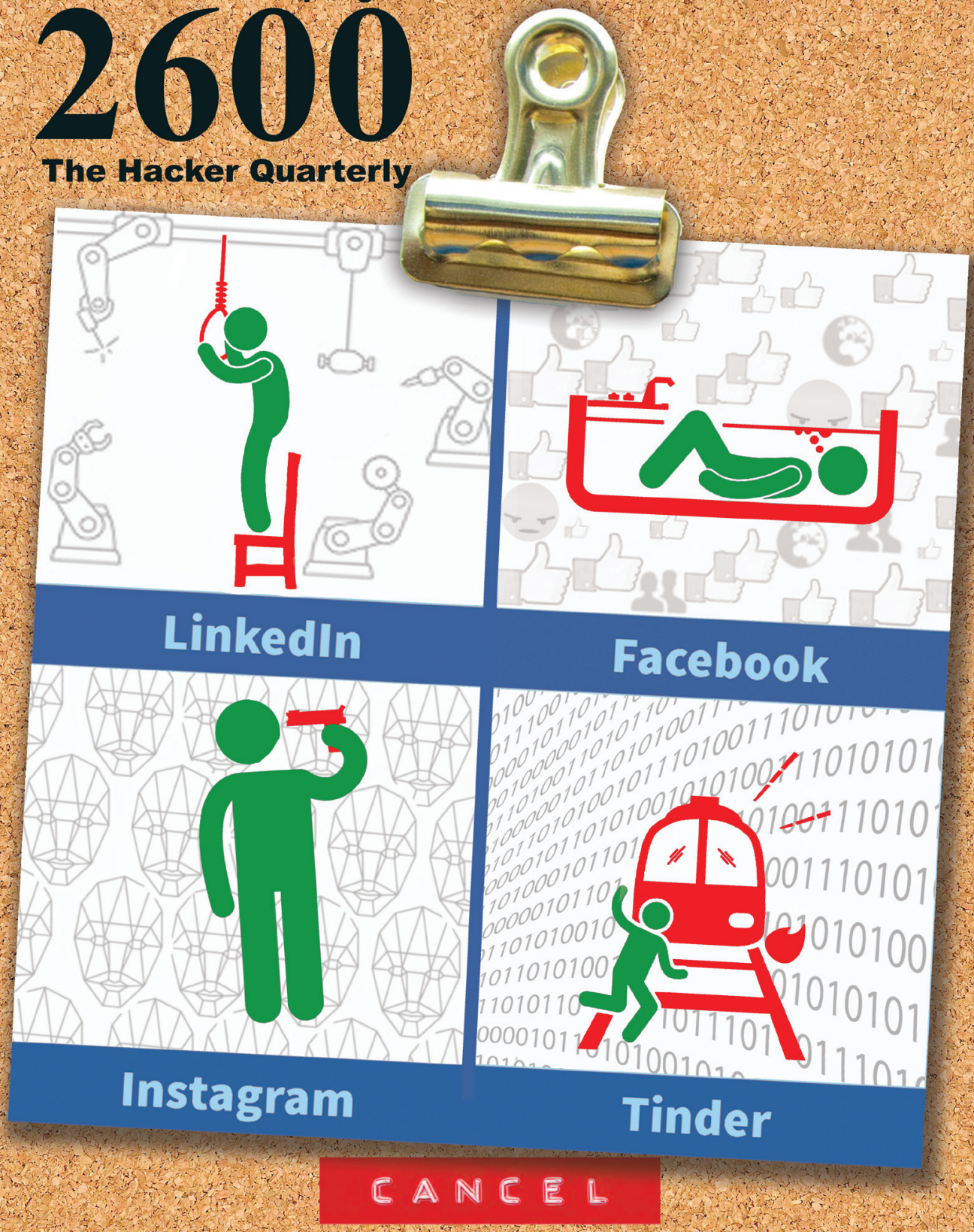
Volume Thirty-Seven, Number One!
DIGITAL EDITION Spring 2020

2600

The Hacker Quarterly



Hawaiian Payphones

Kauai. Found in the Poipu area near a natural feature called The Spouting Horn. If you made a call on this, you'd have to battle the roar of the waves through the lava tubes in order to be heard. Hawaiian Telcom, now owned by Cincinnati Bell (it's true), used to be part of GTE's non-Bell landline network.

Photo by DarkLight

Maui. This is what you'll find at the Maui airport. Millennium phones like this one used to be run by Nortel, but now WiMacTel is the only operator of them in both the United States and Canada.

Photo by Babu Mengelepouti

Maui. This poor thing was seen in Lahaina where it apparently was the bearer of bad news for someone. Operated by WiMacTel, in theory at least.

Photo by _hazy

Oahu. Found at Honolulu International Airport, this phone shows the collaborative spirit that exists between WiMacTel and Hawaiian Telcom. And you may even recognize the old GTE model 120B from the 1980s that's still in use. (Fun fact: Hawaii has more payphones per capita than any other state.)

Photo by Chris Gibson

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 (Do not send us links as photos must be previously unpublished.)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)

Hypotheticals

The New Social Disease

It was supposed to be fun. The whole idea of social networks was meant to augment our actual lives. Instead, in far too many cases, it's practically replaced them.

