 X2, 2015.
9. Plore, "Side-channel Attacks on High-security Electronic Safe Locks", DEF CON 24, 2016.
10. I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, D. Song, "On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces," USENIX Security Symposium Bellevue, WA, 2012.
11. Teledyne e2v, "1.3MP BORA CMOS SENSOR", www.e2v.com/products/imaging/cmos-image-sensors/bora-1-3-time-of-flight-sensor/.
12. F. Li, F. Willomitzer, P. Rangarajan, M. Gupta, A. Velten, O. Cossairt, "SH-ToF: Micro resolution time-of-flight imaging with superheterodyne interferometry". ICCP 2018, 2018.
13. K. M. Snyder, Y. Ashitaka, H. Shimada, J. E. Ulrich, and G. D. Logan. "What skilled typists don't know about the QWERTY keyboard". *Attention, Perception, and Psychophysics*, 76, 162–171. 2014.
14. Intelligent Environments, "Now You Can Log Into Your Bank Using Emoji," Jun. 2015, www.iedigital.com/resources/press-releases/now-you-can-log-into-your-bank-using-emoji/.

The Hacker Perspective

by Captain Crackham

Sometimes, hackers of a certain age may feel that they were born a generation too early. With the abundance of silicon in every setting powered by the kind of processing grunt that was unthinkable a few short decades ago, and the proliferation of free online courses in programming (that's what we used to call coding, youngbloods), obstacles to becoming the next visionary of the digital age have never been fewer.

Like so many hackers of my generation who grew up in England, I only got into computing from such a tender age through sheer luck. An older sibling bought a Sinclair ZX81, a monolithic piece of black plastic that connected to a flickery CRT television. I was instantly drawn to it like a magnet.

Learning how these beautiful, mysterious, and, at first, horrifically unreliable works of art ticked was far from an easy task. Being a child of the eighties, reference guides couldn't even be found in most local libraries, the Internet had yet to make an appearance, and schools could barely afford a single BBC Micro, never mind staff who had actually been trained to use them. Code, however, wasn't buried away to the same extent that most proprietary junk is today. In fact, entire programs were printed out in enthusiast magazines for the patient and studious to copy out into their beloved computers. And of course, once you realize how the words on the pages push the pixels and bitmaps around on the screen, you can adapt and bend them to your will.

Despite barely getting a look-in himself, my brother went on to upgrade to a Sinclair Spectrum 48K, a Commodore 64, and the mighty Commodore Amiga. By this point, the gaming scene had really taken off, and copious demos and other software were given away on magazine coverdisks. These coverdisks would include a menu system to access what was on them which, with a modicum of effort, could be copied, tweaked, and customized. And so, I would busy myself compiling and adapting the best demos from across the mags onto one glorious disk, ready for my brother to enjoy with the increasingly limited time he had to spend with what was still technically his computer. Yes, you really could fit multiple demos onto one 1.44MB floppy.

Around the same time, Datel released the

Action Replay cartridge. This came with a hardware button that, when pressed, would instantly halt whichever game was running and give you access to a console where you could examine the code that was in memory and, better still, mess with it. This opened up the possibilities of taking screenshots long before this functionality became baked into OSs, and altering values that were in the RAM to award extra lives or to kill timers in trial software that otherwise planned on ruining our fun. At one point, I'd managed to mod a copy of the original *Worms* so that the titular stars would swear like dockers throughout every game.

Running alongside all of this was the public domain scene. Much like the open source scene today, PD wares consisted of various utilities and demos put out by passionate programmers who wanted to help their fellow enthusiasts push their systems to their very limits. The most exciting aspect of this was the demo scene. These weren't demos in the same sense as the game demos distributed on coverdisks, but more like mostly non-interactive technical demos that would package together some truly incredible audiovisual experiences that didn't so much move the benchmarks of what was thought possible with the hardware at the time as absolutely obliterate them.

These took many forms, ranging from compressing "Flash" by Queen onto a single floppy long before the MP3 standard was even thought of, showcasing the brilliant animated short "Pugs In Space," and melting eyeballs with psychedelic proofs of concept for what our hardware was really capable of. These latter demos were produced by several pioneers of the time, but many of the most impressive were the product of the mighty Red Sector Inc. If you're unfamiliar with their work, I implore you to search for the "RSI Megademo" on YouTube to enjoy some of the greatest chiptunes to be committed to magnetic media.

PD was distributed through mail order adverts in magazines where you would pay for the cost of the disk and postage, through gatherings such as computer shows and parties, and via the good old-fashioned Sneakernet. Outside of the public domain scene, more corporate interests were trying incredibly hard to convince us that free distribution would lead to the down-

fall of computing itself, but we had other ideas about that.

While the hobby was becoming increasingly popular, it was still largely restricted to those of us who gladly embraced the nerd and geek labels that were nowhere near as cool then as they've become today. Finding fellow enthusiasts lurking in the school library would always lead to an excited meeting where both parties would produce their cases of copied floppies. At the front of every case was X-COPY, the de facto copying software of the time that was so good it was quickly hacked to be effective at natively defeating almost every copy protection that existed, even the DRM ironically placed onto later versions of X-COPY Pro. Whoever had the older copy of X-COPY would always begin the ritual by making a copy of the newer version for themselves, and then the real fun would begin.

Whilst fully entrenched in the golden age of Amiga computing, IBM-compatible PCs were starting to appear in schools. I began my high school years experimenting with the new, exotic but somehow inferior file systems employed by the PCs that made up what could quaintly be described as the school network. Security was barely thought about back then, but it was still a surprise when experimenting with the command line interface led to me stumbling upon the password file for every account holder in the school in plaintext.

Our school was big on learning by doing, so they must have been delighted when they found that one of their students had supplemented their IT classes with a few extracurricular activities. On the hackers' curriculum was swapping the staff passwords around, helping the deputy headmaster to declare his undying love for the headmaster via the network's internal messaging system, and hosting a full copy of *Doom* in the headmaster's personal storage space for the students to download and run on the other school computers.

As school gave way to university and the simple pleasures of cloning the copy cards containing printer credit for the libraries, a new spin on a much-treasured pastime had come about: home copying was being replaced with Internet piracy. This was of great interest to me for two reasons. First of all, I was resolutely unsurprised to discover that, despite all the rhetoric of the "Don't Copy That Floppy" advertising, the games, film, and music industries were somehow still going despite a few nerds making copies in playgrounds and offices. Secondly, it dawned on me that there was a beautiful confluence between the two things in life that had always enthralled me: hacking and piracy.

Of course, *2600* was way ahead of the curve on this. Anyone who saw the June 1987 issue (4:6) will have enjoyed the sight of a jolly pirate lurking over a phone ready to be phreaked in protest of the corporate monopolies of the time. Personal privacy aside, hackers believe in the freedom of information, and tend not to take kindly to corporate interests telling them how to behave. While not every pirate is a hacker, piracy as it is today would not exist without hackers creating tools such as Napster and BitTorrent, and busily cracking and stripping away the DRM that's increasingly infested our otherwise open digital lives.

As university progressed, and I once again noted that the "You Wouldn't Steal A Car" nonsense didn't successfully predicate the downfall of the entertainment industries, I realized that there wasn't much actual, proper, decent academic research into all this. And that's when I decided to become a researcher in online file sharing.

Whilst working as a lecturer for the university at which I'd graduated, I diligently spent my nights designing, implementing, and executing an online survey into piracy. A year and one thousand responses later, I submitted my research study, conclusions, and all of my data to an academic journal. At the time, this was the largest study of its kind into piracy that had ever taken place, which made the results all the more exciting. Basically, people who pirate stuff without paying for it tend to spend more money on the same entertainment products than people who don't.

The world apparently didn't share my excitement, as my study was largely ignored. This didn't particularly bother me as I hadn't expected otherwise, and the fun of carrying out the study was more than enough to make it worthwhile. But then, a few months later, a study similar to my own was released. This was fascinating for a number of reasons, not least in that it had been carried out similarly to my own study, and had coincidentally been produced by a team at my university (albeit in a different department, so it genuinely was a coincidence). But the biggest surprise is that it had been released by the university to great fanfare and, consequently, had been picked up by most of the press.

As the study was similar to my own, I was keen to examine it and compare the data sets. However, the data sets hadn't been released. No matter what I tried, I absolutely could not pry the raw data from the researchers who had put this beast together and, being of the pirate-hacker mindset, I just couldn't understand why this particular information was not free. It turned out that it was "proprietary," and thus not to be shared.

But surely a university which, like all of them, has charitable status due to its supposed contributions to public knowledge would also consider this data to be public knowledge, wouldn't it? Except it didn't, because it didn't pay for it. It was, in fact, paid for by a coalition of companies who represent copyright holders. You know, those guys who have been trying for years to perpetuate the fantasy that noncommercial piracy is killing their staggeringly rich and constantly growing monopolies. And so it was that I discovered what I now know to be the phenomenon of scholars for dollars.

It's simple, really. You're in the business of producing popular culture, but you don't like the fact that some people think you charge too much for it. You've tried paying for advertising and throwing out snappy little slogans but, try as you might, you can't convince those pesky consumers of culture that not being ripped off by you is the equivalent of grand larceny. If only you could get those damned troublesome consumers to see things your way, and get them back in line.

But wait a minute, if they won't listen to you, surely they'll listen to those brainy types who hang around in universities? So, all you have to do is write a big fat check from all the money you've parasitically siphoned away from creators and consumers, and hand it to a university. A few months later, that same university will produce a publication that says, "We carried out a study into piracy, and can conclude that it's comparable to genocide." You can then put the full might of your PR department into pushing this line right up until someone asks for the actual data so they can check if it's been collected and analyzed properly. At which point you can say, "Sorry, bud, but this is commercially sensitive proprietary information that absolutely nobody can look at, ever."

On this planet, it's PR departments who set the news, not rationality and common sense. This is why laws and treaties are still written and court cases still decided on the basis of what is a proven lie that's been perpetuated by the copyright industries through the reliable scholars for dollars route. This misrepresentation of cold hard facts has become so bad that, in the U.K., copyright industry coalitions are partly funding a specialist police force that's dedicated to arresting and harassing those who challenge their attempts at imposing artificial scarcity to digital culture, and the government has mandated the brainwashing of children in our schools with anti-piracy propaganda. Do you older folk still think you were born too early?

There is a happy end of sorts to this tale. Another of the many breathtakingly dishonest rackets I've encountered in my time as a

researcher who asks too many awkward questions is academic journals themselves. If you're a researcher and you want to publish your hard work, you've traditionally had to submit it to one of these journals. Said journal will then pay not a single penny for this work, which is fine, considering we're supposed to be doing this stuff for the advancement of public knowledge. What's less fine is that they then charge universities and students, if they're rich enough, thousands to access all of these studies that they've acquired for free.

Happily, the brightest minds of academia have pushed back against this with schemes such as the Social Science Research Network, where researchers can host their papers for anyone with an Internet connection to access for free. Never ones to be left out, the pirate-hackers have played their part too with *Sci-Hub*, the wonderful repository of knowledge and information that would otherwise be scandalously locked away behind a paywall. Due to submitting some of my earlier work to the academic racketeers at the start of my career, I've actually had to pirate some of my own papers to submit them to these fantastic institutions. Needless to say, I've published everything since under a Creative Commons license.

If life on this weird planet has taught me anything, it's that describing yourself as a hacker or a pirate to anyone who doesn't identify as either of those things themselves unfailingly courts gasps of horror. It's also taught me that hackers and pirates are the only groups left who actively give a damn about freedom and openness, who honestly believe that sharing is caring, and who will always be ready to push back when we're told that our technology and behavior is a threat to the world's backwards way of doing things.

The playground didn't care when the corporations tried to tell us not to copy that floppy, and the Internet doesn't care that the same gluttons are trying to build laughingly ineffectual artificial barriers on top of it to push around the same community on a larger scale. A youth spent immersed in the world of a fledgling technology that was nourished by a culture of openness and sharing has taught me to live by those principles. I don't tell people that I'm a hacker, or a pirate. I tell them that I'm a pirate-hacker, and will proudly fly the black no matter what they think.

Captain Crackham is still writing and asking awkward questions. He continues to immerse himself in the latest developments in the piracy scene, and is now learning how to make games. If any make it to release, they will not contain DRM.

Rehabilitation Center - (Attacker's) Mission Complete



by Ig0p89

In general, people for the most part are healthy. At times, we have issues requiring surgery and later rehabilitation. Based on the injury, this could be a short or long journey. Regardless of the length of rehabilitation, the patient needs to provide certain data and information to the facility where the treatment will take place. This data is personal and confidential, and should be protected with all appropriate levels of security. Unfortunately, a rehabilitation center in the Michigan system was recently compromised.

This affected the Sacred Heart Rehabilitation Center. As noted, this is located in Michigan in Macomb County. The facility provides HIV/AIDS care. There are also substance abuse treatment services. They operate as a nonprofit, beginning in 1967. As this is a nonprofit, the last thing they needed was the expense of a compromise, incident response, and placing new controls and policies in place. That's only on the internal administrative side. There will be more issues with the U.S. Department of Health and Human Services, as this involved HIPAA data and information.

Attack

The tool the attackers used is too familiar. This unfortunately has a great ROE (return on equity), and ease of use, which makes it a favorite choice. This successful compromise shows the phishing attack is alive and well. The compromise was due to a simple, yet successful, phishing campaign. The estimated attack period was from April 5-7, 2018. From the forensic work already done, it appears as though one employee's email was compromised.

This significant, deep compromise is another example of what can go wrong when one employee's email is compromised. All it takes is the right person in the right position and department to click once.

Data Exfiltrated

The compromised employee's email account unfortunately contained the patients' information. This included the patients' full names, addresses, health insurance information, medical treatment information, medical diagnosis, and/or Social Security number. This

is just the right combination of data to make someone's life even more interesting. As the patients are exceptionally sick, they and their families did not need this stress. On the other side of the coin, the data and information is very valuable to the attackers, and could be sold in a lot, or divided into sections and sold to many persons.

Remediation

Once the administration learned of the issue on November 16, 2018, the rehabilitation center began an investigation, which is a great idea. The rehabilitation center contracted with third parties to complete the cybersecurity forensic work. The Sacred Heart Rehabilitation Center notified the affected parties. The forensic work indicated the affected parties, thankfully, were limited. Letters were mailed to the affected parties on January 9, 2019. The patients whose Social Security numbers were exposed were offered a credit monitoring service and identity theft restoration for a year, free of charge. The patients also have been given a best practices document to show them how to best defend their data. The rehabilitation center is also providing additional training for the staff.

Questions

The compromise itself brings up many issues. Since the successful attack and compromise took place in April, why did it take seven months for them to figure it out? If there was a SIEM (Security Information and Event Management) in place and being monitored, it seems as though this should not have taken nearly this long. Even if there was not a SIEM in place, which sounds odd, there should have still been a periodic log review. Surely the massive amount of data flowing to an odd IP address would have indicated something odd or unique was going on.

The credit monitoring sounds good to the consumer and patient, however, a year does not mean much. The data exfiltrated for the unfortunate patients is static for that point in time, and some of this is permanent. If the attackers were to attach a disclaimer onto the data as they sell it to the many people and organizations interested to wait one year and one week to do anything with it, the defensive measure would be an epic fail.

HOW TO GET FREE WI-FI ANYWHERE

by Curufuin

The purpose of this article is to provide an easy method for acquiring free Wi-Fi access from a van or RV in most major cities. (I am happy to report that many small towns in Vermont also have free Wi-Fi and this method works there as well.)

We will need to set up a Raspberry Pi to more or less act as a router that you will connect to from your Wi-Fi enabled devices and it will forward your devices transparently to a nearby open Wi-Fi or a password protected Wi-Fi for which you put credentials in the passwords.txt file. As you come into range of a network or multiple networks, the Pi will connect to the one with the strongest connection. You can also blacklist things like Comcast open networks, since they may have a good connection, but require credentials through a captive portal interface. If you are a frequent 2600 reader, you will be familiar with spoofing your MAC address to connect to a network that uses a captive portal, but I will not cover that here, though I may add that functionality to my program in the future.

So I had a kind of unique problem getting started with my Raspberry Pi. I live in a van and, until recently, connected to the Internet via mobile hotspots (which I was paying \$70 a month for through Cricket (not a terrible deal if you can afford it, but totally unnecessary now)). I don't have, nor do I want, a spare monitor hanging around as I don't want it to take up room in the van. So I had to do a little digging.

The first steps to installing your Pi are as normal. Download a Raspian image and use the "dd" command to load it to an SD card that has been formatted with FAT.

First, determine where Linux has mounted your SD card before plugging it into your card reader. Go ahead and type the following into your terminal application of choice:

```
fdisk -l
```



Now plug it in and type the previous command again and the new device is your SD card. Most likely it will be at /dev/sdb.

Next, format the SD card for FAT or VFAT if your card is 32GB (make sure you have the right drive unless you want to get acquainted with hard drive recovery software, as this will overwrite the partition on the current drive):

```
mkfs.fat /dev/sdb
```

Next, download and unzip a Raspian image and copy the image onto your SD card:

```
dd bs=4M if=path_to_raspbian_
  image of=/dev/sdX(probably sdb)
  conv=fsync
```

This step often fails because crappy card readers can't seem to handle it. If that is the case, you may have to buy a card reader that can. I have one from Steelton Tech that works well, but the one built into my laptop does not. It can be a real pain, but if you can find one that works well, it will save you many headaches.

Now that you have the image on the SD card, remount the card and add a blank file named ssh to the /boot partition as well as a file called wpa_supplicant.conf, which we will edit as follows:

```
ctrl_interface=DIR=/var/run/wpa_
  supplicant GROUP=netdev
network={
  ssid="YOUR_NETWORK_NAME"
  psk="YOUR_PASSWORD"
  key_mgmt=WPA-PSK
}
```

Save the file in the /boot partition.

Finally, we need to edit the /etc/dhcpd.conf file. Add this to the bottom of the file and save it:

```
interface wlan0
static ip_address=(IP ADDRESS
  YOU ARE ASSIGNING HERE)/24
static routers=(IP OF ROUTER)
static domain_name_servers=
  8.8.8.8 8.8.4.4
```

Finally, you can unmount the SD card and

plug it into your Pi.

Plug in the Pi and the red power indicator should stay on, and the green ACT indicator should blink a bunch, stay on for about 30 seconds, and then turn off.

At this point, from the computer you would like to SSH in from, ping the IP of the Raspberry Pi until it comes online:

```
ping (Pi's IP here)
```

When it comes online, you will see it change from Host Unreachable like so:

```
From 192.168.43.6 icmp_seq=19
↳ Destination Host Unreachable
From 192.168.43.6 icmp_seq=20
↳ Destination Host Unreachable
From 192.168.43.6 icmp_seq=21
↳ Destination Host Unreachable
From 192.168.43.6 icmp_seq=23
↳ Destination Host Unreachable
From 192.168.43.6 icmp_seq=24
↳ Destination Host Unreachable
64 bytes from 192.168.43.10: icmp_
↳ seq=26 ttl=64 time=1706 ms
64 bytes from 192.168.43.10: icmp_
↳ seq=27 ttl=64 time=683 ms
64 bytes from 192.168.43.10: icmp_
↳ seq=28 ttl=64 time=10.2 ms
```

Now you can login using SSH:

```
ssh pi@ (Pi's IP here)
```

The default password will be “raspberrypi” and we will go over how to change that shortly....

Now that we are connected, we need to connect another wireless adapter to the Pi. I chose the ALFA AWUS036NH, which is boosted by an amplifier connected to a 16 dBi antenna.

Next, we will need to bring in some tools to turn the Raspberry Pi into a hotspot like so:

```
sudo apt-get install python-pip
↳ hostapd dnsmasq git
```

Now we need to stop hostapd and dnsmasq from running while we configure them using:

```
sudo systemctl stop hostapd
sudo systemctl stop dnsmasq
```

Next, we need to configure a static IP for wlan0 in /etc/dhcpd.conf like so:

```
interface wlan0
static ip_address=192.168.4.1/24
nohook wpa_supplicant
```

where 192.168.4.1 is the static IP for wlan0. This could be any IP of your choosing.

Next, let's configure the DHCP server.

First, make a backup of the default:

```
sudo mv /etc/dnsmasq.conf /etc/
↳ dnsmasq.conf.orig
```

Then we will edit /etc/dnsmasq.conf by adding the following:

```
interface=wlan0
dhcp-range=192.168.4.2,
↳ 192.168.4.20,255.255.255.0,24h
```

Now we need to configure hostapd by creating/editing:

```
/etc/hostapd/hostapd.conf:
touch /etc/hostapd/hostapd.conf
```

and edit it to contain the following:

```
interface=wlan0
driver=nl80211
ssid=NETWORK
hw_mode=g
channel=7
wmm_enabled=0
macaddr_acl=0
auth_algs=1
ignore_broadcast_ssid=0
wpa=2
wpa_passphrase=PASSWORD
```

```
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
```

Then we have to tell the Raspberry Pi where the configuration file lives by editing /etc/default/hostapd:

```
DAEMON_CONF="/etc/hostapd/
↳ hostapd.conf"
```

Now we need to forward the traffic between the interfaces. In the /etc/sysctl.conf, uncomment the line that says:

```
#net.ipv4.ip_forward=1
```

It should now just read:

```
net.ipv4.ip_forward=1
```

Now we will enable IP masquerading on wlan1 with the following iptable rules:

```
sudo iptables -t nat -A
↳ POSTROUTING -o wlan1 -j
↳ MASQUERADE
sudo iptables -A FORWARD -i
↳ wlan1 -o wlan0 -m state
↳ --state
RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i
↳ wlan0 -o wlan1 -j ACCEPT
```

and save it:

```
sudo sh -c "iptables-save >
└─ /etc/iptables.ipv4.nat"
```

Next, tell the Pi to reload the iptables on boot by editing `/etc/rc.local`. Just add the line:
`iptables-restore < /etc/iptables.ipv4.nat`

and reboot:

```
sudo reboot
```

Once the Pi is booted, give or take about a minute and a half, you should see a Wi-Fi network with the name you assigned in the previous steps and you should be able to log into it using the password you assigned. Then you can SSH in again and change the password for the user Pi:

```
passwd
```

You will be prompted for the current password, which is just "raspberrypi" and then to enter a new one. Keep it secret, keep it safe (insert rant on password security here). If you keep it the same, somebody on a network you connect to can easily just SSH into your router and muck about, which is certainly not ideal.

Next, we need some dependencies for the python script that will look for open Wi-Fi for us. The following should pull all of those in. (By the way, the script is using Python 2.7, not Python 3. Sorry, not sorry, feel free to fork it and fix it.)

```
sudo pip install wifi wireless
└─ netifaces
```

Everything else should be in the standard libraries.

Now make a folder where you want the project to live and clone the git repository as follows:

```
git clone https://github.com/
└─ curufuin/vanlife
```

This should give you a few Python files as well as some text files.

`blacklist.txt` is an ESSID blacklist you can fill with the names of Wi-Fi networks you don't want to connect to in the future. It has a few defaults, but you can add new ones, one name per line.

`passwords.txt` contains passwords for secure Wi-Fi for which you have the password. The format is `ssid:password` - one entry per line.

Finally, `connector.py` is the program that does the heavy lifting. I have it run once a minute from the crontab. You can edit the crontab as follows:

```
sudo crontab -e
```

Select your favorite editor and add the following to the bottom of the file:

```
* * * * * /usr/bin/sudo /usr
└─ /bin/python (path to connector.
└─ py) >> (path to log file) 2>&1
```

For good measure, I automatically restart the Pi every five hours because `hostapd` has some bugs that are sorted by restarting, so add this line below the previous:

```
1 5,10,15,20,23 * * *
└─ sudo /sbin/reboot
```

Now test this against some networks and everything should be working at this point.

The great thing about a setup like this is that you can also use the Pi as a Samba server for media, which you can connect to with your phone using VLC. You can also use Google Voice for phone calls and texts and get rid of your normal phone. I won't cover that here as this article could get quite bloated if I discuss everything I did for my van, but I will discuss one more thing. I like my privacy... a lot. So I wrote a little shell script that will give your computer a randomized hostname and MAC address. It is included in that git repository, and I suggest using it if you have a network card that supports it. First install `macchanger`:

```
sudo apt-get install macchanger
```

All you have to do to use that is add another line to your crontab:

```
sudo crontab -e
```

And add the following at the end of the file:

```
1 * * * * path to changemac.sh
└─ >> /home/mac.log 2>&1
```

In addition to this, I suggest using a reputable VPN such as `protonVPN` while connected to any open Wi-Fi you plan on using to log into anything requiring a password. There are working MITM attacks that could jeopardize your credentials.

Finally, you will probably run into some problems with paths in both `changemac.sh` and `connector.py` and, if you are running them from cron as should be the case, we will need to change some of the paths to be absolute. Open up `connector.py` and where it says `self.blacklistFile`, change the path to the absolute path on your system to the blacklist file. For me it is something like `/home/pi/connector/blacklist.txt`. Your mileage may vary. Then do the same for the `self.passwordsFile` variable. Now do the same for `changemac.sh`. Change `./hostnames.txt` to its absolute path. This should fix any problems you might be experiencing. Now reboot and reconnect.

```
sudo reboot
```

Good luck!

WHAT IS HACKING?

by JT Gordon

Let me illustrate the great difference between hacking with a club, a broadsword, a crystal ball (yes, people in the Middle Ages hacked with things similar to fortune cookies), and those things we use now.

Modern times have brought computers our way, things that at times I think, created our planet. Yes, I think that extraterrestrials built our planet with formulas and machines, or our so-called planet, an amalgamation of solids, liquids, and gases that has a pre-designated expiration date. Probably these extraterrestrials had to settle some sort of legal issue - maybe our species was enslaved - and as payback, this construct world was built. So, extraterrestrials are not always there, as not all extraterrestrials are nice or good or even decent.

No need to pay me, as I have no proof that I even exist. You'd have to hack into a database to get my birth certificate. I have no recollection of exactly what day in June I was born on. My relatives are going to prey on this fact, and what I do is basically work as a groupie for my own family. I have been told this, point blank. This makes me an undocumented American, basically. That is, until I am able to pull the records out of the files, which means that I will need to study computers. I had to rebuild my neurological components after the last attempt, however, that was back during the 1990s, before "Made in China" products became such a problem. Back then, the Brother personal notebook was just a toy, and the idea of offending Chinese and Japanese manufacturers with all sorts of barking mad intrusions designed to extract finances out of a company manufacturing products in the United States that was based in Japan was normal or de rigueur for many of my peers. If the Brother Corporation still manufactures any sort of a computer terminal, it is not being sold in the United States, and I'm not going to be able to read about it in English or any language in the Roman alphabet. Since then, I've forgotten kanji, which is the alphabet that Chinese is based upon, above a street punk or homeless person level. Getting the data from Chinese computers requires a certain language skill set. There is more to hacking computers than just buying expensive equipment. I can still write treatments in Chinese for brainless scripts like the *Resident Evil* series, which, of course, my superiors in Hollywood mistook for the *Rango* sequel script. Just in case you were wondering why *Rango 2* was not released, the script, obviously, was not going to work. Maybe the lizards should have written it.

Which brings me to the conclusion that the geckos are indeed the superior race, and might be responsible for the election of President Donald Trump. We're still not sure why reptiles prefer our current president, however, these creatures are world powers that would probably survive a nuclear war, which is something science has ignored for too long. Maybe it's classified information or something, so excuse me for even writing that, no worries, nobody will ever read it. Delusional and classified information are almost synonymous, so, it would probably be left off as something written by someone who had their brain fried by one of those power surge protectors. I woke up too stupid to file for my Brother personal notebook refund. No worries, my peer group's competition from the Cornell Farm got their hands on the fried personal notebook, and probably left their fingerprints on the inside of the machine. My fingerprints were also on the inside of that machine. However, I did not file for the refund.

Of course, sewing machines and sewing machine networks are all computerized - it was just that whatever consortium of business is going on in the Pacific decided that us wild and crazy gaijin barbarians were going to hack their networks to bits with more upgraded equipment, and that we Americans deserved more learning experiences, not more technology. Thus began the beginning of Project Dumbdown.

There is a difference between hacking or looking at data and corrupting data. A professional hacker will not corrupt data, however, we live in a corrupt society on a planet with a lifespan that is extremely limited, as any forward-thinking individual might state it. Corrupting, or even fragmenting data is something that also requires a hacker to repair. There are all sorts of ways of making data files full of things, like Microsoft Excel macros, which will render them unreadable. The majority of "computer viruses" are actually Microsoft Excel macros gone amuck. So, for those of you still on the learning curve, like me, there are times to go off-line, such as while becoming proficient at advanced functions of Excel.

There are ways of fragmenting data across networks, across computer terminals, across computer sectors - of turning important documents into jigsaw puzzles so to speak, or of reappropriating data. This is something that a computer hacker can sniff out and repair. Sorry, this is boring, it's not exciting, it's not rocket science or nuclear power plant repair - it's data management.

SENTIMENTS

Visibility

Dear 2600:

So I thought this was really cool. I am one of the very fortunate people in this modern era because I still get to go to my local Barnes and Noble bookstore right by my house and pick up the latest issue of 2600, which I do all the time. It's a fun treat that I always look forward to. Today I went there and 2600 was missing from the magazine section. I looked frantically, behind other magazines, checking other sections thinking they moved it, but it was nowhere to be found. Saddened, I went up to the clerk to ask if they too had finally stopped carrying my favorite publication. She looked it up on the computer and said "Oh no sir, we actually have it displayed on a special featured magazine shelf" located right in the middle of a high traffic section of the store, near the front door even.

I thought this was super cool. Not only are you guys still valuable to the local Sacramento people, you are showcased!

@brokergabe

This is indeed great news. We just hope people don't give up when they can't find it in the usual location. Maybe this will help bring in even more new people, which is what we ultimately want. (To find a store near you, check our new list of stores that carry us at www.2600.com.)

Dear 2600:

I have been a longtime follower of 2600. I first became aware of the zine in the mid 1990s and started to collect for a bit. I am not exactly a hacker, but have been close with a number of hacktivists for many years. I recently became chief editor of Anonymous's news website and admin of our Facebook page with over 10 million followers. I was wondering if you might be looking for writers and/or editors. Below you'll find links to my blogs and I have attached my resume. I hope this message finds you well and look forward to your response.

Anonymous

You actually signed a real name, which was yet another example of how this didn't seem too Anonymous-ish. Regardless of whether you're someone with no name at all or the duly elected King of Anonymous, if you write good articles, we will consider printing them. We hope you send us something.

Dear 2600:

I am in the process of setting up a website to sell hacking-related stickers, clothing, and loot. I was wondering if you sell wholesale and if you have stickers. If you don't have stickers, would you be interested in letting me sell them through the new site?

Let me know if you want a little more info or background. Thanks!

Cor

You certainly don't need us to sell stickers. In fact, with a free classified ad in the Marketplace, we can help you sell whatever you come up with through your own site. When we've had stickers in the past, we've usually given them away with orders of other stuff. If anyone is interested in designing something for that purpose, we'll certainly take it under consideration.

Dear 2600:

Random question - would you ever be interested in selling any of your web projects? I'd be interested in talking about <https://www.2600.com/> if you're open to the idea!

Do let me know.

Allie Floyd

Business Aquisition Specialist

You know what? Getting the "www" part of our site to work properly was a real project in itself. We'll sell that to you! (We actually took the time to send this response.)

Dear 2600:

I've enjoyed 2600 Magazine as an off and on print/digital subscriber and newsstand patron for about 15 years. I pride myself in reading the magazine cover-to-cover, but I have clearly been skipping over the Marketplace section. What's with all the letters from pedophiles requesting pen pals? I know the Marketplace has a disclaimer to contact these advertisers "at your own peril" and most readers should know better than to contact inmates without at least doing a quick search of their name, but why are these letters being published in the first place?

Thank you for reading.

Jeff Future

We don't do background checks on people submitting ads for the Marketplace, or anything else for that matter. As you mention, it's fairly trivial to look up those in prison to see what they were locked up for, and to then decide for yourself how to proceed. We don't believe prisoners lose the right to communicate with the outside world, regardless of what crimes they've committed. But we also believe people should exercise extreme caution whenever communicating with anyone they don't know - or when simply sharing personal info in social media.

Dear 2600:

I want to get my own story out (atmcrime.wordpress.com). There are a couple of mainstream news pieces on me and some clear bullshit like www.snopes.com/fact-check/reverse-pin-atm-alarm/.

Joe Zingher

The idea of having an emergency PIN to alert police to a robbery at an ATM is definitely an interesting concept, but we wonder how many people would remember it in a crisis or simply spell out something obvious like HELP, which robbers likely

wouldn't appreciate. We'd love to see an updated article on where this stands with new ideas or theories.

Dear 2600:

Howdy y'all nice persons. Been a bit since I dropped greetings in a message. I found the attached zine shelves you may find joy in seeing. Stay the way you do.

pic00



What time machine did you travel through to find this? Is there really a 1986 edition of our zine on a shelf somewhere? What a world this is sometimes.

Dear 2600:

Just following up on my email from the other day. Have you given any thought to selling <https://www.2600.com/>?

Do let me know what kind of price point you'd be looking for and I'd be happy to discuss it with you.

**Allie Floyd
Business Aquisition Specialist**

Well, the story seems to have changed since the last offer. You wanted to buy one of our web projects before. Now you want the whole site? That obviously is going to move the price point substantially. But it's not us you have to convince.... (We left it like that and haven't heard back as of press time. But, seeing as how they're in the business of acquisitions and can't even spell that word correctly, this is probably going nowhere fast.)

Dear 2600:

I am the writer of a blog about my journey into cybersecurity and ethical hacking as a 15 year IT professional.

I will be taking courses, reading books, attending events, and obviously purchasing the kit to use.

The site is [thesecuritynoob.com](https://www.thesecuritynoob.com) and, although new, has received an amazing initial response both in daily page views and responses on Reddit and other forums.

I will this week be setting up the Facebook page and turning my Twitter account (over 15k followers) and Instagram to being more focused on this and linking them to my site and LinkedIn.

I don't know if you have any sponsorship criteria or if you even do it at all, but I would love to get involved, if not now, then in the future for a subscription that I could read and post about on my site.

Please get back and let me know any information on how you work (even if at all).

The second post on my blog had already got me asked to guest blog on the site for the company who held the event The Techforce and I fully expect to see the grown of my blog grow exponentially the rest of 2019 and into 2020.

The site has been going great and has a few hundred unique visitors a day already.

Sorry for the seemingly random email, but I suppose if you don't ask then you don't get.

Alex

While what you're doing is pretty far from what we're doing (we think ethical hacking is a big scam and this all seems overly corporate to say the least - and what's with that "kit" that you're "obviously purchasing"?), we do have to acknowledge that you've got things organized pretty well and you're obviously dedicated to this pursuit. We have no problem sharing info about your project and we hope you have no problem subscribing to what we do. We'll leave it to our readers to decide for themselves if this is the kind of thing for them.

Permissions

Dear 2600:

I would like to share on my website articles from old versions of *2600 Magazine* that I purchased a long time ago, mainly for nostalgia purposes, but also to pique the curiosity of non-security IT people who are curious about the field of cybersecurity.

I cannot find the 2600 policy on if and when articles become free to distribute openly. Please advise.

George

This has never been an issue for us - the articles are meant to be shared. We just ask that the author is properly attributed and that info on us or a link to our site also be included. (We love that you refer to old editions as versions.)

Dear 2600:

I used to pick up your magazine whenever I could and enjoyed it when I did. I have started a new career in film and plan on shooting a short later this year or early next, and I was hoping to get permission from you to have your magazine in my film. The film is about a hacker who hacks corporate web servers to gain information on them to be a whistleblower. While he is cracking a site, he comes across an AI that has set up residence there and goes about manipulating him for its own means. I thought *2600* would be a good fit to have on his end table and thought you wouldn't mind the extra advertising. Also, any programs or graphics that you would recommend to be seen in the film would be appreciated. It is a flight of fantasy.

Christopher

This is also something we generally don't have a problem with. In fact, we have trouble with the concept of asking permission to have a product in a film to begin with. All we can suggest graphics-wise is to not go overboard or try to be flashy. That's never been what this scene has been about. As for

programs, whatever gets the job done and isn't glamorous is probably the best fit, if we're reading your tone correctly. Best of luck with this project! We hope to see many others.

Information

Dear 2600:

Have you heard about the 2020 presidential candidate's family that got detained at the Disneyland resort property in Anaheim, California for possession of marijuana on August 13, 2019 at approximately 9 pm in the Mickey and Friends parking area?

#bannedfromdisneyland

No, but it sounds like a great story. And that's a real fun hashtag.

Dear 2600:

I recently learned what may have been widely known already. The story of how this IPv6 assignment was determined would perhaps be of interest to your readers.

<https://whois.arin.net/rest/net/NET6-2600-1.html>

Was it a colossal coincidence? Or was there a considered choice involved?

dp

If you're referring to Sprint having the IPv6 assignment of "2600" and not us, we definitely were not a part of how that played out. We'll have our revenge when IPv9 is implemented.