We've been big fans of the virtual world for as long as we've been around. In the beginning, it was primarily about communications. Being able to connect with people from all over the world was truly a magical - and often illegal - achievement. In the age of smartphones, the very concept of long distance has become a thing of the past for many, defeated by various "unlimited" packages. Of course, we're still paying the same companies vast amounts of money. But we achieved the global connections we were striving for in those early days of hacking and blue boxing. We won.

But things started to take a wrong turn when we began to lose our perspective. People in control - whether in governments, schools, or homes - feared the power of new technology while also embracing it. Therefore, anything that threatened to upset their perception of the status quo was treated as a greater danger than any equivalent act in the non-virtual world. This led to crackdowns on hackers throughout the 1990s that saw offenders sent to prison for minor transgressions on computers - and often sentenced to more time than individuals convicted of violent crimes. They were often punished not for what they did, but for what they *could* have done. This is what happens when those in charge don't have a firm grasp of how it all works. Making judgments while being afraid nearly always results in bad decisions.

At the time, we argued that hacking a website was the equivalent of painting graffiti. But that was often not how the courts saw it. They chose to look at the (often merely potential) financial damage caused by this act of virtual vandalism. And it all came back to one thing: people taking technology far too seriously. In those relatively early days, websites were a fairly new concept, and things went wrong all the time. And the poor security that was endemic on many of them was simply part of the growing pains we all were experiencing. If our own website had ever been hacked (which, sadly, it wasn't), we would have taken the opportunity to learn from our mistakes and build something better, while swallowing the mild embarrassment the incident would have caused. Instead, corporate America and government institutions declared war on anyone or anything that showed their systems to not be what they imagined them to be, all the while refusing to learn how to fix their setups. It was a scenario where everyone lost.

Today, we see much the same thing in the form of social networks. Yes, the websites are more secure and professionally run. But now the problem mostly centers around the actual content. Again, we find ourselves taking things far too seriously. Reactions on outlets like Facebook, Twitter, and Instagram seem to matter more than reactions in real life. Often, the latter is even defined by the former. Make no mistake - this *can* be a good thing. But it invariably turns bad once we sign over our common sense to the latest virtual trends.

Throughout history, crowds have been assembled for both good and evil. A civil rights rally or a Nazi rally each took preparation, organization, and an already existing group of people. But online mobs can be put together much more quickly and without the infrastructure. And it becomes impossible to ignore them, a fact that can greatly enhance the reach of fringe elements. Virtual mobs are able to greatly influence our behavior due to the perceived numbers behind them, even though we have no idea how many people are actually involved. All it takes is the *perception* that lots of people are behind a trend or movement for real humans to take it seriously and become involved. Of course, many times it works the other way, where movements are born in the real world and use social networks to strengthen their organization and become more well known. This is the difference between using social networks as a tool and being a tool of social networks.

Over the years, we've been known to embrace the phrase "become the media." One of our HOPE keynote speakers (Jello Biafra) has made this a foundation of his spoken word presentations. We still very much believe in this premise, where we all have the power to be heard and to provide an alternative to the mainstream news we hear every day. But, again, this concept is tainted when we legitimize sources by default. When all of our media comes from a single mainstream outlet, whether it's

Pravda, CNN, or Fox News, we're going to only get certain stories. Others simply won't be covered. And we will likely be influenced by their bias - and they *all* have bias. Knowing this simple fact is often enough to get someone to seek out other perspectives. However, today's landscape is such that *literally* anyone can become the media on platforms like Facebook without having any actual journalistic ability, other than the desire to get a particular message out. This is hardly the same concept as alternative voices becoming the media by shining light on ignored items with verifiable information. Instead, it's basically agenda-driven individuals making up stories to influence large crowds of people, who then go on to legitimize them through numbers instead of facts. Often, artificial intelligence is used to help spread the word. And it's working - because we don't question it enough.

We often hear the phrase "everyone is entitled to their own opinions, but they are not entitled to their own facts." Yet, this is precisely what we are faced with when people only rely on news and information from sources like Facebook, where literally anything can be packaged as news. When people get their information on such health hazards as coronavirus primarily from sites with absolutely no standards, the results can be catastrophic. In the hands of the dishonest and/or uninformed, the potential for danger is staggering if we treat such sources with the same seriousness as we do the ones that have been vetted as legitimate and knowledgeable. Literally anything can be presented as the truth if it has a fairly polished look and is spread around by enough of us: flat-Earthers, lizard people (look it up), anti-vaxxers, etc. (There are a lot more examples we could cite, but we honestly worry that so many already take them seriously that word would get out and we'd be dealing with angry responses for months.)

Legitimacy needs to be earned over time and what we are seeing in social networking runs counter to that. Facebook allows you to connect with all kinds of friends and relatives who can then bombard you with "news" items that look real without being checked for accuracy, resulting in all sorts of misinformation being spread around with very little opportunity to refute it. On platforms like Twitter, mysterious algorithms decide whose words resonate more while others are ignored completely. Twitter alone decides who is legitimate (they call it "verified") and who isn't, even though they themselves have no real standing to do this. The result of such arbitrary authority is an environment where it's not about what people are saying but rather *who* is saying it. So instead of fulfilling what could have been an opportunity to be a great equalizer, Twitter has become just another echo chamber for the elite, while the rest of us struggle to get any message at all out.