Dear 2600:

I wanted to send in a note about the Tacoma Telephone Pioneer Museum. It's located in downtown Tacoma off of 9th Avenue at 757 Fawcett Avenue. Their hours are 8:00 am to 12:00 pm (only on Thursdays!).

Allow at least one hour for a tour of the museum. As noted above, they are only open one day a week for four hours! When we visited, there were three or four docents and each with a *lot* to say about phones and telecommunications history. Drink plenty of coffee before you arrive.

This museum opened in the fall of 1991 and was built from the collections and donations of former employees and AT&T. AT&T provided space on the first floor of the AT&T office building in Tacoma for the museum. The museum contains a variety of exhibits, including:

- Vintage telephones, many crank type old sets, both foreign and domestic.
- The first cordless telephone from the Seattle World's Fair held in 1962.
- An early video phone from the World's Fair.
- A wire chief's desk from the 1920s.
- A working 701A step-by-step PBX. It was donated by AT&T in The Dalles, Oregon. It is in good working condition.
- Several vintage teletype machines and related equipment all in working condition.
- A multitude of old pictures of employee groups, telephone buildings, old construction projects, etc.

- Many old manual switchboards, a long distance operator's board from the old Tacoma office, several old manual PBX boards including two local battery drop signal models.
- Toll test boards, a Morse board, and a primary board are equipped with a working Morse telegraph key and sounder. Two of our docents still were able to use the code.
- Old telephone directories, including some from the turn of the century.
- A working crossbar dial system.
- Two phone booths equipped with lights and telephone sets.
- A display of electronic tubes that were manufactured by the Western Electric Company.

If you are in the Puget Sound area or just visiting Tacoma, it is a must-see. It is a great little museum and provides a window into telecommunications and how it got that way. We were even given vintage glass insulators just for showing up!

Geoff

These museums are a great way to see old technology and learn some history. We know of similar setups in Seattle, Waltham (Massachusetts), and Ellsworth (Maine). We'd love to hear reviews from those places and learn of new ones. Thanks for sharing.

Dear 2600:

Please send snail mail address for donations to 2600 - I have no credit card!

Jim

That address is easily found on our various sites and in each of our issues, but we'll repeat it here: PO Box 752, Middle Island, NY 11953 USA.

Deceit

Dear 2600:

Can you please help me? Someone tricked me into sending them nudes and they are blackmailing and telling me that they'll share it everywhere if I don't pay them by today. If you're a hacker, can you please do anything to help? I'm begging you. I'm so desperate and I can pay you if you want. Here is his number on WhatsApp.

EM

This is definitely not something we need to get involved in. Of course, it's hard to imagine you expected to actually find someone within a single day to help you here. Even on a TV show, that's a bit of a reach. The only thing we can do that might be of help is to emphasize the point that when something is put or sent online, it's entirely possible that it will one day find its way elsewhere, whether through accident, incompetence, data breach, or just plain evil behavior. Of course, that doesn't do anything to help you, but there really isn't much that can be done when things reach this point. Perhaps if we lived in a world where people weren't shamed or otherwise abused when such things happened, it wouldn't be as much of a traumatic experience. The only other possible consolation is that all kinds of evil programs are being developed to create fake

images, both still and moving. Soon, it will become a real challenge to tell what's authentic and what isn't.

Dear 2600:

Hello!

I am a representative of the Chaos hacking group. In the period from 30/06/2019 to 24/09/2019, we gained access to your account tickets@2600.com by hacking one of the 2600.COM mail servers.

Have you changed your password yet? Good! But our program intercepts it every time. And every time I get your new password!

Linwood Scoggins

We're going to stop you right there since this goes on for quite a while and follows the familiar pattern of trying to scare someone into thinking they've been caught in a compromising position by someone who has their password (not very likely with the HOPE ticket department). Sometimes it's made more believable by actually revealing a password the person once used which can really scare the shit out of them if it's a password they're still using. (To avoid this, never use the same password on multiple systems - or for years at a time.) That password is often obtained by simply cross referencing a massive list of compromised passwords that have corresponding email addresses. It's important to note that the email address itself isn't necessarily compromised, but is usually a part of a throwaway pair used for anything from buying tickets to signing onto a Wi-Fi network. So if you were once asked to make a useless account somewhere with an email address and a password in order to get something quickly, the above letter may find its way to that address while quoting that password, thereby freaking you out if you remember the password. And then, of course, the next step is to extort money out of you by directing you to a bitcoin wallet with the promise that your "secret" will be safe if you pay up. It's always complete bullshit.

But you know all that. The only reason we even focused on this in the first place is because the letter was alleged to have come from the "Chaos hacking group." We thought it was funny. We don't know if our friends at the Chaos Computer Club feel the same way.

Dear 2600:

I found in my bank statement transactions from your website, but the fact is that I did not buy anything from you and never even visited your web store. The first 4 digits of my credit card 5931 I have detailed fax from the bank if you need it.

Edward

What's weird about this is that you're emailing an address that has nothing to do with our store. That, and your name doesn't match the name in your email address, which claims to be from Hungary. Despite that, this still concerned us greatly, as unauthorized charges from our store simply don't happen. We were really tempted to reply. And then....

Dear 2600:

I found in my bank statement transactions from your web store, but the fact is that I did not buy any-

thing from you and never even visited your online store. The first 4 digits of my credit card 5931 I have detailed fax from the bank if you need it.

Nathan

Now what are the odds? This time the email came from Finland and was sent to a completely different address and, again, the names didn't match in the sending address. The slight variance in the text is probably what fascinated us the most, though. Someone made a conscious decision at some point to change "website" to "web store" (or vice versa). But the real mystery is what the actual scam here is in the first place. There were no attachments, no links, and no requests to send along bank account information. We're curious if anyone has ever fallen for this one. We suspect that replying is what gets the scam going in earnest. So, if anyone is game, pal.matyas@tvnetwork.hu and nezir@hkcrusers.com probably have a lot to say.

Dear 2600:

I just wanted to take a moment to reach out to you in regards of your website 2600. If you are open to it, we'd love the chance to have you host an advertisement for our company.

Please let me know and I look forward to hearing back from you.

Erika Cao

Marketing Outreach Coordinator

One of these days, we should just take these people up on one of these offers and see what happens. The fun we could have if only we had more time....

Dear 2600:

This immediate assignment note/advisory alerts all media to the November 7 sealed-bid auction of Democracy.com through Heritage Auctions. Offered at auction for the first time in history, bids for this category-defining, one-word domain name must be submitted by 5 pm EST (New York, New York) on Thursday, November 7. The Democracy.com domain name will be owned by the highest bidder over \$300,000 (plus 15 percent buyer's premium).

At a moment when democracies worldwide are in crisis, who will own Democracy on the Internet?

DALLAS, Texas (November 4, 2019) - Democracy is in crisis across the globe and in the news every day. Hong Kong consumed by daily pro-democracy protests. Russians accused of tampering with U.S. elections. Britain in endless turmoil over Brexit. Impeachment proceedings in the United States Congress. A presidential election in 2020.

The Democracy.com domain carries enormous and unique significance in this moment in history as nations across the globe struggle to define what will happen to their democracies.

"As we watch democracy threatened worldwide, this auction is a unique chance to own what is perhaps the most important domain name of our time," said Paul Minshull, CTO of Heritage Auc-

tions. "We have seen interest from a number of nations already, with multiple bids placed. This will certainly be a one-of-a-kind auction."

"There are very few domain names of this caliber available on the Internet," Minshull continued. "Democracy.com is truly iconic - a single word that inspires the grandest of mankind's ideas and aspirations. Our hope is this domain finds a home with an individual or organization that has the resources and intentions to do something positive for democracy in their community, nation, or globally."

"The auction countdown for Democracy.com has begun for this once-in-a-lifetime opportunity," Minshull said.

"As an investment, one-word domain names such as Democracy.com present a rare opportunity to own an entire concept on the Internet with instant name recognition and credibility, and such category-defining one-word domains can attain significant value."

- * Voice.com sold for \$30 million in 2019.
- * Freedom.com sold for \$2 million in 2017.
- * Ice.com sold for \$3.5 million in 2018.
- * We.com sold for \$8 million in 2015.

The Internet's most popular auction-house website, HA.com, has over one million registered bidder-members and searchable free archives of four million past auction records with prices realized, descriptions, and enlargeable photos. Reproduction rights routinely granted to media for photo credit.

Interviews available:

Eric Bradley, Public Relations Director

Well, if this isn't a huge load of steaming shit, we honestly don't know what is. These are people who literally put a price on freedom and democracy, plus a whole lot of other words. What's crazy is that so many of us fall for it. What they all fail to realize is that it's not the words that matter; it's the idea behind whatever project is being launched. Google, Flickr, eBay, Paypal... those weren't even words before they became popular. It's highly annoying to see how much money is being thrown around, almost literally for nothing.

For the fun of it, we looked into how the sale of democracy.com went and it turns out it was actually bought by billionaire Mark Cuban who claimed to have no plans to actually use it and bought it simply "to make sure somebody didn't do something crazy with it." Too late.

Screwups

Dear 2600:

When I open 2600.com/phones and then on the newly opened page click on "Europe" on the map, I get sent to www.2600.com/phones/newindex.khtml?region=europe and, while everything works (besides the fact that the Bulgaria page says there are four photos but it shows only two), the Europe page shows the SQL query for the content:

```
No such region (europe) or query ( SELECT country.country, country.name, count(*) as pcount FROM country, payphone WHERE country.country = payphone.country AND country.region = GROUP BY country.country, country.name ORDER BY country.name) failed
```

IFo Hancroft

You're looking at an old page that we've forgotten about multiple times over the years. The proper link is 2600.com/payphones. We've finally disabled this antiquated page.

Dear 2600:

People have probably already emailed you about this, but it appears the SSL cert for 2600.com expired yesterday.

Thanks!

Brian

Did they ever. While we often bemoan the lack of authentic feedback and communication in the online world, it seems that all we have to do to open the floodgates is to make a mistake or overlook something. That's truly the best way to reestablish contact.

Dear 2600:

I can only find source code through 2017. Where is 2018-2019?

toby

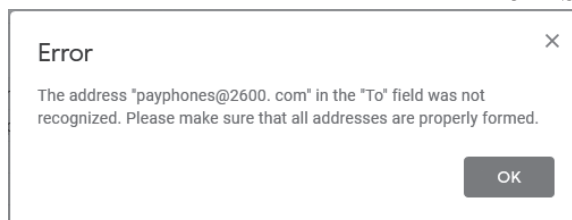
We fell short on this yet again. If it's not up by the time you read this, we will be very disappointed in ourselves.

Dear 2600:

I encountered the attached error when attempting to email you with a payphone photo today on my gmail account.

Not sure what is going on, but it is a valid address.

Jim St



To us, it looks like there's a space between the dot and the "com". We've uncovered many plots against us, but this doesn't appear to be one of them.

Dear 2600:

My article made it into the Winter 2017-2018 issue (34:4). It was "Nightmare on E-Street: Modem and Me Against the World." I read in the letters section of one of the next issues that there were lots of reader responses. ("We were blown away by the amount of responses this article generated.") I still really would like to read some of them and I am wondering if you have some sort of policy against that. I would really appreciate if you could let me know your position on this. I never found all the answers I needed and other input would be greatly appreciated. (My PC is now nonfunctional.)

Again, thanks for publishing it and the follow-up. I really enjoy 2600.

Also, you printed "Twitter the Enemy" by Michaleen Garda twice and back to back, however the second one is titled "Student Privacy by Practice - Not by Policy," yet it is the exact same article by Michaleen Garda. I imagine this has been pointed out to you multiple times, so I will be surprised if anyone reads this. On the other hand, due to the very small possibility that this was one of a few hard-copies of which there were few enough they could be culled, I would appreciate it if you sent me a corrected issue. I would like to read that article about student privacy as I am a student-worker. And no, I don't want the digital edition.

Emily S.

Speaking of lots of reader responses, this incident confirms that making a colossal mistake like this is one way to really get the keyboards typing in our direction. (The correct article replaces our staff section in this issue, so the only thing you're missing out on are our names, the music we listened to, and a clever quote.) Digital readers weren't affected by this.

As for the letters responding to your article, we believe we printed a good number of them over a few issues, and any specific suggestions on how to address your problem were shared here.

Dear 2600:

Dear awesome and amazingly informative 2600 - just a heads up on an article that is missing/duplicated. Page 29 ("Twitter the Enemy") of 36:3 (Autumn 2019) is also on page 31 but under a different title "Student Privacy by Practice - Not by Policy."

Thanks for being.

GH

We would never have gotten such a nice letter had we not screwed this up. We're learning.

Dear 2600:

The grandest of greetings!

Let's start this off right by my expressing my gratitude for all that you all do at 2600!

I am a long time reader that more recently subscribed. I have life experience confirming myself as, what one of my closest friends has termed, an extremist. I push envelopes quite invariably, and quite frequently due exclusively to there being any proposed limit at all. I also collect tools, so, therefore knowing that any tool can be used correctly or incorrectly, i.e., for good or for bad, I tend to prioritize seeking possession of those tools that are considered more "dangerous." It pleases me to have in my hot little hands a series of articles upon which, if utilized and interpreted correctly (or incorrectly as it may be), could result in my catching a felony case. I suppose my somewhat unique tendencies come from a few desirable results of being like this: I only attract fearless realists or deviant criminals which grants me a more meaningful existence and gives me yet another envelope to push. The

latter has been, as wisdom has proven, not worth the sacrifice because I am no deviant, truth be told.

Enough about that. I am writing because I read your latest issue's "assessments" and in the first letter under the "problems" section, a reader wrote of his last issue being misprinted. I also have a misprinted issue, it being the same volume as his. My Summer 2019 issue (36:2) also has a repeated section. It's the same misprint repeating pages 19 through 26 and picking back up at page 43. I felt a little incomplete when I read it, but decided not to bother you guys since I so appreciate what you do. But I would like to read the articles that are missing! Can you send me a copy? If you are as over-worked and underpaid as me, don't worry about it, but it would be nice.

Thanks and keep sending me tools!

(You may want to tell the fellow or lady that is responsible for binding your issues to lay off the sauce a little (just a little) when he/she is supposed to be concentrating on page sequences and print settings... unless it's automated, in which case you might want to have a look at the control of the machine or its components. Oh, you probably out-source the printing, huh? In that case, I have another issue that can fortify your case for cheaper rates!)

Steve

At least this screwup was completely at the hands of a machine. But it still resulted in some kind words for us. As for defective issues, forwarding them to us will result in an immediate replacement, plus something else for your trouble. Thanks for letting us know.

Dear 2600:

I imagine people have already emailed you but, if not, the Autumn 2019 edition had the same story printed on consecutive pages but with different headings, page 29-30 and 31-32.

On a separate note, can I still extend my subscription even if I have a few more issues to come? I just want to add two years and it says to indicate the issue I want to receive. My subscription isn't up until Spring of 2020, so I just don't want to wind up with double issues, for instance. I saw the note about adding subscription status in the comment section, but just wanted to do what is easiest for you guys.

Bill

If you write those instructions in the comment section of your order, it'll ensure that it's filled correctly. But you've given us an idea to add a new category to the issue choices for people who want to do what you're doing. Thanks!

Opening Minds

Dear 2600:

First off, thank you for printing 2600 for all these years, publishing two great collections (*Best of 2600* and *Dear Hacker*), and organizing HOPE. I just finished issue 36:2 and wanted to comment on a few articles and letters.

I felt overjoyed at your response to Walter's letter about silencing Trump supporters - both at your response and that you printed their letter at all. There is a lot of wrongness in it, but it would be wrong to "de-platform" Walter and his group, even though part of me would like to. See, I came to the U.S. over a decade ago and have met with kindness and generosity at every corner from all kinds of people, and I made this place my home. From my experience, the great majority of people, no matter which party they registered for, think along similar lines: safety, prosperity, respect, etc. I've come to realize that the people from the political fringe here are more similar to each other than to members of their own party. The fringe groups are OK with using violence, with taking away basic, inalienable rights ("it's not about free speech, it's about 'de-platforming'" - amazing doublethink), and with treating the other side as something less than human. I imagine if you put Walter in a dark room with someone from the alt-right, they'd get along perfectly fine until you turned on the lights. As you wrote, it's important to get more people into the conversation. Folks like Walter are doing what they can to keep people out of the conversation.

I enjoyed kyber's article about the magic of cloud. The problem he pointed out is not a technical one, but an organizational one. I consider it part of my job to engage with less technical parts of my company in order to make them aware of the benefits and limitations of using a specific technology. If they choose to ignore me, then I have to do the non-nerdy thing and build a relationship with them to avert disaster. If I'm not up for it or it can't be done, then I know I'm just a warm body and scapegoat, and I should get away from that company as soon as possible because it's a losing game. A junior developer knows how to write code. A senior developer should know why they're writing code and when to push back on stupid ideas.

Finally, some pushback to paulml's review of *Broad Band: The Untold Story of the Women Who Made the Internet*, which sets up a straw man: "The history of computers has always been thought to be full of men doing amazing things" - who has always thought that? Anyone who peels back the first, atom-thin layer of Silicon Valley pop culture and looks beyond Steve Jobs and Bill Gates quickly learns about all the wonderful women who contributed to this industry. Adele Goldberg and Diana Merry from Xerox PARC contributed immensely to developing Smalltalk (*Dealers of Lightning* by Michael Hiltzik). Radia Perlman created the Spanning Tree Protocol that pushed Ethernet networking into a new age. I could go on, but this information can be easily found in books about Silicon Valley, compsci, and gaming history or in magazines from the era. Anyone who's spent an afternoon studying this history wouldn't think that it "has always been thought to be full of men" - it's always been a joint effort of all kinds of people. I hope that it was an

accidental and not deliberate misrepresentation of computing history.

kingcoyote

Addressing your first point: yes, conversation and communication are vital and infinitely full of potential, but we need to be clear. There should be no tolerance for hate groups or those who make it a policy to dehumanize anyone. We never have and never will open those doors. There is a huge distinction between that and what you're talking about above, which continues to provide us with hope that we'll eventually get past all the divisiveness.

As for the book review, while history clearly shows the reality, we have to agree with the assertion that many people simply don't do that small amount of digging to learn the facts. This results in a distorted view, which is repeated over time, adapted into films and mini-series, and turned into reality for far too many. (It's even reflected in the title of the book.) At least now, we're having that conversation and moving into a more accurate representation.

Dear 2600:

I just finished reading 36:2 (Summer 2019) and a few things stood out to me. But first: I am a long time reader of 2600. I usually pick it up in a Books-A-Million in town. I have been interested in hacking ever since I was a youngster and my parents had an Apple II with BASIC on it. Lately, I've been building tube type stuff, guitar amps, radio receivers/transmitters, and other sundry items.

But this letter is not about that. It's about a growing trend. The trend to change the things that are normal. I am an American and I believe in freedom, not oppression. What I am seeing is the forced acceptance of abnormal behavior. For instance, the declaration that there are more than two genders. Not according to science there aren't. You could call yourself whatever you want - this is America (isn't it?). As a grown adult who is not harming anyone else, sure you are free to practice whatever weird religion, sexual deviance, or style of dress you feel like. But when you start telling me that I have to acknowledge your make-believe gender, or god, or whatever, you are infringing on my freedom.

Own your choices. If you choose to be a homosexual, own it. If I choose to be a hotdog-eating fat man, that's my choice, but can I really say I was born that way? I am, and have for as long as I remember been a proponent of the nurture over nature.

I enjoy the magazine, and I hope the freedom of thought presented in its pages will not just cover what is popular, but also what I wrote which I understand is not the current trend.

Ruikmuir

Where to begin. For those who think this isn't relevant to our pages, we're sorry, but it is (even though we don't know what specifically prompted this letter). We have some of the most freethinking

people on the planet who read these pages and we can't just let these words go unchallenged because it's not a specific tech problem. It affects the tech community (and every other), therefore it is most definitely a tech problem.

While much of what you say angers us, we feel it would be more productive to react with patience and try to explain why this way of treating people is so harmful and unhealthy.

You don't have a corner on the definition of normal. Just because we've lived a certain way for an amount of time doesn't make that way the correct one. Normal changes. We used to hear crap about how abnormal certain races or religions were. (Not surprisingly, we're seeing a resurgence of that as people continue peddling the belief that they're somehow under threat by others who aren't just like them.) Collectively, we're slowly moving in a more enlightened direction.

Nobody is telling you that you can't believe in whatever you want. And we seriously doubt you've ever had to live a single day without being acknowledged for who you are. Can you at least try to imagine what such a life must be like? Why is it so hard to extend that basic courtesy to others? To refer to people as "make-believe" or to imply that it's all a choice that could easily be changed is to make them less human and not worthy of respect, rights, or the ability to be honest to themselves. Or, as you say, not even to be acknowledged.

If there's anything that's inspired us in recent years, it's the courage shown by the transgender community, as well as so many others who've had to fight for their very identities. And to see people shine when they're comfortable with who they identify as is one of the best feelings there is. You may not like it, but this is the face of freedom and an inspiration for everyone.

Try that on for a while. Nobody is telling you that you're not real or that your identity is invalid. Yet there are so many who have lived entire lives that way. Isn't it time that we all get to be treated with the same respect and be offered the same opportunities?

We really hope you think this over.

Good Clean Fun

Dear 2600:

Have you tried tracerouting to bad.horse? It's really amazing. What is the story behind it anyway?

Anonymous

Yes, this is always good for laughs. You'll need to run the command ("tracert bad.horse" on UNIX variants, "tracert" for Windows, or use the Network Utility application on Macs. It doesn't always work perfectly since it's reliant on connections to a multitude of places at a single time. (The traceroute command, for those who don't know, shows the path between your machine and the one you're defining with every IP number and corresponding name displayed in an unfurling list.)

What follows is what you get when tracerouting

to the domain known as bad.horse (yes, .horse is a top level domain and 2600.horse is up and running). We left off the beginning to avoid giving out our internal addresses and also left off the connection times to avoid showing how bad our connectivity is.

10 bad.horse (162.252.205.130)

11 bad.horse (162.252.205.131)

12 bad.horse (162.252.205.132)

13 bad.horse (162.252.205.133)

14 he.rides.across.the.nation (162.252.205.134)

15 the.thoroughbred.of.sin (162.252.205.135)

16 he.got.the.application (162.252.205.136)

17 that.you.just.sent.in (162.252.205.137)

18 it.needs.evaluation (162.252.205.138)

19 so.let.the.games.begin (162.252.205.139)

20 a.heinous.crime (162.252.205.140)

21 a.show.of.force (162.252.205.141)

22 a.murder.would.be.nice.of.course (162.252.205.142)

23 bad.horse (162.252.205.143)

24 bad.horse (162.252.205.144)

25 bad.horse (162.252.205.145)

26 he-s.bad (162.252.205.146)

27 the.evill.league.of.evill (162.252.205.147)

28 is.watching.so.beware (162.252.205.148)

29 the.grade.that.you.receive (162.252.205.149)

30 will.be.your.last.we.swear (162.252.205.150)

31 so.make.the.bad.horse.gleeful (162.252.205.151)

32 or.he-ll.make.you.his.mare (162.252.205.152)

33 o_o (162.252.205.153)

34 you-re.saddled.up (162.252.205.154)

35 there-s.no.recourse (162.252.205.155)

36 it-s.hi-ho.silver (162.252.205.156)

37 signed.bad.horse (162.252.205.157)

So what is going on here? First off, these are the words to the "Bad Horse Chorus" from Dr. Horrible's Sing-Along Blog. (You'll just have to look that up if you don't know what it is.) The owner of this network simply had a bit of fun with some unallocated IPs, each using a "PTR record" which can use completely made up addresses. It's as simple as that. The Internet really can be a fun place if you let it.

Dear 2600:

Apologies, but I'm sending the attached image to both the letters email as well as the payphone gallery as I think it may apply to either.

My sister-in-law witnessed the scene; apparently youth interest in "old" technology is high these days. The next generation of phreaks is on the rise!

Uhrfo



And to think that these very same Canadian phones (Nortel Millenniums, to be precise) could have been used by phone phreaks way back in the 1990s, though not with red boxes, as those models didn't

use ACTS (Automated Coin Toll Service). But the method of swarming around the phones is virtually identical.

Going Digital

Dear 2600:

I'm in the U.K. and have been receiving my electronic 2600 Magazine via Amazon. Will this channel still be used?

Steve

Yes, the Kindle is very much a part of our electronic distribution system. This letter, incidentally, was in response to our introducing a new PDF version of the magazine as an experiment. It's too early to tell if the experiment was successful, as we need to add a bunch of new readers on that platform to help defray rising production costs on other platforms. But the results are encouraging so far.

Dear 2600:

I'm in. Don't always agree with your political positions but your voice is essential. Thank you and good luck.

Alex

If we can reach those people who aren't near a bookstore and who don't want paper editions, we think this could work out to everyone's advantage.

Dear 2600:

(1) It would be awesome to have a digital subscription option that covered these PDFs, rather than the yearly digests. Would definitely pay full price.

(2) An EPUB option would also be awesome!

Nathan

We only just now finished archiving our entire back catalog into digests. It was a tremendous amount of work, but everything is finally available digitally. We've also just introduced the PDF option for the current issue. If sales are strong, then we can put more resources into expanding that method of distribution, both for the future and the past. We love hearing ideas on what we should be doing, but the only way we can get there is through reader support, especially those readers who may not even know we're still around. This happens a lot when bookstores close and babies are born. So helping to get the word out is probably the best way to ensure that we have a chance to develop all of these platforms to their maximum potential.

Dear 2600:

Thank you for resending me the link to Volume 13. I now have all 35 digital volumes that you've published.

Thank you so much for making those digital copies available along with your printed volumes.

Please keep up the great work!

Ivan

You're more than welcome. We're thrilled that the entire collection is now available at last. It's a great solution for those who want everything, but don't want all of the paper that comes with that.

New Projects

Dear 2600:

Regarding your concentrationcamps.us project, you're doing the lord's work. Thank you.

Jacob

We don't usually get told that, but it's a refreshing change.

Dear 2600:

I'm currently working on a documentary of the concentration camps list, and wanted to let you know that the address for Yuma is incorrect. It should be 7125 Juan Sanchez Road. Thanks again for compiling this, and if you want to see some of the coverage I'm doing, check out my Twitter.

@Gillis57

It can be really confusing and time consuming to keep track of all of the facilities and addresses. What we had for Yuma (7125 East Cesar Chavez Boulevard) is what the Arizona Department of Corrections itself has listed. We'll try to confirm this.

Dear 2600:

Regarding concentrationcamps.us - next steps. Still stuck at finding the perfect logo for your brand?

Choose from the following logo options:

Anastasia Steele

Oh God, no. We're getting inundated with offers for concentration camp logos. Fortunately, none of them are at all relevant to the subject matter, but how long will it be before some AI figures out the perfect look for marketing this site?

Dear 2600:

I'm trying to think about the best way to long-term store and transport zines, especially 2600. I've done some research online, but haven't found anything that works as well as I would like for home collections. How is everyone else storing them?

Beaches

We would also like to know this. There have been some really clever solutions that we've seen in the past and perhaps it's time to showcase some of them. Please send us your pictures or descriptions of how you store your back issues. Extra points for those who include the early ones.

Dear 2600:

Hey! I love the magazine but more so the clothing! You guys at the office should crank out some new designs for us to pitch money at!

Jeremy

We do occasionally play around with new designs. But a little inspiration sure couldn't hurt. What kinds of things do readers want to see in their hacker garb?

Further Info

Dear 2600:

I found an article indicating that WBAI effectively went under and is now totally satellite-fed as if it were an iHeartMedia station.

What ends up happening with "Off The Hook" now? The radio landscape has been getting weird

where two of the local commercial stations close to me have been having outages. WWOW-AM simply went no-carrier silent this afternoon while WFUN-AM was transmitting an open unmodulated carrier Saturday night for almost an hour. I'm just curious what your options are as I know precious little about the New York-area radio scene.

Good luck and good hunting.

SMK

We doubt any of these events were related, other than the fact that radio is a very turbulent industry and that often the wrong buttons are pressed. In the case of WBAI, it was a hostile takeover by a rogue faction of the station's parent company, which was later overturned in court. So "Off The Hook" (at least at press time) is back in place. But that doesn't mean the station is out of the woods by any means. Operating a full power radio station in New York City without commercials is a daunting challenge, and it will take tremendous effort on the part of many people to keep this 60-year project alive in these times.

Dear 2600:

I have two topics. First is a question on beating facial recognition. As your magazine has reported, government uses your driver's license photo to match your face while they scan crowds of people. I've heard of people using face paints and other coverings to throw off facial recognition in public, but that doesn't work if I'd rather not look like a clown in public. So how can we hack the source data: the government's photo ID? Face paint is illegal for that photo, but it's not illegal for men to grow our facial hair in a similar pattern as face paints, like growing a checker pattern or something else crazy. Maybe you can even dye each checker patch a different color! So grow a beard, shave it into something ridiculous looking the day you renew your ID, get your ID photo, then shave it off immediately when you get home. Do any of your readers have data to confirm that getting a photo ID with a crazy facial hair pattern could defeat facial recognition when you're clean shaven? And what sort of hair patterns work best?

Secondly, responding to "Potential VPN Attacks," the writer is correct that default ISP equipment is a security risk, but not for what he thinks. Generally, ISPs don't employ good security. For example, my local ISP used the password "admin" for its admin, something I have found is true for many other ISPs as I travel with Airbnb. Even without that knowledge, Reaver was able to quickly crack my wireless password using the infamous WPS flaw. Although using your own secured hardware or reconfiguring your ISP's hardware can protect you from these hacks, it won't protect from the exploit the original article described. I live in a rural place where DSL is flaky. Sometimes it just resets due to too much moisture in the ground hurting the signal. Sometimes the phone line completely dies from a fallen tree. These situations cause the exact same

behavior this article described even using my own hardware. In other words, your ISP can reset your connection no matter what hardware you use and cause your VPN to drop.

If you want to prevent apps from connecting to anything but VPN, then you need something that completely blocks any unwanted connections from exiting the non-VPN route. Here is what I do with Tor on Linux. I run Privoxy under user ID "proxy" and have iptables rules preventing that user from connecting to anything except tor localhost port 9050 (Tor). Then I have a user ID called anonymous that is similarly restricted to connecting only to Tor or localhost port 8118 (Privoxy). Lastly, it logs any dropped connections, which can help me identify if an app is going rogue trying to get outside my Tor sandbox. Now if I am running anything under the anonymous user ID, I can be reasonably assured it is not leaking any data outside of Tor. The config is below. It should be easily adaptable to restrict certain logins to your VPN interface device (-i parameter) rather than certain ports like Tor.

```
Chain OUTPUT (policy ACCEPT)
Target prot opt source destination
ACCEPT tcp -- localhost localhost
↳ owner UID match
anonymous tcp dpt:9050
ACCEPT tcp -- localhost localhost
↳ owner UID match
anonymous tcp dpt:8118
LOG all -- anywhere anywhere
↳ owner UID match
anonymous LOG level warning prefix
↳ "IPTables-Dropped"
REJECT all -- anywhere anywhere
↳ owner UID match
anonymous reject-with icmp-port-
↳ unreachable
ACCEPT tcp -- localhost anywhere
↳ owner UID match proxy
tcp dpt:9050
LOG all -- anywhere anywhere owner UID
↳ match proxy
LOG level warning prefix
↳ "IPTables-Dropped"
REJECT all -- anywhere anywhere
↳ owner UID match proxy
reject-with icmp-port-unreachable
```

David

We believe it is well within everyone's rights to fool tracking devices of any sort and to defeat facial recognition. We're extremely interested in methods of doing this. Of course, so are the trackers, so this must be a constantly evolving topic. We would love to learn more and hope to print detailed articles on the subject.

Dear 2600:

I really enjoyed "The Telecom Informer" column in the Autumn 2019 issue. There has been growing awareness and interest in how incarcerated persons are forced to pay exorbitant prices for services and content that would be free, or much cheaper, outside of the prison environment. The column is an excellent addition to this awareness.

As the article mentions, many or most pris-

ons prohibit possession of cell phones. They are very restrictive about, or prohibit, prisoners from having e-readers, tablets, computers, etc. Locked-down central systems may be usable for email, but at exorbitant rates and requiring recipients outside of the prisons to first set up their own accounts and agree to monitoring.

Free content, notably Project Gutenberg (who got a shout out in the same issue), incurs access charges. In an expose in 2017, *The Philadelphia Inquirer* found that Pennsylvania prisoners were paying well above retail price for contemporary eBooks, as well as per-item charges for free books from Project Gutenberg. Indications are that GTL (Global Tel Link) has now shifted to per-minute fees to access free or non-free content instead.

Prisoners are among the most disempowered and disenfranchised of all people in our society. Those lucky enough to have family or friends outside of prison are reliant upon them to shoulder the costs. Others must work at near slave-labor wages in the prison system, or they must simply do without. The ability to communicate freely, and to have access to the tools of literacy and education, are fundamental rights for people outside of prisons in the U.S. Within prisons, though, such rights are removed, taxed, or restricted.

Below is what the Wisconsin prison system sends someone when a prisoner attempts to reach them by email:

*From: CorrLinks <info@corrlinks.com>
To: nonesuch@2600.com
Subject: Offender: DOE, JOHN*

This is a system generated message informing you that the above-named person is a WIDOC prisoner who seeks to add you to his/her contact list for exchanging electronic messages. There is no message from the prisoner at this time.

You can ACCEPT this prisoner's request or BLOCK this individual or all WIDOC prisoners from contacting you via electronic messaging at www.corrlinks.com. To register with CorrLinks you must enter the email address that received this notice along with the identification code below.

*Email Address: nonesuch@2600.com
Identification Code: 17KIBAN9*

This identification code will expire in 10 days.

By approving electronic correspondence with WIDOC prisoners, you consent to have the WIDOC staff monitor the content of all electronic messages exchanged.

Once you have registered with CorrLinks and approved the prisoner for correspondence, the prisoner will be notified electronically.

Estragon

Another very disturbing trend we've noticed in prisons today is elimination of in-person visits, to be replaced with "video visits," which charge people up to \$1.50 a minute for a Skype-like con-

nection to their friend/relative behind bars. And, in some cases, they still have to travel to the prison to make use of the service! This increasing dehumanization is an insult to everyone involved.

Dear 2600:

Amateur radio transmissions are not allowed to be encrypted by any means. This doesn't mean that you cannot use a digital mode, just that anyone wanting to receive the transmission should be able to decode the digital mode. Essentially, if you want to use a digital mode, the particulars of the mode must have been published. There is an exception for transmissions used to *control* satellites. When using a satellite to communicate, the transmission must also be in the clear or a published digital mode. Note: add analog mode as well, I forgot about slow scan TV.

I'd give you my call sign, but that would be identifying information.

E85

Indeed it would be. But we do want to know more about using amateur radio transmissions to control satellites.

Danger

Dear 2600:

I was wondering what you thought of this story about a Japanese stalker who found out where a celebrity lived through Google Street View. "Following his arrest later that month, he told police he was a big fan of the woman, who was described as a 21-year-old "Japanese idol" in local media reports. The suspect told police that after zooming in on the image of her eyes, he used Google Street View to identify the [train] station. He also said he had studied videos the woman shot in her apartment, looking at details such as the placement of curtains and the direction of natural light coming through the window to try to determine exactly which floor she lived on, reports said."

Paul

This is both creepy and frightening. There are steps we can all take to preserve our privacy, such as making sure all location data is disabled whenever we post photos online or being extremely careful not to reveal personally identifiable information in our social media posts. But when companies like Google or Facebook delight in revealing as much personal data as they possibly can, they become the ultimate stalking tool. In this case, perhaps nothing could have stopped this person with his determination and skill level. But the big data aggregators of the world need to understand that the information they peddle is a whole lot more than bits and bytes. It represents our actual lives and we clearly need to be able to have more control over how (or whether) it's used.

Dear 2600:

Regarding your broken toys... WBAI was just the beginning.

Daffio International

Well, isn't that nice? A dark promise of doom in the future. We hate to disappoint, but the radio station is back on the air. In fact, so many times when things seem to be at their worst, we see an outpouring of support that not only helps, but actually makes things better than they were. It's the power of community and people who care. You might want to try that sometime instead of reveling in destruction.

Dear 2600:

Why is Facebook suggesting that I update legacy contact? Is it just me or something? Don't tell me Zuck knows exactly when I'm gonna die.

J

If you think social media is weird now, just wait until it spans generations and/or lifetimes. But it's probably more realistic for us to be the ones asking Facebook how they want to be remembered when they're gone.

Inquiries

Dear 2600:

I have previously given a talk about "hunting for phish kits" but I have not written an article about the topic. It would be loosely related to the talk I gave, but not directly. Would this fit within your guidelines?

Josh

It most certainly would, providing the talk itself is something of interest to the community.