And this brings us back to the unwarranted seriousness that people afford these services. We saw it with early websites that were easy to hack into. Now we're seeing people charged with crimes for figuring out how to take over Twitter accounts - but only the "important" ones. That very sentence 20 years ago would have seemed absurd. Now it's our reality. But all the wishful thinking in the world won't make an Instagram posting or a bunch of tweets into anything more than what they are: a temporary means of conveying a message that may or may not have come from the source indicated and which will likely be forgotten after a day. When we say it like that, its actual importance is defined much more accurately. Sure, there are people and companies who take their social network presence super seriously and would easily see its compromise as equivalent to an actual armed robbery. *That* is what the real problem is that we need to address and fix. In much the same way we used to tell people to relax if they found themselves kicked out of an IRC channel because "it's only IRC," we need to do the same thing with the various communication methods of today's social networks. They can be great, but they're no substitute for real life interactions or secure communications. Once we put all that into perspective, they will lose the undue power they're having over so many of us - which is precisely what those invested in these platforms *don't* want.

It's easy for us to say that these services are letting us down in so many ways, despite the positive features they give us. What's difficult is designing something better. Consider that in all of this critique, we haven't even touched upon the tracking and privacy intrusions we're all subjected to whenever we sign into one of these networks. We can and must do better. In all likelihood, that next generation of social networking will come from within the hacker community, as we tend to have a keen sense of the value of privacy, the threats of blindly following anything or anyone, and the undying importance of the individual. What we have now illustrates very clearly what the dangers are and gives us an all-too-brief look at the positive potential of the social networking project. And, as with any project, revisions, upgrades, and rewrites are inevitable.

Cracking Your Neighbor's Wi-Fi for $180

by zeitgeist

Back in the days, when wardriving was still a thing, Wi-Fi networks were not as common as today and a lot of them were open. Wireless security was in its infancy and WEP was - if at all - used as a security measure so that not every random stranger would hop on your network. I remember driving around the city with my buddy Mac in the car, the Orinoco Gold card in the laptop and an antenna on the roof of the car, trying to find Wi-Fi networks. These were the good old days.

But I am not one to look back and wish for these old days back. I am glad that almost all wireless networks are now secured with WPA2 or (especially in corporate environments) even better means of security. But your neighbor's Wi-Fi will most probably just have WPA2 as a security measure in place and it's leaking its radio waves into your apartment. So why not try to have fun with it from the comfort of your couch? Of course, you will inform your neighborhood buddy who owns the Wi-Fi that you are trying to crack before starting. Do not attempt anything illegal - circumvention of a security measure is in most jurisdictions a felony of some kind.

But how do you attack a WPA2 encrypted network? Fortunately, it's much more difficult than attacking a Wi-Fi network secured with WEP, which only takes seconds to decode after sniffing the traffic for a couple of minutes. Let's take a look at the theory of how WPA2 secures your network before attempting to pry it open.

When a client joins a WPA2 encrypted network and the secure connection is established, a process called the four-way-handshake is initiated. This four-way-handshake is initiated for two reasons, the first reason being so that client and access points can prove to each other that they know the password to the Wi-Fi network - or more commonly known as the pre-shared key (PSK) - without ever transmitting the PSK itself. The second reason is to negotiate the WPA encryption keys which are used for the secure communication between access point and client for the duration of the session, i.e., for the duration that the client is on the network. Once the four-way-handshake is successfully completed, a client is said to be authenticated for the network and can start sending and receiving packets to and from the access point. The four-way-handshake is always initiated by the access point, not the client. This will become important later.

The four-way-handshake can easily be sniffed by an attacker that is in range of the wireless signals of the network. It is merely four packets being transmitted over the air between client and access point. Once an attacker has sniffed and recorded these four packets, they can be cracked by means of dictionary or brute force in order to get the PSK.

As an attacker, you now have to just sit and wait for a new client to join the network you try to attack. When you are dealing with your neighbor's Wi-Fi, you can just sit on the couch and wait, but it might be a while.

In 2016, a group of Belgian researchers came up with a way of increasing the likelihood of an attacker being able to sniff the initial four-way-handshake. They do this by watching already authenticated clients on the wireless network and sending back a fabricated third step of this four-way-handshake on behalf of the client. This will deauthenticate that particular client from the network. Once the access point notices this, it will start to reinitiate the four-way-handshake with this client, thus increasing the likelihood of a four-way-handshake being sniffed by an attacker.

There are a number of tools with which you can catch these four-way-handshakes and also deauthenticate clients from the network. The most common ones that I have seen are Kismet, airodump-ng, or Wireshark. But I have come to love the versatility and flexibility of using Bettercap. Bettercap is like a Swiss army knife for performing attacks on all kinds of networks - wired and wireless. Bettercap also offers the possibility to deauthenticate clients from the network, but it is a manual process. The creator of Bettercap has come up with a fun tool called Pwnagotchi, which uses AI to carry out the attack using the scripting capabilities of Bettercap. On top of that, it offers a fun interface, you can carry it around just like a Tamagotchi (if you remember those from the time when wardriving was still a thing). Sniffing the four-way-handshakes with Pwnagotchi is really fun and effortless. Wardriving now becomes warwalking, with the added benefit of capturing four-way-handshakes while walking around your neighborhood. It's also good for your health to take long walks!