Dear 2600:

I'm an actor based in New York City. I am looking for an experienced computer tech who can build my actor website for me to showcase my talents. I wanted to put an ad in your online magazine classified, but see no opportunity to do that. I realize creating a website can be very expensive. I am offering one year of free music lessons in exchange for building my actor website. I've been playing the saxophone for 47 years and private teaching instruments for 21 years. I can also teach clarinet, flute, or beginner piano. Can you offer any advice or suggestions?

Fred

OK, a couple of things. When you refer to our "online magazine," it would be helpful to know how precisely you're reading us. Are you reading the digest, a Kindle version, or a PDF edition? Each is slightly different insofar as how the Marketplace is presented. But you should still see info on how to submit an ad. If you're an electronic subscriber, just email us at marketplace@2600.com with a receipt that shows you're a subscriber. For paper readers, either your address label or a receipt will do. We hope that helps.

Dear 2600:

Any plans to make more blue box hoodies? Please!?! All the best to the 2600 crew.

Christopher

They should be in stock now. That's the power of "please."

Dear 2600:

Why, in the name of all that is holy, do you link to Facebook on your web page?

Facebook! Yeesh.

Michael

Let's just calm down a bit here. We didn't invent Facebook and we have a great deal to say about how it invades our privacy, closes people's minds, and is dumbing down our society. But we also have to come to terms with the fact that lots of people use it and lots of people in the hacking community are a part of that. Pretending they're not there isn't going to solve anything. But connecting to one of our Facebook groups (we have three now!) may introduce you to some intelligent thought on that platform. It's certainly worth a try.

Dear 2600:

Are there license restrictions for articles published in 2600? In other words, can I submit an article to 2600 that I have already had published in another publication, provided they don't have any license restrictions?

Ryan

We prefer for anything we publish to not be available elsewhere before we print it. Of course, if it was in a publication that was super obscure or in a different language, then the odds of our readers having already come upon it are pretty slim. The same goes for posting it on a blog if only a handful of people have seen it. What we don't want to do is have recycled material. If you think we got a strong reaction to printing the same article twice in a single issue, you'd better believe we'd get an even stronger one for reprinting material that's easily found elsewhere. And we probably wouldn't get the nice comments that we're getting now.

Also, once your article appears in our pages, you're free to do whatever you want with it.

Dear 2600:

We're updating our records and would like to confirm if your site accepts vendor-neutral, non-promotional contributed articles? If so, can you let me know the process to submit an article?

**Tim Mochin
Intern**

Tim, what you're describing here are articles which, by default, have nothing to do with vendors or promotions. We're not sure why a marketing company like the one you work at would be at all interested in such a thing, but that's pretty much what we specialize in. If you're truly interested in submitting articles, you simply email them to articles@2600.com or physically mail them to PO Box 99, Middle Island, NY 11953 USA. If we use it, you get a subscription and a shirt! Put that in your records.

EFFecting Digital Freedom

It's Time to End Stalkerware

by Jason Kelley

Someone with unfettered access to our phones or computers essentially has unfettered access to our lives. For many, computers and phones contain not only private information, but the contents of our very thoughts. We text our friends and family and partners our feelings, we take notes, we talk about plans; and this is on top of data about where we travel, websites we visit, and who we're talking to. That's why we absolutely must put an end to stalkerware.

Stalkerware, also known as spouseware, is software that is installed covertly on a user's phone to collect and share information with another person without that user's knowledge - essentially, to digitally stalk someone. By sharing personal details about who someone has called or texted, pictures they've taken, where they've traveled, or even what they have discussed in private conversations, apps like these let abusers menace and torment their victims. This technology is often used for domestic violence against spouses, children, and exes. The people who end up with this software on their phones can become victims of physical abuse - and worse. By design, these apps are secretive, and even if users suspect that they might exist on their device, it's often difficult to know how to take action or how to protect themselves.

For years, stalkerware has often been ignored by many anti-virus (AV) companies and malware scanning tools. App stores like Apple's have allowed the software, which is often advertised as a way to monitor a child or an employee. But in practice, it's nearly impossible for an app developer to establish or monitor its users' relationships to their targets, or to ensure that they will use the app how they say they will. A product designed for covertly monitoring children's activity could just as easily be installed on a partner's phone. There are simply no legitimate purposes for secret stalking apps.

But we're fighting back. A new coalition of anti-virus companies and human rights groups, including EFF, have joined together to create the Coalition Against Stalkerware, which will work to address the use of stalkerware and raise

awareness of it, provide help for victims, and bring leaders in AV together to establish best practices for ethical software development. The coalition also provides online resources and help for stalkerware victims at stopstalkerware.org.

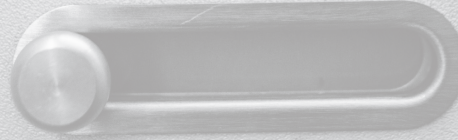
AV companies have already gotten the message. Several, including Kaspersky and Malwarebytes, have improved their flagging of stalkerware, and the FTC took action against stalkerware developer Retina-X (albeit for poor security, leaving open the unfortunate possibility that Retina-X could continue to offer its software in the future).

This flurry of activity is thanks in part to EFF's director of cybersecurity, Eva Galperin. In 2018 she offered assistance on Twitter to any woman who was sexually abused by a hacker who threatened to compromise their devices, and when hundreds responded, she began working to help - and she began to fight the problem on a larger scale by pushing anti-virus companies to flag the malicious software. Her work and the work of survivor groups has propelled the battle into the limelight, and helped to begin the dismantling of the industry.

It won't be an easy fight. According to Kaspersky, the number of its antivirus users finding stalkerware on their devices rose by 35 percent in 2019, up to 37,532 from 27,798 in 2018. The varieties of stalkerware have increased as well, with Kaspersky detecting 380 various forms of it in the wild in 2019 - 31 percent more than a year ago. But all of this work has already made an impact. The coalition wouldn't have been possible a year ago, and a year from now, with the group working together to protect people from stalkerware and hold vendors and abusers accountable, we're that much closer to eradicating this entire industry.

There is simply no acceptable use case for running a consumer spying app covertly on someone's device. Having access to someone's phone is akin to having access to their mind, and no one should be able to peer into your mind without your consent: not the government, not a company, and not an abuser. It's time to end the development and sale of these privacy violating tools.

Maximizing Privacy in a Digital World



by Terry Clark II

With the proliferation of personal computing devices, explosion in social media, and increase in number of people connected to the Internet, privacy is now more important than ever. From unscrupulous individuals looking to steal your credit card data to companies like Facebook and Amazon looking to track you to make money off that data, the average user is under a constant barrage of technologies that slowly chip away privacy. How does one defend against these invasions of privacy? Technologists often joke that there is no privacy on the Internet and, to an extent, this is true. However, there are some things that can be done to increase privacy.

This article will examine three levels of privacy enhancement. The first are low effort solutions that require little to no change in computer usage habits and have minimal, if any, cost associated with implementation. Next, we will cover intermediate modifications that may require some technical knowledge to implement, may result in mild inconveniences when using the computer, and may cost a bit more to implement. The final section will touch on some advanced privacy methods that may require a significant change in browsing habits or incur significant costs to set up.

Level 1: Basic Privacy Modifications

As mentioned, the basic modifications will require little technical knowledge and be cheap or free to implement. Included under this umbrella are password generators, two factor authentication, ad blockers, and increasing the restrictiveness of social media settings.

Password generators automatically create a unique password for each website or service used and protect these passwords with a master password. As a result, the user only needs to remember a single password while reducing the risk of attackers being able to break into multiple accounts due to duplicate pass-

words. There are two big players in the area of password managers. These are LastPass and KeePass.

The main difference between the two is ease of use for non-technical users and cost. KeePass requires manual configuration that takes several steps to get everything up and running. Additionally, KeePass does not automatically synchronize passwords between devices without further configuration. LastPass does not require these extra steps, but has a cost associated with some of the premium features, such as multi-factor authentication, support for third party applications, and encrypted storage for files. According to an article from LiquidVPN, “If you are ready to finally secure your passwords and the thought of entering API codes and changing some settings in XML files is new jargon to you then LastPass Pro with two-factor authentication is the tool for you. Otherwise, go with KeePass.” (“Which Password Manager,” 2017) The main reason for this is that LastPass stores the passwords in an encrypted cloud. While this is probably safe enough, some people may be paranoid about any usage of cloud solutions and may wish to have their data stored on their own devices instead, a feature offered by KeePass.

Like password generators, two factor authentication increases security by requiring access to another device, usually the user’s cell phone to fully authenticate to an account. A possible other method of verifying identity via 2FA is using biometrics. However, “biometrics still has a long way to go before it can be considered a rock-solid security technique.” (Gillin, 2018) Current biometric techniques can either be fooled relatively easily or are not 100 percent accurate, necessitating the need for backup authentication methods. This obviously defeats the point of using biometrics in the first place.

Both ad blockers and more restrictive social media settings attempt to limit tracking and potential exposure of information to the general

public. There have been cases of websites both tracking users through ads and tracking users between sites to serve them personalized ads. (Dangerfield, 2018) By utilizing ad blockers and turning off targeted Facebook ads, this tracking is decreased. Additionally, by putting in place social media settings that only allow friends to see the details of our profile, we decreased the ability for random strangers to scrape information from this source.

Level 2: Intermediate Modifications

Beyond the basics presented in Level 1, there are some additional things users can do to increase privacy without much more loss of functionality. These include changing the default search engine, private browsing modes, using a VPN, and using a Tor browser. Except for the VPN, all these options are free. Even the VPN option could be free, depending on what the user's exact goal is when implementing this technique.

Most users likely have Google set as their default search provider. While this is convenient because of Google's search algorithms and potential integration of search history across devices, it is no secret that Google tracks searches by user. This is part of what makes the targeted ads in Part One work. For instance, have you ever searched for some obscure product and immediately started seeing ads on other platforms for that thing? That's Google tracking at work. By switching to another search provider such as DuckDuckGo or Startpage, this tracking is minimized.

To take this idea a step further, the user could choose to use private browsing mode. This will automatically delete browsing history, cookies, and all information that has been typed into online forms when the browser window is closed. This is useful to prevent cookies from tracking a user between sessions. However, by doing so the user will lose some functionality such as the ability to put things in their cart on a shopping website and return later to purchase those items. Because cookies are not being stored between sessions, the cart information will be erased when the browser is closed. Additionally, information about the user's computer and browsing habits are still accessible by websites being visited and any network administrators that may have access to the connection, including employers and ISPs.

To take this concept a step further and start to anonymize the data sent to websites while also minimizing the tracking ability of employers and ISPs, the user may choose to set up a VPN service. There are really two choices here. The user can choose a publicly or privately hosted VPN. The privately hosted VPN is essentially a VPN set up by the user themselves at their home. While this will not do much to hide their browsing habits from the ISP, this solution can be useful if the user knows they will use insecure Wi-Fi connections such as in coffee shops. Having the home VPN set up will add a layer of security such that a malicious person in the coffee shop cannot simply sniff all traffic originating from that user. As pointed out in an article by *PC Mag*, "Just because it's called Starbucks_WiFi doesn't mean it's really owned by a well-known coffee purveyor."

The publicly hosted VPN is, theoretically, more useful. These VPNs allow all traffic to be encrypted, even when the user is home. Additionally, when the user connects to a website, their IP address is hidden from that server and instead appears to be the endpoint of the VPN. This tunneling functionality, which is the heart of a VPN (Park, 2017), allows a user to mask browsing information from their ISP. The ISP *will* be able to tell that a VPN is in use but will be unable to see the traffic flowing back and forth in that VPN tunnel.

However, this is not to say that one should simply hop online and enroll in the first VPN service they come across. There have been some cases in which the VPN provider has either turned over customer data to law enforcement or allowed customer data stored on their servers to leak publicly. Obviously, the user should research their VPN provider regarding these issues if they feel this is necessary.

To get around these potential limitations of VPNs, a user may choose to use a Tor browser. These are browsers that are designed to use the Tor protocol (previously The Onion Router) in which traffic is encrypted and then routed between multiple hosts (at least three by default) before coming out the other end. (Mason, 2018) This makes it more difficult to backtrack through the routing protocol as might happen with a VPN. Additionally, because Tor nodes are operated by volunteers, there is no centralized business that a law enforcement

agency can target for customer records. There are various best practices that can be used with Tor for very paranoid users, but most users will be happy with the anonymity provided by the base package.

Level 3: Advanced Modifications

For the more technically savvy and/or paranoid users, a third category exists which may require significant effort to configure or significant modifications in computer use habits. The options covered in this level include using virtual machines to sandbox computing tasks and use of privacy-focused live boot operating systems.

The use of virtual machines has long been of interest to those involved with information technology and information security. With the advances in modern hardware, it is feasible to do all computing within a virtual machine, or to run multiple virtual machines at the same time for different tasks. Additionally, virtual machines are often used in malware analysis as a way of isolating known or suspected contaminated files from the root system. The malware is executed within a virtual environment, studied, and the virtual environment is then deleted, taking all trace of the malware with it.

On top of being used for malware analysis, virtual machines are being used to hide the existence of files. In a paper from the 17th International Conference on Computational Science and Engineering, a way of utilizing virtual machines in this way was presented. Essentially, the files are encrypted and then placed within what is known as a deniable file system. This effectively hides the existence of encrypted files altogether. The issue, as presented in the paper, is that some applications, such as Microsoft Word, may not be designed with this goal in mind. As a result, the application may inadvertently leak information about the hidden file. To get around this, the paper introduces a concept known as Shadow Execution Environment which uses virtual environments to prevent this data leakage. (Wen, Fang, Zhao, and Li, 2014)

Using privacy focused operating systems, users can further hide their tracks. For full effectiveness, users should use these operating systems in a live boot environment. While this means that users will typically lose their data when the system is rebooted, it is the

most secure way of utilizing these systems. Additionally, use of these OSEs can increase the effectiveness of the Tor browsers covered earlier. Along with some of the other best practices, the user can achieve quite a high degree of privacy and anonymity. (Hampton, 2013)

However, much like the VPN solutions presented earlier, privacy focused OSEs such as Tails offer no guarantees of privacy. Much of the effectiveness comes down to user behavior and situational awareness. For instance, these OSEs cannot always protect against compromised hardware, BIOS attacks, or man-in-the-middle attacks. Additionally, anyone who knows how to read network communication will almost certainly be aware that you are using Tor and potentially even that you are using one of these OSEs. (“Warning”, n.d.) However, if the best practices are followed and everything is configured properly, these solutions will be more than adequate for the average user. The only people that would even really need to worry about this level of detail are those targeted by advanced persistent threats such as nation-states of other government backed intelligence agencies.

Conclusion

As should be clear by now, there are many options for attempting to ensure one’s privacy on the Internet. These range from relatively easy to implement and cheap or even free to requiring advanced technical knowledge and potentially significant investments. However, as mentioned at the beginning, true privacy on the Internet is almost unachievable if the attacker has enough resources and tries hard enough. While an acceptable degree of privacy can be achieved by the average user, true privacy is only possible by avoiding the Internet altogether.

Given that most people will not want to live a life without Internet access, each user must perform their own assessment of how much privacy they are willing to give up for the different services. As a final note, some of these products *are* commercial offerings. While in a perfect world, we could just trust people, some companies tend to stretch the truth in their product marketing materials. Always keep a hint of skepticism if someone makes a claim that seems outlandish and always do your own research.

Do-It-Yourself Cloudflare on a Budget

by aestetix

As the American political landscape gets ever more heated and divisive, many tech companies are throwing their hat in the ring and treating customers differently based on their political views. I think this is an incredibly stupid move for a company, regardless of whether or not I agree with the company's politics, because I believe companies should only be focusing on their products. It makes me ask questions like: "could a company ever drop my account over politics?" Because such questions scare me, I often seek to figure out ways to replicate what the company does on my own and, if possible, for free. In this article we'll explore one such example that could also wind up saving you some cash in the long term.

A well known company that has recently made decisions based on political views is Cloudflare. Their technical offerings are twofold: they offer website caching via a global content distribution network that can make your website much faster, and they offer protection against distributed denial of service (DDoS) attacks. While the caching offering is useful especially if you want to boost your site in search results, the DDoS protection is actually pretty easy to replicate on your own, provided you don't need deep packet inspection performed, which most sites don't. When you add to this the fact that all of your DNS records must be hosted with Cloudflare to use their service, a less intrusive alternative that can handle some forms of DDoS mitigation for free sounds fairly appealing.

There are several kinds of DDoS attack. While some aim at knocking a service or website completely offline, others are more focused. A very common form of DDoS, and what we'll focus on here, comes not from trying to get the site shut down, but from attempting to brute force a login without getting banned. While setting a CAPTCHA

for an IP after too many failed login attempts is helpful, it still allows traffic to reach your web servers and cause undue stress on your system's CPU. It's far better to have a way to automatically cut off offending traffic before it even hits your web servers.

One of the best free tools to protect against a DDoS on Linux is called Fail2Ban. This tool runs as a service, monitors your logs, and modifies your firewall according to the rules you set. Therefore, you can configure it to protect against a simple DDoS in a few easy steps. From this point on, I'm assuming you are running Ubuntu 18.04, but these steps can easily be translated to other Linux flavors.

Fail2Ban provides a number of security features out of the box, such as protection against ssh brute force attacks. To mitigate these, Fail2Ban scans the access log (usually `/var/log/auth.log`) and, if it sees an IP attempt unsuccessfully try to connect to the system via ssh (port 22) too many times, it will ban that IP in iptables for a set period of time. But since our focus is web traffic, let's take a look at a log entry and convert it into a Fail2Ban rule. For our example we are using the load balancer HAProxy, but you could easily translate these steps to Nginx (or Apache).

First, make sure Fail2Ban is installed:

```
apt-get install fail2ban
```

Next, we look for an offending traffic pattern. After a glance at the HAProxy log (`/var/log/haproxy.log`), we see a bunch of lines that look like this:

```
Oct 21 07:28:00 localhost
➔ haproxy[2342]: 192.168.0.1:
➔1337
[21/Oct/2015:07:28:31.337] https
➔_frontend~ wp_backend/wp 0/0/5/
➔287/750 200 34854
- - ---- 384/384/213/0/0 0/0
➔ "POST /wp-admin.php HTTP/1.1"
```

It looks like some attacker is trying to access our Wordpress admin login form. Not

cool! Let's go ahead and set up an automated way to ban them. First, we want to craft a regular expression (regex) that matches the line in the log, but won't hit a false positive. If you're new to regular expressions, you can use the "fail2ban-regex" tool (included when you install Fail2Ban) to test your regex against the logs in question after you've set up the filter.