The next step after acquiring the four-way-handshakes is to crack these. Brute force cracking or performing dictionary attacks is no fun on regular machines that you normally have available. If you are into serious cryptomining, then you might have a machine in your basement that you can use for that, but for everyone else, there is the joy of cloud computing.

Using AWS, there are special instances that have GPU cards available to them. I would recommend going with a p3.16xlarge instance in order to get the most out of your cracking. Be careful though: you get the power of eight GPUs with 128GB GPU RAM (and 64 regular CPUs and 488 GB RAM, but we are not interested in that) for $24.48 per hour. So keep an eye on those machines and spin them down as soon as you do not need them any longer.

Once you have spun up this wonderful piece of virtual hardware with your choice of a Linux operating system (the following tutorial assumes Ubuntu, but should be easily adaptable to any flavor), you will need to install some additional software on it.

Install packages to compile and build packages on your machine:

```
sudo apt-get update && sudo apt-
➥get install -y build-essential
```

Next, download and install the Nvidia Tesla drivers (please note that the URLs might be different, depending on when you read this article):

```
wget http://us.download.nvidia.
➥com/tesla/410.104/NVIDIA-
➥Linux-x86_64-418.87.run
sudo /bin/bash NVIDIA-Linux-x86_
➥64-418.87.run --ui=none --no-
➥questions --silent -X
```

You can verify that things are working as they should:

```
sudo nvidia-smi
```

You should be getting some output that represents the number of virtual GPUs that you have available.

We are going to perform the attack using the Hashcat utility. So, we need to download it from their site and extract it:

```
wget https://hashcat.net/files/
➥hashcat-5.1.0.7z
7za x hashcat-5.1.0.7z
```

Pwnagotchi captures the packets which contain the handshakes in the standard pcap file format. Hashcat does not directly understand the pcap files that you have now - they need to be changed to the hccapx format. The simplest way of doing this is through a convenient website that the Hashcat people provide, it will also tell you if the handshakes found in there are any good:

```
https://hashcat.net/cap2hccapx/
```

Once the hccapx file is available on the system and Hashcat is installed on your AWS instance, you can perform different types of attacks on it. A very basic dictionary attack with a wordlist would be done in the following way (where capture.hccapx is the converted pcap file and rockyou.txt is the file of your wordlist):

```
hashcat -m 2500 capture.hccapx
➥rockyou.txt
```

If you are just a script kiddie who does not care about the inner workings of the wonderful Hashcat utility, then the tool naive-hashcat is for you. It will take care of everything for you by making educated guesses about how to crack your captured data.

Clone it:

```
git clone https://github.com/
➥brannondorsey/naive-hashcat
cd naive-hashcat
```

Download a pretty good dictionary file to feed to naive-hashcat:

```
curl -L -o dicts/rockyou.txt
➥ https://github.com/
➥brannondorsey/naive-hashcat/
➥releases/download/data/rockyou.
➥txt
```

Start the cracking:

```
HASH_FILE=capture.hccapx POT_
➥FILE=hackme.pot HASH_TYPE=2500
➥./naive-hashcat.sh
```

Now I would suggest running the above command in some form of virtual terminal that you can disconnect from. I like to use tmux for this. Once the job is started, go out and kill some time because this surely takes some.

When done, the password will appear in the file hackme.pot. It's a colon separated list, one wireless network per line, the last column of every line contains the password to the wireless network you have attacked if successfully cracked.

During my testing in preparation of this article, the process of cracking took a little more than six hours, which left me with an AWS bill of roughly $180. You will have to decide yourself if spending this amount is worth the result that you get out of it... just be sure to power the AWS instance down again after you are done with your experiment, otherwise you will lose some serious money.

Big shout outs to my buddy macglove!

▸ Data Transfer		$0.00
▾ Elastic Compute Cloud		$0.00
▸ No Region		-$182.85
▾ EU (Ireland)		$182.85
Amazon Elastic Compute Cloud running Linux/UNIX		$182.84
$26.44 per On Demand Linux p3.16xlarge Instance Hour	6.915 Hrs	$182.84
EBS		$0.01
$0.00 for 14 Gbps per p3.16xlarge instance-hour (or partial hour)	6.915 Hrs	$0.00
$0.11 per GB-month of General Purpose SSD (gp2) provisioned storage - EU (Ireland)	0.078 GB-Mo	$0.01
▸ Key Management Service		$0.00
▸ Relational Database Service		$0.00

HaxOrz? Sniffing My Critical Infrastructure?! It's More Likely Than You Think!

by Tim Tepatti, tim@tepatti.com

Part One: Building a V2X Wardriving Box for $200

If you haven't heard, both cars and Wi-Fi are going through big changes! A spicy new topic has been racing through the automotive industry: the 802.11p standard! An extension to the 802.11 standard which will add "Wireless Access in Vehicular Environments" or "WAVE."

Why is this spicy, you ask? Because this new 802.11p standard was introduced with the plan of connecting *every* car, heavy truck, traffic light, street sign, road sensor, etc. to the Internet.

Oh boy! Nothing could go wrong with connecting critical infrastructure to the Internet, right?

....right?

So if I didn't have your attention before, hopefully I do now! There's one major problem with these new standards, though: There's not enough community information on them! Sure, you can go buy the IEEE standard. Sure, you can go look for engineering documentation. But there's no easy way for security researchers to actually get their feet wet with these new wireless standards in a simple way!

That's where I have to give credit to Harrison Sand[1]. He published an amazing blog post fully detailing his forays into V2X (Vehicle-to-Everything) sniffing. After reading it, I immediately:

- Built my own V2X sniffer
- Thought: "How can I spread this information to the masses?!"

This article will speed run you through building your own 802.11p wardriving box, and hopefully answer some questions on how 802.11p works along the way! It builds off of Harrison's wonderful work, but tries to speed you through the small details to get you up and analyzing faster. If you really want to do a deep dive into these new protocols, I'll add some handy keywords to search at the end. Side note: If you're an automotive engineer who is disgusted at me breezing over small details, feel free to email me! I'm always down to hear critiques and publish errata.

First, some background. Let's get the acronyms out of the way. Depending on what part of the protocol or standard you're looking at, the names could differ. DSRC is the technology name, standing for Digital Short-Range Communications. 802.11p is the physical and MAC layer. WAVE is the application layer, which stands for Wireless Access in Vehicular Environments. The basic use case of DSRC is cars being able to communicate the road situation to each other to avoid accidents and increase overall safety. Example: Your autonomous vehicle malfunctions and the camera breaks. Oh no, you can't use computer vision to recognize the color of the traffic light anymore! No problem, the traffic light ahead is broadcasting its status over DSRC/802.11p! Now your car knows the light is red and is able to brake. It's a built-in redundancy layer to go with the rest of the sensors in the vehicle. While it hasn't been put into any current generation cars, many companies are banking on the technology. In 2018, General Motors stated that they planned on rolling out V2X to a portion of their vehicles by 2023. That's only a few years away! Plus, you can find your own sensors placed around town that are still under development, but live and broadcasting....

Now, the technical goodness! DSRC is in the hella high gigahertz, yo! It uses the 75MHz spectrum between 5.850 and 5.925GHz. This means you can't use traditional Wi-Fi hardware, as most only does 2.4GHz to 5GHz! Or uh, well - you can, you just need to use one that has hacked firmware and 5.9GHz capabilities. We're going to be using a modified Wi-Fi card and a custom-built Linux kernel to create our sniffer. For software, we'll just be relying on Wireshark and tcpdump. Easy-peasy!

Hardware

- PC Engines APU.2D4 System Board w/ 4GB RAM
- Blue Enclosure - 3 LAN, USB (you can pick any color!)
- 12V U.S. Plug AC Adapter (don't buy the U.S. plug if you're not in the U.S.)
- SSD mSATA 30GB MLC Phison (pick a size to your liking - I like 30GB)
- Compex WLE200NX miniPCI Express Card (our 5.9GHz Wi-Fi!)
- Cable I-PEX -> Reverse SMA (x2)
- Adapter USB to DB9F with USB Cable (for connecting over serial)

Total Cost: ~$203.40 USD

The main reasons for choosing this hardware are:

- We need a computer that can use a miniPCI Express Wi-Fi card
- We need it to be portable, something you can throw in your trunk

I ordered all of the above from pcengines.ch - they're a great embedded hardware developer from Switzerland. While the shipping may take a week or two to get to the United States, I was able to order everything I needed in one purchase. Alternatively, if you have a laptop with a miniPCIe slot on it, you can forego the APU entirely! Just pick up the WLE200NX and you'll be able to mess with 5.9GHz Wi-Fi. Unfortunately, I won't be able to help you compile Linux for your laptop's architecture.

The only thing I would recommend buying in addition to the APU are some magnetic mounted high-gain antennas. I opted for a cheap-o set of 7dBi magnet-mounted RP-SMA antennas from Amazon. I chose ones that had two coils mid-antenna, since the overall shorter length makes them stand out less when on my car.

Software

We need to build our own kernel for this step. We're going to use OpenC2X (again, props to Harrison Sand for the recommendation!) and we'll need to be running Linux for the build environment.

First, install dependencies:

```
sudo apt install git build-essential libncurses5-dev zlib1g-dev unzip python
```

Clone the OpenC2X embedded git repo:

```
git clone https://github.com/florianklingler/OpenC2X-embedded.git
```

Update the feeds:

```
cd OpenC2X-embedded
./scripts/feeds update -a
./scripts/feeds install -a
```

Create kernel configuration file:

```
./create_config.sh x86_64
make defconfig
```

Bring up kernel configuration menu:

```
make menuconfig
```

Then, select all of the following to add to your kernel:

```
Network > tcpdump
Network > firewall > iptables > iptables-mod-tee
Network > Time Synchronization > chrony
Utilities > strace
Utilities > grep
Utilities > Shells > bash
```

Build OpenC2X, where X in -jX is your core count+1:

```
make download
make -jX V=s
```

(for my poor single-core Centrino, I was running -j2…)

Now you just wait a million hours and your finished OpenC2X Embedded image will land in ./bin/targets/x86/64/.