Now that we've crafted a regex to match the offending line, let's create a filter for Fail2Ban. Create the following file and add this code to it:

```
(contents of /etc/fail2ban/filter
➤.d/haproxy.conf)
[Definition]

failregex = ^.*haproxy\[([0-9]+\)\]
➤: <HOST>.* "(GET |POST )/wp-
➤admin.php HTTP/1.1"$

ignoreregex =
```

This filter definition file contains the fail-regex variable, where we define the regex Fail2Ban will use to remove and block offending IP addresses. The two important parts are the HOST variable, where it grabs the IP address, and the path part, where it makes sure the offender is indeed trying to log in. Once a request matches this regex and an IP address is logged, it then gets parsed by the jail config, so we need to enable it by adding the following to the end of the jail config file:

```
(entry in /etc/fail2ban/jail.
➤conf)
[haproxy-login]
enabled = true
```

```
bantime = 4800
findtime = 120
maxretry = 5
filter = haproxy
logpath = /var/log/haproxy.log
port = http,https
ignoreip =
```

There are a few important variables to set here. First, the logpath should correspond to where the log Fail2Ban needs to scan exists. If you're using Nginx instead, the logpath should probably be something like "/var/log/nginx/access.log". The port in our case is standard (80,443), but if you're using a non-standard point, you'll have to modify this accordingly. The filter value should correspond to the filter we just created. Finally, the bantime, findtime, and maxretry variables need to be set. In plain English, our config is set so that if an attacker attempts to log in more than five times in 120 seconds (two minutes), their IP will be banned at the firewall level for 4800 seconds. After the bantime has passed, the IP address will be unblocked from iptables and allowed access again. That said, if you plan on using this in a system that you use frequently, you should probably add your IP address to the "ignoreip" variable to make sure you don't accidentally ban yourself from your own server.

In conclusion, while this trick isn't fool-proof especially against major actors, for the average person it works pretty well and can save us a bit of money, as well as peace of mind that the service we're paying for won't randomly drop our account.

BOOK REVIEW

Artificial Intelligence: A Very Short Introduction,

Margaret A Boden, Oxford University Press, 2018, ISBN 9780199602919

Review by paulml

Many advances in artificial intelligence have been made over the past several years, starting with Siri and Alexa, but much more remains to be done. This book gives the details.

The science of AI involves many other sciences, including neurophysiology, logic, and psychology. A major challenge is how to present a problem, or a question, to a computer in a way that the computer will understand. Another challenge is how to show a computer things like emotion and creativity. What is

consciousness? Is intelligence more than just IQ or the Turing test?

Robot designers have had better luck creating robots that resemble insects with six or eight legs than in creating robots that look human with two legs. When is the singularity coming? When is Skynet coming? The general answer from this book is: not anytime soon.

This is a very well done introduction to the world of artificial intelligence. Some of it gets rather technical, but most of it is good for the general reader. It is very much recommended for anyone who wants to learn more about AI.

CITIZEN ENGINEER

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

Demystifying and Designing for USB-C

If you're like us and have been creating or working with computers over the decades, you have a box somewhere in your home with adapters of all sorts. Null modem cables, VGA gender changers, DVI to HDMI converters. The medium-low protocols like ADB, PS/2, parallel, and serial all got merged into the USB (Universal Serial Bus) standard. Starting with version 1.0 that was for mice and keyboards, it was then expanded up to 2.0 for disk drives and cameras. Engineers at this point bumped up against some physical properties of USB - it was only two data pins and power maxed out at 5V 1A (technically, you weren't supposed to draw more than 0.5A, but most folks ignored that recommendation).

At that point, disk drives, video cameras, and networking devices needed faster data transfer and more power. So USB 3.0 came out with really unusual connectors that extended the data and power capability. This is when everyone making devices threw up their hands and said, “Look, we've got all this technical debt that we've built up over the years - too slow, confusing connectors, low power, OTG incompatibilities, weird mutant connectors.... Let's try to design something to one standard connector that you can't connect wrong.”

They... sorta... succeeded. But, there's still plenty of gotchas that are literally hidden inside the cable! Now with USB-C, the cable always plugs in, both ends are identical and reversible, but there are at least six different types of USB-C cables. Designing electronics for USB-C is a lot more complex than the classic USB with only four pins, all well defined.

All USB-C connectors use a standard 24 pin oval connector. Four are ground, four are power, there are the classic USB data connector pairs D+/D-, as well as four more differential data pairs (five data pairs total), and then four more pins for configuration and non-data-sideband usage. Since there's still millions of computers with classic USB connectors, the USB-C standard is a simple super-set that can be used for USB by only connecting the power/ground/D+/D- wires. If you have USB

3.x, those pins can also be connected to the USB-C with a mechanical adapter.

Thanks to the four sets of power pins and four extra differential pairs, USB-C cables can handle high-power/current and high-data transfer uses such as device charging, monitor/laptop power, up to 40 Gbps data (aka Thunderbolt 3), or any audio/video standards like HDMI/DisplayPort/Mobile High-Def. For power usage, cables can carry 20V 3A and, in some cases, 20V/5A.

But... that's just what USB-C is specified to support. Whether you can actually use a USB-C cable for these purposes depends a lot on who made the cable and how much you're willing to spend. After all, to carry 100W you need a lot of thick copper to avoid voltage drops. To carry 4K DisplayPort, you need all those extra wire pairs. That means more soldering and more cost. Most people who want to connect their keyboard or charge their smartwatch don't need 100W and 40Gbps and they don't want to spend \$10 per cable. So a lot of cables skimp on the copper and wires, and that is where a lot of the confusion with USB-C comes in.

If you're using USB-C to replace your classic USB A/B devices, you'll only need USB 2 compatibility at 480 Mbps (nearly any cable and length up to four meters can handle that). As you move up to USB 3.0 / 3.1 Gen 1 (5 Gbps), the max length goes down to two meters. At 3.1 Gen 2 (10 Gbps) and 3.2 Super-Speed+ (20 Gbps), you will need to make sure your cable is designed for that purpose and it won't be able to go farther than one meter.

Alternative modes are protocols that are different than USB, but can use some specific USB-C cables that, again, are designed to handle the high data rates. Those modes cover Thunderbolt 3, DisplayPort, HDMI, MHL, and VirtualLink (as well as whatever we come up with next).

For example, Thunderbolt 3 cables that are longer than 0.5 meters need to be “active,” which means they have electronics inside to amplify/equalize the signal for extended length

cables or to perform protocol conversion. If the cable is 0.5 meters, it's called passive.

If you're connecting to a monitor, use a cable that is marked for use with DisplayPort. If you need 100W to power your laptop, do not use a 3A USB-C cable when you need a 5A one. How would you know what capabilities your cable has? Well, USB-C cables are required to contain a power e-mark chip programmed to identify the cable and its capability. However, e-mark chips cost money, and people don't know what e-mark is. So if they can save \$1 on a cable, they buy the one without. The effect of all these different cables, without chips, and perhaps even mis-marketed, is people who have been conditioned for decades to believe that connector shape dictates functionality. They are getting confused because cables that fit don't work and there's no way to know why.

So now you know what to watch out for with cables. What if you are designing hardware to work with USB-C? Compared to classic USB, C's specification is a juggernaut, hundreds of pages long. If you're just trying to update your design to allow USB 1.x/2.x compatibility, it's not too hard:

Connect the four V+ pins together and the four GND pins together, and that's your 5V supply.

D+ and D- are just like you remember, but don't forget to connect *both* D+'s and D-'s together so the cable is reversible.

Connect a 5.1K resistor to ground from each of the CC1 and CC2 pins.

That's it! The 5.1K resistors signal to the power delivery chip that you'd like 5V and up to 1.5A of current (assuming the port can supply 1.5A). If you need to determine how much current the power delivery can supply, you can measure the CC1/2 pin voltage before the pull-down - the pull-up on the other side of the cable can be calculated - 10K pull-up

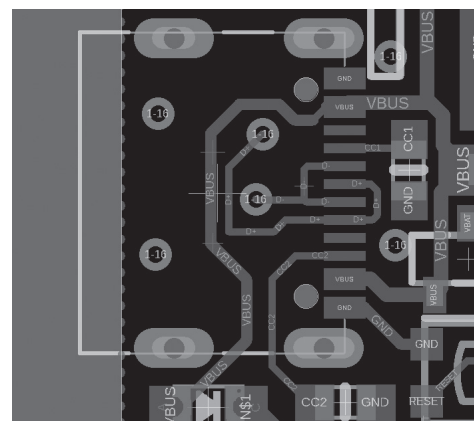
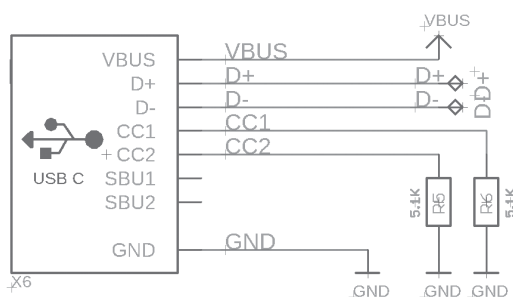
means up to 3A, 22K means 1.5A, and 56K is 0.5/0.9A max at 5V. So for basic usage, there's no additional silicon required, just some small resistors, which makes updating designs easy.

Want more than 5V? Or have a design that can act as either host or device? That gets a little more complex, but you can add a power delivery (PD) negotiation chip that will request higher voltages and currents, or manage sourcing or requesting power depending on what role you are playing in the connection. The BOM cost rises here, but is offset by being able to take part in the wide offerings of USB-C power supplies. And it isn't much more expensive than the original engineering solution where everyone used barrel jacks plus diode plus regulator to protect against plugging a 12V supply into a 5V device, or one with negative polarity. PD chips can be strapped with resistors or I2C programmable.

This isn't easy to get right: first generation Raspberry Pi 4 computers didn't have those two CC resistors. Instead, only one was placed, which meant that some smart power delivery chargers would not work to power the Pi 4. Nintendo Switch also doesn't have PD spec compatibility. Only official chargers/cables are recommended, although without schematics it's hard to know exactly what went wrong.

Despite these hiccups, we like USB-C, especially for low-cost/power/data devices. It's back-compatible enough and the connectors are great - strong, easy to manufacture with, not too large but easy to use. In most cases, you can get away with low-cost simplified USB-C connectors that have only one row of pins. They're about 25 cents each and not much larger than a USB micro B. We'll be using USB-C for all our new hardware designs, and we recommend you do too!

Good night and good luck.



Reflections on Hackers

by Eugen Spierer

My favorite movie is Iain Softley's *Hackers*, but this story is not about it. Instead, it is the story of a young man in great distress who finds solace in a world very reminiscent of the one portrayed by the movie. It is the story of me, whether I like it or not.

I once thought I liked the movie because it had to do with computers. But I've come to realize that's not the real reason it had stayed with me for over 20 years as my favorite one. As I got older and tried my luck in the computer industry (and failed), a creeping feeling made its way from the back of my mind to a sobering understanding: what I really loved about the movie was its spirit of youthful rebellion, of camaraderie among like-minded individuals, its fashion and soundtrack, and above all the fact that it reminds me of my younger self.

Having a bunch of close friends like the ones the movie revolves around is a rare commodity these days, especially for introverts like myself who seek their solitude on most days. Having such a tight knit group of friends also endows you with a sense of belonging, a concept which has become quite foreign in my own personal world. Belonging is hard: it makes you doubt your decision of joining a given group and, in worse cases, it even makes you suspicious and unable to trust other members of that group. I guess being a team player is an acquired taste. However, the friends portrayed in the movie, despite describing themselves as individuals first and foremost, are banded together in an effort to bring down The Plague. Even their skills seem to complement each other's, as one is better at rigging phone lines while another is able to recall the most minute details of his everyday experiences, the third is a master at cracking hidden codes, and so on.

And they're all young and beautiful and hate authority figures! Three traits, so I've learned, very typical of the punk subculture, which I now identify myself with from afar, as I am still a lone wolf. An innate disgust of authority has made me unable to be a part of large scale social systems, a fact which

lends itself to perpetual aloofness, a moderate amount of loneliness, and a general ineffable feeling of cruising through life like an un tethered balloon trying to find its path among what seems like a vast, empty space. Nevertheless, a man's got to do what a man's got to do and I can do no other: I try to shy away from places which put one man above another and, whenever I force myself to take part in such systems, I become entrenched in self pity.

I realize the costumes, makeup, accessories, and hair styles in *Hackers* have all been designed by professionals, but it is my enduring hope that they are based on actual, daily dress habits of those who proudly call themselves punks. I also realize the punk movement revolves around punk music, which I have not taken a liking to. Despite that, I remain tightly clung to my (erroneous?) notions that the ideology conveyed by punk supersedes my somewhat skewed way of looking at punks and that the fashion and looks which I instinctively attach to punk are true to their cause of romanticizing the movement, albeit not necessarily true to its actual real life appearance.

But the movie is just a movie, right? No real people experience adventures the likes of which are portrayed in it. Actual hacking can be quite dull: it consists of sitting in front of a computer screen for hours on end while *not* attending partly dim nightclubs full of cyberpunk paraphernalia. Once again, I find myself entangled by the false romanticism of the movie. Or do I? Upon much retrospection, I have concluded that I actually did experience something akin to what the movie presents. It all happened during a very dark time of my life, but what happened was a ray of light which (it took me years to realize this) was one of the best experiences I have ever had. This article is an attempt at describing my own personal "Hackers" movie: real life events very closely resembling the movie's attitude and spirit.

The group I can somehow call my own had four members. I say "somehow" because what's now left of it are just dim memories of wonderful friends who helped shine a light in a very dark world. This was 20 years ago,

when I was in the 9th grade. My friends were Zvika, Ran, and Avi. I used to call myself by the handle The Cyborg and Avi's handle was Warhead, Zvika's board was The Lighthouse, and Ran called himself Cyberhead.

These were the last days of the BBS era. We used to hang out during school breaks and sometimes after school and talk about what magnificent BBSes we logged onto or how great Zvika's board was. I probably went on and on about whatever programming project I had going on, of which the main one was "nIRC" (more on that later). Sometimes we met at a local basketball court and shot some hoops (I don't think I've played basketball since then). But mostly we listened to Zvika and stared at him as if he was the BBS/computer demigod.

There were four of us, and I'll use the original *Hackers* roster to assign each of us to a character from the movie: Zvika would, of course, be Zero Cool, for he was the wisest and most knowledgeable among us. He was also a bit detached, running his own board and not always paying attention to us lowly beginners, and I say that with the utmost fondness. Ran (Cyberhead) could be described as Lord Nikon, for he was the most lovable among us - everyone liked him and got along with him. To my understanding, this goes on to this day. I would affectionately describe Avi (Warhead) as Joey, for he was always trying out the new stuff the others had taught him with great enthusiasm and good-hearted fun. Lastly, for reasons which are to become apparent, I shall describe myself as Cereal Killer. I always had projects which did not interest the others much like the movie character (being a phreak) and, of course, I would have been happy to crash at someone else's place, rather than my own.

Zero Cool had his own BBS. It was one which had existed for a while prior to the formation of our group, and he had already established connections with other boards and started trading warez, which were pirated programs cracked and distributed (mostly) free of charge among BBSes. He had knowledge of other BBSes, their operators and their handles, which he would sometimes blurt out to us in a long list. This usually left Warhead and myself amazed and smitten. Zvika was the one who came by my house and helped me fix the computer my dad had just bought for me. (I had accidentally erased the autoexec.bat and

config.sys files.) To this day, I get the chills whenever I think of what he must have seen there and am thankful that he did not just run away the moment he stepped into the apartment. Later on, Zvika loaned me a hard drive to install in my computer. When my dad found out about me tinkering with it, he smashed the hard drive and left me to come up with an excuse why I couldn't return it. I told Zvika it slipped my hand and fell because I was utterly embarrassed to tell him the truth. He said it was OK and that I shouldn't worry about it. That's just the kind of nice guy he was. Zvika is a naturopath today and lives with wife and son not far from where we grew up.

Lord Nikon (Cyberhead) made all school-work seem like a walk in the park. He was a straight A student, (which explains his future academic accomplishments) and was very much liked by his teachers and friends. I used to play basketball with him at the court next to his house. He was the one I could talk to the most about the program I had been writing during that period, since I don't seem to remember any of the others being interested in software programming. During school hours, we used to exchange knowing glances about little tricks such as finding a back door in the school's Microsoft Word program which enabled us to access the network's command prompt, a thing which was strictly forbidden by the school's computer teacher - let's call him Agent Gill. Cyberhead was the one who helped test the program I'd written, named nIRC after the popular Internet Relay Chat client mIRC, on the school's network. It was a chat program designed to allow two users on the same LAN to chat with each other. We tried it on the school network covertly using the loophole we had found in the Microsoft Word program, and I was very proud when I was barely able to talk to Cyberhead on it while he was sitting at a different console.

Agent Gill, the computer teacher who was perceived by us (well, Warhead and myself at least) as the quintessential "bad guy," used to shout a lot in a high pitched squeaky voice. He was the one who denied us access to various programs we found interesting. We were to stick to the programs we were assigned to during class, he said - which amounted to the above mentioned word processor. When Warhead and I later misbehaved, Cyberhead was the one among us who got to go on a school

trip to the U.S. He later got to travel quite a bit and for a long time I resented the school who gave opportunities to those who already had plenty and denied them from those who had the world closed off to them. Cyberhead now lives with his family in a small village. He went on to have a successful military career, undoubtedly making his parents and everyone else around him very proud.

Joey (Warhead) had friends from a wide range of social circles, so what we were doing was probably just one of many endeavors he was involved in. He really liked the world we inhabited and often expressed great interest in learning more about BBSes and the big white clumsy boxes we were playing with. Along with myself, he would listen to Zero Cool's stories of far away (though in the same calling code) boards, and enjoy hacking away at Agent Gill's school computer network. Though the memory is dim, I seem to remember that he was with me when we tipped a hot water pot and caused the water to run into the computer room. We were later told the water had evaporated and damaged the computers, but I'm pretty sure that was just a hoax. We ended up not partaking in the aforementioned foreign exchange trip because of that. When we got older, Cyberhead became a religious person and now lives in Israel's occupied territories. He is involved in various right wing groups and describes himself as an itinerant lecturer on subjects of right wing politics.

All of this brings me to Cereal Killer (me). I most fervently sympathize with this character for a number of reasons, not the least of which is him being a punk. Doing business on a shady side street selling pirated music to innocent passersby. I don't fancy myself as a salesman, but I do identify with the cyberpunk underworld he inhabits. I too have an enduring dislike and disrespect for authority and often find myself at the fringes of society because of it. I do admit that I like Cereal's attire, too. The notion conveyed by it is one of a spirit marching to the sound of its own drum. Of originality manifested along with total disregard to what society has to offer. Even among his own friends, Cereal is somewhat of an outsider: His domains of expertise lie in a different domain - he is a phone phreak.