Now we just need to flash it onto the APU2. To do this, we'll use the PC Engines recommended method of making a bootable TinyCore Linux USB.

To do so, download the file TinyCore6.4_2017.tar.bz2 from the PC Engines website[2]. Unzip it somewhere like Documents or Downloads - you'll need to copy these files later.

Next, insert a blank flash drive into your computer. Install GParted and syslinux:

```
sudo apt install gparted syslinux
```

Open GParted, select your flash drive and click "Device' -> 'Create Partition Table". Your device will now be 100 percent free space. Right click on the unallocated space and click "Create new Partition". Increase the size until it takes up all of the unallocated space, and set the File System to FAT16.

Now, you'll need to make the flash drive bootable using syslinux. Open up a terminal and type "df -h" to find the block name of your flash drive. If you only have one HDD (/dev/sda1), the flash drive will most likely be /dev/sdb1. *Always* be sure to check the size of the device to ensure it matches the flash drive you inserted. If you accidentally fuck with one of your HDDs, you won't have a good time!

Since my USB is located at /dev/sdb1, that's what I'll be using.

```
syslinux -i /dev/sdb1
```

The -i flag will install it on your flash drive, and if you browse your flash drive in your file browser, you'll see new files: ldlinux.sys and ldlinux.c32. At this point, we're ready to copy the TinyCore files! Open up your file browser and browse to where you extracted the TinyCore Linux archive from the first step, and copy all of the extracted files to the root of your flash drive.

Your USB should now contain:

```
autostart.sh
core.gz
ldlinux.c32
ldlinux.sys
syslinux.cfg
vmlinuz
```

We need one last file! Copy your new

OpenC2X image over to the flash drive as well. It's located in your OpenC2X Embedded folder at ./bin/targets/x86/64/ and should be called "lede-x86-64-combined-ext4.img.gz".

Plug the APU into your computer using the included DB9 to USB adapter and connect to it with the following command:

```
minicom -D /dev/ttyUSB0 -b
➥ 115200
```

(If you don't have minicom, just `sudo apt install minicom`)

Plug your TinyCore Linux flash drive into the bottom USB port on your APU and turn it on. Your minicom console should come alive and you'll be root!

Browse to the root of your USB (should be /media/TINYCORE/, but it may differ based on your flash drive) and run the following commands:

```
gunzip lede-x86-64-combined-
➥ext4.img.gz
dd if=lede-x86-64-combined-
➥ext4.img of=/dev/sda bs=4M
sync
```

Congrats, you've flashed OpenC2X! Remove your USB and reboot, and you should boot directly into LEDE.

Capturing Packets

I highly recommend making scripts for this part. You're going to be performing four basic steps to start capturing packets:

- Bring up your Wi-Fi interface
- Enable monitor mode on the interface
- Rotate your frequencies to jump between possible broadcast frequencies
- Run tcpdump to capture packets to a pcap

I've broken it down into three scripts and one command:

bring_up_interfaces.sh:

This script will set up the wireless interface and join the OCB network. The "5900" designates the 5.9GHz band. Once you run this, you can use "iw phy0 info" to ensure that it's working correctly, along with "iw wlan0 info"

```
iw reg set DE
iw dev wlan0 set type ocb
ip link set wlan0 up
iw dev wlan0 ocb join 5900
➥ 10MHZ
```

enable_monitor_mode.sh:

We want to enable monitor mode so that we can capture packets using our APU. This script will put both of the wireless interfaces into monitor mode, just to be safe.

```
iw dev wlan0 interface add
➥wlan1 type monitor
ifconfig wlan1 up
# Enable promiscuous mode (not
#sure if this is necessary on
#both interfaces, shouldn't
#hurt either way)
ifconfig wlan0 promisc
ifconfig wlan1 promisc
```

freq_rotate.sh:

This script will rotate through the channels located in freq.txt. This is to get proper coverage of the entire 802.11p spectrum, not just a single channel. This script has to stay running in the background while you run tcpdump.

```
#!/bin/sh
# Credit to Harrison Sand
# All I did was modify it to
#infinite loop
iw dev wlan0 ocb leave
while :
do
 for freq in $(cat freq.txt);
➥do
  echo "$freq 10MHZ"
  iw dev wlan0 ocb join $freq
➥10MHZ
  sleep 1
  iw dev wlan0 ocb leave
  echo "$freq 5MHZ"
  iw dev wlan0 ocb join $freq
➥ 5MHZ
  sleep 1
  iw dev wlan0 ocb leave
 done
done
```

freq.txt:

This is a list of the different channel frequencies within V2X/802.11p. For usage with freq_rotate.sh to jump between the different frequencies.

```
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
```

The final step is to run tcpdump. This is the tool that will actually dump our packets into a pcap file that we can later analyze with Wireshark.

It's recommended that you have two tcpdump sessions running - one to send packets to a pcap file, and the other dumping packets to the terminal, so you can stay aware of what's going on. Those two commands are listed below.

```
# output to pcap for later
#analysis in Wireshark
tcpdump -s 0 -i wlan1 -w foo.
➥pcap
# output to console
tcpdump -i wlan1
```

And congrats, now you can capture pcaps! I highly suggest throwing your APU in your vehicle and driving around town to hunt for V2X devices. I was able to find dozens of devices installed around me, usually around automotive suppliers and manufacturer's facilities. From here, you can also expand the scripts and commands that were given. Make them start at boot, or even parse the packets and react to them in some way. The APU runs Linux, so the world is your oyster.