But, as mentioned earlier, the thing about him which attracts me the most is his undetailed family situation. You see, during the

time I was a part of this pack of friends, I had also been living with an abusive father. I used to get beat up at school and at home. My life outside of the computer world was narrow, pathetic, and miserable. I wished I could walk around and crash on people's couches with nothing but a toothbrush, but the sad truth was that I was a nonviolent nerd. I used to run away from bullies at school (although I was always bigger than them, why did I do that?) and come home to an empty cold house where I would immediately turn on my computer, either illegally hooking it up to the phone (my dad did not allow it) with a cable I would hide right after, or just sit for hours on end and code various programs in the Pascal programming language, which still holds a soft spot in my heart to this day. I would do that for about eight hours straight and then go to sleep, without doing any of the excessive self grooming mandatory of a healthy teenager. Despite being depressed, programming and the knowledge of being a part of a group which appreciated what I was doing kept my spirit from plunging into an abyss. The main programs I remember from that era are nIRC which I described earlier, a space shooter game, and even a Pascal module designed to allow programmers to use the modem in their programs (that one is still online at the SWAG archive at swag.outpostbbs.net/COMM/0109.PAS.html).

You can obviously see why this was a dark time for me, and it has certainly affected the rest of my life and the way I see the world. However, my group of friends - my Hackers - were a bright ray of sunshine which has instilled itself in my memory as one of the better experiences I have ever had.

The movie *Hackers* actually came out earlier - in 1995. It had been my favorite movie even before the events described, but only decades later did I realize that some of the fictional events from the movie have also happened to me, albeit in a somewhat less dramatic fashion. Only years later did the thought that we actually had our own group of cyberpunk hackers dawn on me, and I am writing this in appreciation of how great it was that we were all brought together by a common interest.

Dedicated to my friends and the SWAG archive staff, who gave me a chance where very few others did.

Pass the Cookie and Pivot to the Clouds

by Johann Rehberger
security@wunderwuzzi.net

Web applications and services use cookies to authenticate sessions and users. An adversary can pivot from a compromised host to web applications and Internet services by stealing authentication cookies from browsers and related processes. At the same time, this technique bypasses most multi-factor authentication protocols.

The reason for this is that the final authentication token that the attacker steals is issued after all factors have been validated. Many users persist cookies that are valid for an extended period, even if the web application is not actively used. Cookies can be found on disk and in process memory. Additionally, other applications on the target's machine might store sensitive authentication tokens in memory (e.g. apps which authenticate to cloud services). This pivoting technique can be extended to bearer tokens, JWT (JSON web token), and the like. Pass the Cookie is a post-exploitation technique to perform session hijacking.

So, let's Pass the Cookie and Pivot to the Clouds.

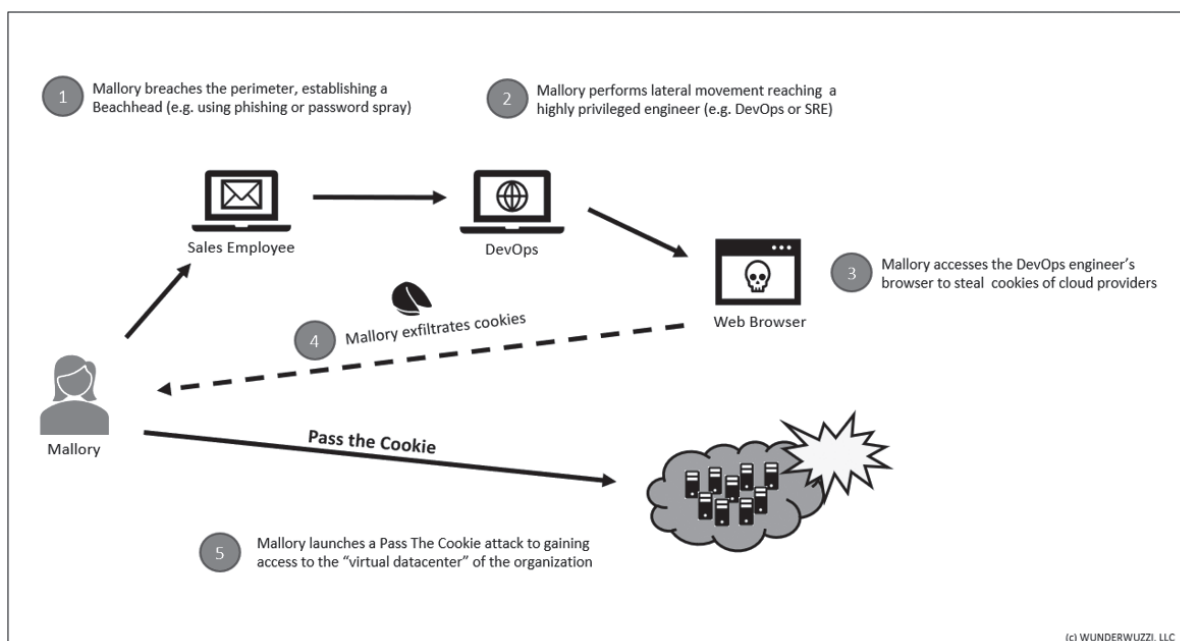
Attack Chain

Disclaimer: Always make sure you have proper authorization before pen testing.

Pass the Cookie is done via the following steps (variations exist):

- Post-exploitation, acquire the cookie from the victim's browser or other processes (e.g. via process dump, or accessing the cookie storage on disk)
- Exfiltrate the necessary authentication cookies
- Open Firefox on the attacker's machine (or any other machine)
- Navigate to the resource to access (the domain the cookie is valid for)
- Use the developer console and update the cookies via the user interface (make sure to set the domain correctly)
- Refresh the page and observe being logged in as the victim

The following is a graphical representation during a typical red team operation, highlighting the steps:



Considering that cloud service providers for many companies are like a virtual data-center, the cookie is comparable to the main entry key to the virtual facility. Pass the Cookie also works on other online services like mail, social media, etc.

Mitigations

To protect oneself from these attacks, it's important to stay up to date with security patches, etc. to ensure your host does not get compromised. As seasoned security engineer, you assume the worst. Here are some ideas on how to mitigate implications of an attack:

- Regularly delete persistent cookies so they get removed from the hard drive to limit exposure
- Delete session cookies as well
- Be the only administrator on your machine
- Leverage features that cloud providers offer (threat detection, IAM (identity and access management), RBAC (Role-based Access Control), firewalls, etc.)
- Browse sensitive sites (high value assets) from isolated or dedicated machines
- Separation of duties
- Disable remote access services on your machine (such as SSH, RDP, ARD)
- Requiring further authentication proof for sensitive operations can help limit the damage
- Requiring client-side certificates makes it also more difficult to pass the cookie

Detections

When it comes to detections, a few things come to mind:

- One can monitor on the client side for applications that perform process dumps on browser processes or others
- Monitor for unusual activity on critical

web assets (e.g. cloud provider management consoles, etc.)

- Monitor for login anomalies (location, time, unusual access patterns)
- Leverage features that cloud providers and web apps provide (threat detection, access logs, etc.)
- Perform authorized adversarial emulation in your organization to test detections

Acquiring Cookies, Tools and Techniques

In case you don't want to write your own toolset, there are a couple of options available to gain access to cookies:

- firefox_creds - access the SQL Lite cookie databases
- cookie_crimes - neat way to grab cookies from Chrome on Macs (also Windows and Linux)
- ProcDump - Swiss army knife to dump strings from any process
- Sniffing Traffic - e.g. using SSLKEYLOG-FILE during post-exploitation, leveraging WinInet tracing

There are good online resources available on how to access and decrypt the cookies in the SQL Lite databases as well if you'd like to dig into a little more under the covers.

Conclusion

Pass the Cookie is a powerful post-exploitation technique to pivot from on-premise machines to cloud assets. It can be leveraged to bypass MFA (multi-factor authentication) techniques as the cookie is in the end still a single factor.

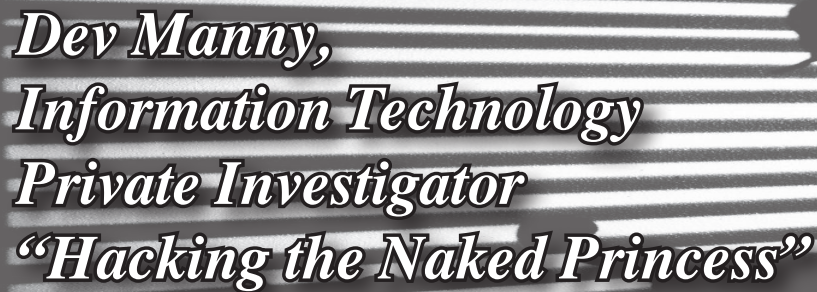
Hopefully this was helpful, so you can build better detections, improvements, and tests into your infrastructure to catch malicious activity.

ANNOUNCING THE 2600 TOTE BAG!

\$7.99 each,
4 for \$29.99 plus shipping

Find this and all kinds of other fun hacker stuff at store.2600.com





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

by Andy Kaiser

Chapter 0x18

One of the last things I remembered seeing at the RedAction HQ was a business-casual ladies shoe as it kicked me hard in the face. Most would consider that a warning sign, but I wanted to get back. First, though, I needed to know where RedAction had dumped me.

Behind me was the crackling and roaring fire of a burning building, where I'd been trapped for who knew how long. Though it seemed I was in the middle of nowhere with no hope of rescue, the black smoke leaping toward the sky was a signal that couldn't be ignored for long. Fire and police would get here soon, but they'd also come with questions I really didn't want to answer.

I walked away, and realized why I was nervous (apart from the recent beating and escaping death by incineration): Whoever had locked me in the old storage building had also emptied my pockets. I had no phone. No Leatherman multi-tool. Those were my weapons and I needed them. If I'd stripped off all my clothes, I wouldn't feel any more naked.

Earth's daily cron job kicked in. The evening grew cool as the world around me shifted into dark mode. The sun set, the sky darkened, and a glow became visible on the horizon. I still didn't know where I was, but that glow was a flame to this civilized moth. I walked toward it. I sniffed the air and caught a whiff of something weird, a faint funk of rot.

My barely-achieved distraction at RedAction had given P@nic the time she needed to inject herself into their network, but I had no clue how much damage she'd caused. I just hoped my concussion had been worth it.

Reboot had brought me into all of this. Not realizing I'd investigate his problem more than he wanted, I'd found the Naked Princess picture and uncovered RedAction's war against P@nic. Based on my sore nose and the taste of blood in my mouth, I assumed the kick to my

face was still visible, yet I was heading back to what was definitely my worst client ever. I owed it to P@nic.

Up ahead were some unusual hills. Strange plateaus of land rose high to gaze down over the flat farmland around me. Dozens of birds circled lazily far above them. Poised at the top of one of the hills, silhouetted beautifully in the setting sun, was a garbage truck. The faint, low thrumming of a diesel engine sounded, and the truck lumbered down the hill. As the wind shifted and a pungent smell carved its way into my nose, I realized I knew this place.

This was a garbage dump, a massive solid-waste landfill serving most of West Michigan. After decades of use, the trash piles dominated all. Trash was reclaimed for recycling where possible, otherwise it was poured into the hills before me, where it sat and rotted. Bacteria blossomed in a beautiful ballet of chemical farts. The resulting methane gas was collected and routed to processing for energy generation.

Anyone driving the wrong way out of East Rapids knew this smell. I was in Cooperstown. For the first time in my life, I was happy to be here. I took a deep breath, choked on a smell so strong it had a flavor, and I began to jog to where I knew the expressway on-ramps would be.

A few minutes later, I switched from an athletic jog to a gasping speed walk, because I rarely exercised and already felt like I was about to collapse. A few minutes after that, I reached a gas station.

I was able to make a phone call, courtesy a trusting, friendly gas station employee. My first priority, I called a number I'd set up that would send a kill signal to my cell phone. I'd check on it when I got back to my office, see what the GPS logs could tell me about where RedAction had taken it. They probably wouldn't be so stupid as to keep a working stolen cell phone, but weirder things had happened.

Second priority, I needed to get out of here. This was thanks to the same employee,

who was now noticeably less trusting and less friendly since I still hadn't returned his phone, despite the very specific words he was using to describe where he was about to shove that phone if I wanted it that bad.

He got his phone back because I was done: An Uber ride was heading my way.

I had the Uber take me back to the city, but first with a circling the block before stopping at RedAction. I didn't need to be that careful. The building was dark. The entrance doors were unlatched, open, dancing gently in a slight breeze. The security cameras that had covered the building's strategic sight lines had all been removed.

The building had been gutted.

I hadn't been unconscious for that long. After I woke up, it must have taken a couple hours to get back downtown. In that time, it looked like RedAction had cleared out everything important. Since my appearance rarely struck fear into anyone's hearts, I assumed P@nic's plan had succeeded. She'd shut their network down. Hard.

I made sure the Uber driver saw my account credit balance, told him to wait for me, and I went inside the building.

The entrance was dark, shadows played on top of shadows, barely visible by the faint city lights from outside. It was enough for me to find a wall switch, and I began clicking on the lights as I continued to explore.

The office cubicles were still here. The computers were gone. The cubes looked like they'd been cleaned out, too. I saw none of the usual proof of humans: There were no family photos. No corporate-critical comic strips posted on the walls.

I found the cube I'd originally used to inject P@nic's USB key. That too was empty, save for a comfy-looking desk chair with lumbar support. I explored further and found the server room and office demarc, what had to have been the nerve center of this stripped skeleton.

There were no servers, switches, routers, or anything else I'd expect to see. The only clues left were a single empty 42U rack bolted to the floor, the door hanging open and unlocked, and a thick umbilical of CAT7 cabling drooling out of the ceiling. Examining the mess of cable ends hanging above my head, I saw they'd been cut, like someone had just hacked them off with scissors.

In the center of the rack, there was an inside shelf. The shelf was empty, except for a tiny

blue USB flash drive.

I stared at it.

Whoever had run this evacuation, they'd been in such a hurry they hadn't the time to even unplug anything - they'd sliced the cables and ran out with the equipment. They'd been extremely thorough, so they also must have made a point to leave this USB drive here, placed conspicuously in the center of the rack shelf.

Was the USB key a message for someone? For me? Was it a trap of some kind, and I'd plug it into my test rig and it would explode in my face?

There was only one way to find out, so I grabbed the blue drive and dropped it into my pocket. I'd be as careful as I could, but I couldn't resist seeing what this was when I got back to my office.

My heart was pounding, but my apprehension dropped a bit. Yeah, it looked like P@nic had finished her inject into the network. I didn't understand why they'd cleared the building, though whatever she'd done must have really hurt.

I went back to the Uber.

I was dropped off at my office. Standing out in the dark street with the night too silent around me, I looked up to my rental's second floor, at the window of my office.

The lights in my office were off, but the window shone from a faint inside light. I recognized the glow and the white-blue color.

It was one of my office computers, the one I usually left on the desk for miscellaneous research and case work. The one I'd protected with drive encryption. And two-factor authentication. And a dead-man's switch ticking away in the OS.

I hadn't left it on. Someone, right now, was in my office and they were on my PC.

I sprinted up the stairs and slammed my shoulder into my door, realizing that if the intruder had simply slid the deadbolt closed, I was about to be in a lot of pain.

Not only was the door unlocked, it was unlatched. I launched into the room with unexpected speed and expected clumsiness.

The lights in the office were out. In the darkness, the monitor's LED lit P@nic's face a ghostly white. She looked up in surprise as I stumbled in front of her.

"Hey, how's it going?" she said, her eyes shining from the monitor's glow, and also something more. "We need to talk."

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, *email us* at 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 31 - February 2 May 14-15
ShmooCon 2020 **Converge 2020**
Washington Hilton Hotel Cobo Hall
Washington DC Detroit, Michigan
www.shmoocon.org convergeconference.org

March 14-15 May 15-17
LibrePlanet 2020 **NolaCon**
Boston, Massachusetts Hyatt Centric
libreplanet.org/2020 New Orleans, Louisiana
nolacon.com

April 10-11 June 12-14
CarolinaCon 2020 **CircleCityCon 7.0**
Embassy Suites Uptown The Westin
Charlotte, North Carolina Indianapolis, Indiana
carolinacon.org circlecitycon.com

April 10-13 July 31-August 2
Easterhegg 2020 **HOPE 2020**
Maschinenfabrik Kampnagel St. Johns University
Hamburg, Germany Queens, New York
eh20.easterhegg.eu www.hope.net

May 5-6 August 6-9
RVasec **DEF CON 28**
University Student Commons Caesars Forum, Harrah's, Ling, Flamingo
Virginia Commonwealth University Las Vegas, Nevada
Richmond, Virginia www.defcon.org
rvasec.com

May 8-9 August 11-18
THOTCON 0xB **BornHack**
Chicago, Illinois Funen, Denmark
thotcon.org bornhack.dk

*Please send us your feedback on any events you attend
and let us know if they should/should not be listed here.*

Marketplace

For Sale

OPEN SOURCE HARDWARE: crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see [bunnie huang's NeTV2 project](#)).

HACKERSTICKERS.COM now carries cDc merchandise, sells lock pick sets, Bawls energy mints, and an awesome lineup of hacker clothing including the new Johnny Cupcakes x HackerStickers collaboration Hacker Big Kid Shirt. Get all the goods at [HackerStickers.com](#).

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at <https://leanpub.com/techgeek>. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

HEATHKIT BOOK: Interested in vintage electronics? *Classic Heathkit Electronic Test Equipment* by Jeff Tranter covers Heathkit's test equipment line, with in depth coverage of different models including oscilloscopes, meters, tube testers, etc., as well as a history of Heathkit and resources for collecting and restoration. 140 pages in 11 chapters plus appendices. Retail for \$19.95 from [lulu.com](#) and [amazon.com](#).

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at [HackerWarehouse.com](#).

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from [SecureMac.com](#). Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

PORTABLE PENETRATOR. Find WPA WPA2 WPS WiFi Keys Pen Testing Software. Vulnerability Scanning & Assessment Customize reports use for consulting. Coupon code 20% off: 2600. <https://shop.secpoint.com>

SAN ANTONIO RADIO MEMORIES - LET 'EM OUT! Remembering San Antonio Radio (and technology) in the 40s, 50s, 60s, and 70s. Profits go to ARRL. Visit www.velocepress.com/books/arts/sarm.php to order today!

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: \$36.99 per 12 pack or \$53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from [store.2600.com](#).