In Part 2 of this article, I'll go over how to parse the results of your sniffing in Wireshark, along with a summary of the current V2X device and transmission security that's been proposed. In addition, I'll share a few thousand packets that I've captured around town from a few dozen V2X devices so you have some data to play with, even if you can't sniff any devices near you.

For now, I'll leave you with some handy keywords for aiding your research:

V2X, DSRC, OSB, IEEE 1609.3-2016, SAE J2735, IEEE PSID Public Listing

As always, if you have any feedback, feel free to contact me. I'm always open to suggestions or the possibility that I was wrong about something. Happy hacking!

[1] harrisonsand.com/802-11p-v2x-➥hunting/

[2] pcengines.ch/file/TinyCore6.4➥_2017.tar.bz2

Null-Routing Facebook: Using Small Tech to Fight Big Tech

by aestetix

I really hate Facebook. Part of this hatred is a general dislike of "social" media websites which pollute and destroy civil discourse with haphazard policies and elusive "algorithms," but Facebook takes the evil to the next level. In this article, we'll explore how they do this, and what you can do to fight back.

This evil began when Facebook got into the business of mass surveillance, starting with a website widget. According to them, we could add "one line of javascript" to our website, and it would magically enable people to like and share things like blog entries that we had written. This later expanded into other technologies, such as single-sign-on, where we could enable people to use their Facebook accounts to "log in" to our website and use our services.

But there's something that Facebook didn't mention. Every time a web browser makes a request to a website, it requests all the resources on the page, such as images, CSS, and so on. Including that "one line of javascript," which makes a request to a Facebook URL and downloads javascript that enables the promoted functionality. And every time our web browser makes a request to Facebook, it creates a log entry on Facebook's servers with all sorts of information, such as our user-agent and our IP address. For every website we visit that has this functionality enabled, Facebook can track us, even if we don't have a Facebook account.

This is probably how Facebook collected the data that became "shadow profiles." The public first learned about these through a public information request by Max Schrems in 2011 (details at europe-v-facebook.➥org). These shadow profiles - secret dossiers about people's Internet browsing activities compiled without their knowledge or consent - have been the source of a lot of controversy, even coming up in Congressional and Parliamentary questioning, although Facebook refuses to address any concerns.

While the Internet was designed to route around censorship, it was also designed to route around surveillance. When the web browser requests an

asset, such as a javascript file, it has to perform a domain name resolution to a domain name service (DNS) because computers don't really read domain names. When we type facebook.com into the browser, the browser will look in our local DNS cache to find the IP address that matches facebook.com. If there isn't one cached, it will make a request to a DNS server with the domain, and the server will reply with a corresponding IP address. The browser will then put this in its cache and use the IP address to access the website.

In recent years, as websites filled up with annoying and distracting ads, people have started using ad blockers to prevent the browser from displaying the ads. As of this writing, the problem is so bad that it's effectively unsafe to look at most websites without using an ad blocker. And for those of us who don't want to rely on a browser-based solution, we can use Pi-Hole (`www.pi-hole.net`). Designed to run on a Raspberry Pi, Pi-Hole is a self-hosted standalone "ad blocker" that runs at the DNS level, ensuring that requests to known bad websites don't even resolve. This also means that the requests never make it to the servers, so the bad websites can't track us.

Pi-Hole has a great feature: it lets us whitelist and blacklist sites. Although we can do this on our local computer by modifying the hosts file (for example, setting facebook.com to point to localhost), the hosts file doesn't support wildcards. Pi-Hole, using dnsmasq as a backend, does. And we can use this feature to blacklist every URL with a hostname relating to Facebook, allowing our system to null-route all such requests, making ourselves effectively invisible to Facebook's all-seeing eyes.

Using some simple regular expressions, we can block out a multitude of Facebook URLs, as well as their Content Delivery Networks. In my list, I'm also blocking out all Instagram URLs because they are owned by Facebook, as well as Twitter because, honestly, there are very few good reasons to ever look at Twitter. You can put whatever websites you want in here, and metaphorically tell those companies to go steal someone else's usage data.

Here is the list I use:

```
(^|\.)facebook\.com$
(^|\.)facebook\.net$
(^|\.)fbcdn\.net$
(^|\.)fna\.fbcdn\.net$
(^|\.)ftxl1-1\.fna\.fbcdn\. net$
(^|\.)instagram\.com$
(^|\.)tfbnw\.net$
(^|\.)twitter\.com$
(^|\.)xx\.fbcdn\.net$
```

Once we've set up Pi-Hole, the last step is to get our system to use it as our default DNS. On Linux systems, this is usually the /etc/resolv.conf file. The easiest way is to add a line such as:

```
nameserver 192.168.0.2
```

above our automatically assigned nameserver, where 192.168.0.2 is the IP address of our Pi-Hole server. If you have the means, I recommend installing Pi-Hole on a cloud VPS, because then you can block Facebook no matter where your computer is. It's worth noting that some systems, such as Ubuntu, automatically generate the resolv.conf files, so you should probably figure out how the system makes it (if it does), and modify the template files so you don't have to re-add the line every time you connect to a new network.