Help Wanted

MEDIA SAVVY HACKERS NEEDED. Want to test your hacking abilities? Think you can make news? Incarcerated prisoner in California institution needs to get media attention. He is locked up with a life sentence illegally. He has proof - including testimony from the prosecuting attorney - that he shouldn't be in prison, but courts (judges) refuse to reverse the conviction because it would open the door to civil action. If the news media & public knew what was going on, it would frighten them to their core. If you can assist in hacking the news media outlets to expose this grave injustice, email: mdwhite2020@gmail.com, with "media hack" in the subject line.

PERSONAL ASSISTANT. I need someone to go online for me because I'm incarcerated and have no Internet access so I'm looking to hire a personal assistant. Pay: As agreed per project about 1-5 hours per month, you choose your hours. Duties: Internet research, Internet shopping, sending e-mail, etc. Must Have: Own phone, Internet access, computer and printer. Experience: No experience necessary but the following skills and interests are helpful. Self-motivated, the ability to follow instructions, and an attention to details. Computer and Internet skills. With an interest in the rehabilitation of criminals and the mentally ill, helping others, fundraising, and advertisement. Please mail me your name, contact address, and phone number, along with reason I should pick you. Eugene Banks, 1111 Highway 73. Moose Lake, MN 55767-9452

JOIN THE [HTTPS://CODEFOR.CASH](https://codefor.cash) community and earn money with freelance programming jobs. All hats welcome!

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the 2600 site in mp3 format! Your feedback on the program is always welcome at oth@2600.com.

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

Services

DIGITAL FORENSICS EXPERTS FOR CRIMINAL DEFENSE! Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. 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. We can recover data nationwide from many sources, including computers, external media, tablets, and smartphones. 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. Sensei's principals have written 17 books on IT, cybersecurity, and digital forensics published by the American Bar Association. 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.

HAVE YOU SEEN THE 2600 STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of 2600 and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. You can also use vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. 2600 readers get free setup! BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for \$5.

GET YOUR HAM RADIO LICENSE! KB6NU's "No Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides/. Paperback versions are available from Amazon. E-mail cwgeek@kb6nu.com for more information.

DOUBLEHOP.ME is an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and transparently exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin and offer automated order processing! Use promo code COSBYSWEATER2600 for 50% off (<https://www.doublehop.me>).

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/>

ANTIQUÉ COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. <http://www.vintagecomputer.net>

SKEPTICAL OF GITHUB? sr.ht is an in-progress software suite for hosting open source projects that's more in tune with the hacker way. sr.ht is more modular and more flexible, with features like mailing list driven development and full virt build automation with KVM. Interested in helping test the beta? Reach out to SirCmpwn: sir@cmpwn.com

SQUIDIX provides serious discounts for fantastic web hosting for 2600 readers. We love our clients and they love us. Our 2600 promotion will give you a Super Squid hosting platform for only \$26.00 for the first year, then only \$9.95 per month when paid annually. Sign up today and get free domain or domain renewal. This offer valid for any new accounts in 2018 and includes a free CPanel transfer of one existing site. Sign up at www.squidix.com

LOCKPICKING101.COM - a locksport community driven by lock picking hobbyists and locksmiths alike. New to lock picking or want to advance your skills or help others learn? Just head over to LockPicking101.com and say Mr. Picks sent you!

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre

distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

Personals

I AM A WOMAN INCARCERATED IN FEDERAL PRISON. I'm hoping to find an intelligent, curious penpal with hacker mentality. I will be released sometime around the holidays this year. While I am here, I do a lot of reading. I'm finishing a vet assisting correspondence course, studying more about Linux, and trying to remain healthy in an unhealthy environment. Besides 2600, I read *SciAm*, cyberpunk, history, animal welfare, behavior and psychology, law and politics - especially computer-related. My interests are far ranging and diverse. I have many passions from outdoor fun to Internet freedom, whistleblower, transparency and privacy causes. I AM opinionated (for example, if you do not support WikiLeaks, don't bother writing), yet also funny, idealistic, and caring. I love to learn and think, and there is not a lot of that available here. I'm considered white collar crime for providing dark web info and anti-facial recognition tools to others. So please write (I can also email if you send your email handle) and tell me what you're about and what's going on in your world. I like science, politics, everything tech - but most of all, a person willing to take time to be an LED in this often dim and dark world. Stacia Quarto, 92274051 Unit 2 South, FMC Carswell, PO Box 27137, Ft. Worth, TX 76127.

I AM A 36-YEAR-OLD FREE SOFTWARE ACTIVIST, interested in all aspects of copyright, trademark, and patent law. Looking to meet similar minded women, 26-43 in the greater-Seattle area. My interests are GNU/Linux, social justice, Mexican food, ghouls, model trains, and video games. Just a Crash looking for my Burn. I have strong opinions about obscure media formats. I like drinking, cooking, doodling, and wildlife. Let's hit the clubs, make each other laugh. I like a laugh, chat, bit of a debate, an argument. I like life. goldentee@gnu.org

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 marketplace@2600.com.

Deadline for Spring issue: 2/21/20.

Hacker Perspective Submissions Are Open

We're looking for a few good columns to fill our pages for the next bunch of issues. Think you have what it takes? You might surprise yourself. "Hacker Perspective" is a column that focuses on the true meaning of hacking, as spoken in the words of our readers. We want to hear YOUR stories, ideas, and opinions.

The column should be between 2000 and 2500 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These questions are just our suggestions - feel free to answer any others that you feel are important in the world of hackers.

If we print your piece, we'll pay you \$500, no questions asked (except where to send the \$500). Send your submissions to articles@2600.com (with "Hacker Perspective" in the subject) or to our mailing address at 2600, PO Box 99, Middle Island, NY 11953 USA.

Submissions only open every few years so don't delay!

HOPE ***** 2020

(the only HOPE with the year in it)

Oh yes, it's happening. And we are super enthused at all of the possibilities.

We have a brand new venue with more space than ever!

Four speaking tracks with rooms as big or bigger than before.

Buildings that are close together and spacious.

24 hour access to as much of the space as we need.

Many additional rooms for new projects or additional speaker tracks.

Plenty of chill space for people to hang out and socialize.

More than 100,000 square feet of additional outdoor space to use for additional projects.

A network at least three times faster than our already record-breaking speeds.

A healthy campus environment with people who appreciate who we are.

Free parking for those driving in (and no Manhattan traffic to deal with).

Only minutes away from JFK and LaGuardia airports.

A one-stop train ride from midtown Manhattan.

Options to reserve dorm rooms or suites onsite for less than the cost of a hotel.

Food options throughout the event onsite.

Nearby discounted hotel space.

And we've already run out of space on this page. But there's so much more to be excited about. With your help and support, this will be the best HOPE yet! Keep checking www.hope.net for details on how to get involved, submit speaker ideas, start projects, and get tickets.

HOPE 2020
St. John's University
Queens (New York City)
July 31 - August 2, 2020

Student Privacy by Practice – Not by Policy by Matrix8967

Hello 2600 readership.

I'm a systems administrator at a large (for the region) school district. I've been in K-12 for about ten years. I left my high school saying: "I'll never go back, even if they paid me!" Then my school said they'd pay me, and I went back immediately. I've changed districts a few times, but I've noticed an alarming trend that's already overtaken K-12: Google, and its lust for your student's data.

To lay the land of the K-12 environment: K-12 has been *rife* with old, dilapidated, and abandoned software. Companies will develop "curriculum" for students in things such as Flash, Shockwave, or Java and sell it to schools for mind boggling premiums. The next step is to hold the schools for ransom for upgrades where one of two things happen:

1) K-12 decision makers won't understand paying for software twice, and ride the old version. As a real example of this: I learned to type in elementary school, and when I began work as an intern in high school, I was tasked with installing the same software....

2) The district begrudgingly pays for the upgrades, and experiences all the joys of "vendor lock-in." For Example: Three year contracts on testing data aggregation, where the test is only administered every two years....

This software ecosystem created a tinderbox for our friendly neighborhood data aggregation company. Google makes its Google Apps For Education suite (GAFE, formerly GSuite) available for free to all K-12 schools. This goes hand-in-hand with its literal truckloads of Chromebooks that are being dropped off at schools each year. Districts are buying these in warehouse quantities trying to go 1:1. In a modern classroom, students will walk in and pick up a Chromebook, login with personally identifiable information, and browse the web with the world's largest advertising agency at the helm.

Google has done some fancy footwork to side-step data collection regulations. GAFE splits its products into "Core Services" and "Additional Services." Core Services are things like Google Sheets, Google Docs, etc. Google's Core Services End User License Agreement (EULA) says: "*User personal information collected in the Core Services is used only to provide the Core Services. Google does not serve ads in the Core Services or use personal information collected in the Core Services for advertising purposes.*"

However, this is where "Additional Services" comes in. GAFE Additional Services are things like Google Maps and YouTube. Google's Additional Services EULA says: "*We also use this information to offer users tailored content... We may combine personal information from one service with information, including personal information, from other Google services... Google may serve ads to G Suite for Education users in the Additional Services.*"

Google's PR department came out in full swing after case studies from the EFF started to ask inva-

sive questions concerning Google's privacy policies. Google's PR privacy site states: "*For G Suite users in Primary/Secondary (K-12) schools, Google does not use any user personal information (or any information associated with a Google Account) to target ads.*" We know that Google would never lie in order to turn a profit, so let's take them at their word for this and ask: "What does Google do with all the student data once the students graduate and move to their own personal Gmail accounts?" It'd take nearly no time at all to marry two sets of data about students, especially if they use the same devices to create a personal Gmail account.

Compounding issues: There's a huge lack of opt-out policies, since this is handled on a district-to-district basis. Assuming a district has an opt-out policy in place, if the whole classroom is using GSuite, it singles out the kid who isn't complying. Special arrangements will need to be made for the privacy conscious student which can also cause issues. (I'm sure each of us can think of a time when being different from the majority ended with an upsetting exchange.)

I've looked at removing the personally identifiable information from student logins in our district, but Google has a fix for that too. In Google Classroom, teachers are able to fill in any blanks it has on children's Google Profiles in order to get their digital classroom up to date. There's also the legal questions surrounding Children's Online Privacy Protection Act (COPPA) violations of IT staff (us) signing up kids under 13 to use GAFE services. Google says that it's products *can* be used in compliance with COPPA, which is not very reassuring.

So, what can be done? Thankfully for public schools, the school board has to answer to the taxpayers and voters. Attending school board meetings and asking for more information about opt-outs and alternatives could yield positive results. In my opinion, Pi Tops are the best alternative to Chromebooks since they encourage discovery and come with a great set of STEM curriculum. They're similarly priced and easier to repair/upgrade, which saves money in the long term. When presented with a viable alternative, the administration and decision makers will be more open-eared, since you're offering solutions, not just problems. (These do have Alexa capability, so that also warrants some strict policies.)

Another viable alternative is flashing GalliumOS onto the existing Chromebooks, which can be a fun learning experience for the students. It's also very satisfying to turn the tools of your enemies against them.

I don't believe in an abstinence-only approach to software. I think privacy by practice, instead of privacy by policy, can set a positive example for students.

gsuite.google.com/terms/education_privacy.html
edu.google.com/training-support/privacy-security

ARGENTINA
Buenos Aires: Bellagamba Bodegon, Armenia 1242, 1st table to the left of the front door.
Catamarca: Rincon Universitario, Av. Belgrano 413, 1st floor. 7 pm
Parana: One Love Bar, Cervantes 384. 8 pm
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA
Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: The Charles Dickens Tavern, Block Arcade, 290 Collins St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

AUSTRIA
Vienna: RIAT - Institute for Future Cryptoeconomics, Neubaugasse 64-66/3/4

BELGIUM
Antwerp: Central Station, top of the stairs in the main hall. 7 pm

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

CANADA
Alberta
Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm
British Columbia
Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba
Winnipeg: St. Vital shopping center, 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, 2nd floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA
Hong Kong: Frites Quarry Bay, G/F Oxford House.

COSTA RICA
Heredia: Food court, Paseo de las Flores Mall.

CZECHIA
Prague: Legenda pub. 6 pm

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm

FINLAND
Helsinki: Forum shopping center (Mannerheimintie 20), food court on floor zero.

FRANCE
Paris: Burger King, 1st floor, Place de la Republique. 6 pm

GERMANY
Berlin: Alexa shopping mall (Alexanderplatz) in front of Manju. 7 pm

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

IRELAND
Dublin: At the entrance to the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL
***Beit Shemesh:** In the big Fashion Mall (across from train station), 2nd floor, food court. Phone: 1-800-800-515. 7 pm
***Safed:** Courtyard of Ashkenazi Ari.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.
Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

KAZAKHSTAN
Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO
Chetumal: Food court at La Plaza de Americas, right front near Italian food.
Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS
Utrecht: In front of the Burger King at Utrecht Central Station. 7 pm

NORWAY
Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm
Trondheim: Den Gode Nabo. 7 pm

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm
Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES
Quezon City: Chocolate Kiss ground floor, Bahay ng Alumni, University of the Philippines Diliman. 4 pm

POLAND
Krakow: VR Cafe (upstairs), Dolnych Mlynow 10. 8 pm

PORTUGAL
Lisbon: Amoreiras Shopping, food court next to Portugalia. 7 pm

RUSSIA
Moscow: RNDM, Nastavnicsheskiy Pereulok, 13-15 Building 3. 7 pm
Murmansk: Freshgame, Rybnyy Proyezd, 8. 7 pm
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN
Stockholm: Starbucks at Stockholm Central Station.

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

THAILAND
Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM
England
Leeds: The Brewery Tap Leeds. 7 pm
London: Trocadero shopping center (near Piccadilly Circus), front entrance on Coventry St. 6:30 pm
Manchester: Bulls Head Pub on London Rd. 7:30 pm
Norwich: Coach and Horses on Thorpe Rd. 6 pm

Scotland
Edinburgh: Nobles Bar in Leith. 6 pm
Glasgow: Bon Accord Pub, 153 North St. 6 pm

Wales
Cardiff: Rummer Tavern opposite Cardiff Castle.
Ewloe: St. David's Hotel.

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

Arizona
Phoenix: Changing Hands Bookstore, 300 W Camelback Rd. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm
Tucson: Barnes & Noble cafe, 5130 E Broadway Blvd.

Arkansas
Fort Smith: Fort Smith Coffee Company, 1101 Rogers Ave. 6 pm

California
Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Idea Fab Labs. 7 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Penngrove: Caprara's Pizzeria, 10060 Main St. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado
Denver (Lone Tree): Park Meadows Food Court.
Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Delaware
Newark: Barnes & Noble cafe area, Christiana Mall.

Florida
Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy.
Titusville: Playalinda Brewing Company, 301 S Washington Ave.

Georgia
Atlanta: Lenox Mall food court. 7 pm

Hawaii
Hilo: Prince Kuhio Plaza food court, 111 East Puainako St.

Idaho
Boise: BSU Student Union Building, upstairs from the main entrance.

Illinois
Champaign-Urbana: Lincoln Square Mall food court.
Chicago: O'Hare Oasis on 294 behind the bank kiosk. 8 pm
Peoria: Starbucks, 1200 West Main St.

Indiana
Bloomington: College Mall food court, 2894 E 3rd St.
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: The Tomlinson Tap Room in City Market.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa
Ames: Memorial Union Building food court at the Iowa State University.
Davenport: Co-Lab, 627 W 2nd St.

Kansas
Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 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 (Cambridge): Starbucks, 2nd floor, Harvard Square, 1380 Massachusetts Ave. 7 pm
Waltham: The Telephone Museum, 289 Moody St.

Michigan
Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota
Bloomington: Mall of America food court in front of Burger King. 6 pm

Missouri
St. Louis: Arch Reactor Hacker Space, 2215 Scott Ave. 6 pm

Montana
Helena: Hall beside OX at Lundy Center.

Nebraska
Omaha: Westroads Mall food court near south entrance, 100th and Dodge. 7 pm

Nevada
Elko: Uber Games and Technology, 1071 Idaho St. 6 pm
Las Vegas (Henderson): SYN Shop, 1075 American Pacific Dr Suite C. 6 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire
Keene: Local Burger, 82 Main St. 7 pm

New York
Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm
Syracuse: Secure Network Technologies, 247 W Fayette St, 2nd floor.

North Carolina
Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).
Raleigh: Morning Times, 10 E Hargett St. 6 pm

North Dakota
Fargo: West Acres Mall food court.

Ohio
Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr, behind the Dayton Mall off SR-741.
Toledo: SIP Coffee, Cricket West shopping center, 2nd floor.
Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

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

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. 6 pm
Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.
State College: Big Bowl Noodle House, 418 E College Ave.

Puerto Rico
San Juan: Plaza Las Americas on 1st floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina
Myrtle Beach: SubProto, 3926 Wesley St, Suite 403.

South Dakota
Sioux Falls: Empire Mall, by Burger King.

Tennessee
Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 301 Plus Park Blvd #300. 6 pm

Texas
Addison: Dunn Brothers Coffee, 3725 Belt Line Rd.
Austin: Whole Foods mezzanine level, 525 N Lamar Blvd. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont
Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia
Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road shopping center. 6:30 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington
Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin
Madison: Fair Trade Coffee House, 418 State St.

URUGUAY
Montevideo: MAM Mercado Agricola de Montevideo, Jose L. Terra 2220, Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, 2600 meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Street Phones



Indonesia. This phone has clearly seen it all and is well prepared for whatever rugged conditions it has to endure. Found in Kuta, Bali.

Photo by Jon Whitton



Dominican Republic. Of course, some phones don't fare as well on the streets as others. This one, spotted in the Colonial Zone of Santo Domingo, has lost its voice (and ears) entirely.

Photo by Sam Pursglove



Bulgaria. Seen on a street near the National Palace of Culture in Sofia, this basic model also provides an outlet for local street artists to perfect their craft.

Photo by Matt Ranostay



Italy. A typical, though increasingly rare, payphone on the street in Florence. What's a bit ironic here is the placement of a "Stop 5G" sticker for what can only be described as the wrong audience: people who are more likely not to own cell phones.

Photo by Indro Neri

Visit www.2600.com/payphones to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photos



We all know what port hacking is about. Scanning for open ports on computers is as old as the hills, and apparently this school in Sydney, Australia has been teaching it since 1959. Discovered by **simran**, this institution also has a motto we can all live by.

Now here's a somewhat sad and funny tale. These folks certainly had an elite address at one time, as found by **pdoherly** in the Windsor Terrace section of Brooklyn, New York. What's funny is the faded out lettering which reads "Buy & Activate Over The Net!" It seems that customers may have taken that advice to heart, making the store itself unnecessary. And that's what's sad.



If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

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

If we use your picture, you'll get a free one-year subscription (or back issues) and a 2600 t-shirt of your choice.