A few more technical notes. First, disable logging. Pi-Hole logs how many requests it blocks and has pretty graphs, but if you don't care about that, it can slow the system down and waste disk space. I also turn off the webserver (`sudo service lighttpd stop`) because I don't need to look at the graphs. Second, if you visit a lot of sites with Facebook embeds, your DNS resolution might take longer and longer over time due to DNS caching, causing all your web browsing to be fairly slow. You can verify if Pi-Hole is causing slowness by running the command from your local shell: `$ dig facebook.com`. If the response is an instant 0.0.0.0, Pi-Hole is working as expected. But if the response takes forever to resolve, then it is probably overloaded. To fix this, log into the server, and run `$ sudo pihole restartdns`. This will clear the Pi-Hole logs and make your system run smoothly again. It's a little annoying, but it's a small price to pay for privacy.

There is a major technology war afoot, and there are big questions about whether we even own our own data. As someone who believes strongly that an individual's right to privacy overrides a corporation's desire to sell that privacy to the highest bidder, I think it is important that, when we are able, we should use technology to ensure that our data cannot be bought, especially without our consent. After all, what these corporations do not have can only make us stronger.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's spring, my least favorite time of year because I'm sneezing up a storm. Tree pollen always hits me the worst, and it starts the earliest and goes the longest. Of course, given the coronavirus panic here in the Puget Sound area, every time I sneeze, people around me give me worried sidelong glances. So, my work is taking on particular urgency since it's entirely possible that I could be quarantined at any time! I'll get to it right after I finish my break and a little "service monitoring" of the local ambulance company.

Today, we're running a test of our exchanges in the 564 area code overlay in western Washington. "Wait a minute," you might say. "564? Is that even a thing? And what's an overlay, anyway?" You'd be correct to note that there are nearly no *subscribers* with numbers in the 564 area code. However, the infrastructure is in place, test numbers exist, and phone companies have even laid claim to some of the best exchanges. Other than an annual exercise to ensure that calls are still routing, the 564 area code continues to lay mostly dormant - but not for long.

Since their inception, area codes were historically assigned by the Bell System to a fixed geographic area via the NANPA, or North American Numbering Plan Administrator. Exchanges were further historically assigned 10,000 numbers at a time. Growth in new area codes was slow and steady, and the original design of the area code system (which used three-digit numbers from 201 to 919, with only a 0 or 1 in the middle) allowed for plenty of growth, which mostly tracked the growth of the population in North America. Decades went by without many changes in area code maps. The name of the company running NANPA changed to Bellcore in 1983, but the people doing the work, for the most part, didn't. They were drawn from Bell Labs and the regional Bell companies after the breakup of the Bell System.

The area code landscape began to change in the late 1980s with the introduction of competitive local exchange carriers, pagers, faxes, voicemail, VoIP, and cellular phones. This massively accelerated in the 1990s as people went from having one or two phone numbers to five or more (such as a home line, modem line, business line, fax line, and mobile phone), and from doing business with one phone company to - in some cases - several. In fact, from the 1990s until the early 2000s, hardly a month went by without an area code split somewhere in the North American Numbering Plan (which is the parts of the U.S., Canada, and the Caribbean represented by country code 1). New area codes marched across the country, usually issued in "geographic splits." Despite reclaiming a handful of area codes from telex services (which were retired), and despite pushing Mexico's Telnor out of the North American Numbering Plan and into country code 52, NANPA ran out of area codes using the historical format in 1995. Two new area codes, 360 and 334, were introduced. And now, despite number conservation measures, area code 360 is nearly exhausted and will be overlaid by a new area code, 564.

Before we get to that, it's worth reviewing a little history. Long distance used to be a *very big deal* - calling outside of your local area was expensive (often very expensive) and generated large profits for phone companies. Area codes always had a 0 or a 1 in the middle, could never have the middle digit at the end (so for example, no 200 or 211), and for the sake of convenience, it was a generally accepted convention not to assign the same numbers to exchanges as existing area codes. The reason for this was when making long distance calls within the same area code, you generally only needed to dial a 1 (for long distance)

plus the seven-digit number. However, allowing this convenience meant that *fully 144 exchanges* had to be reserved (every potential area code, meaning every number with a 0 or 1 in the middle from 201 through 919), because otherwise there would be no quick way for the phone system to differentiate between long distance calls within the same area code (using 1+seven-digit dialing) and long distance calls to another area code.

With the explosive growth in phone numbers, the generally accepted solution was simply to do a "split." Along a geographic boundary that was defined by telephone rate centers, NANPA would propose to split an area code in two. For example, in 1959, the 415 area code was split into 415 and 408. However, splitting an area code created a major disruption for people each time they were forced to move to another area code. Business owners had to update business cards, stationery, and advertising. People had to notify their contacts of the new area code as well. And bear in mind, this was in an era where the normal way to update people was either to make an expensive long distance toll call or send them a letter in the mail!

Prior to implementing a split, a number conservation method was possible: over 1.4 million phone numbers could be freed up by assigning the same numbers to exchanges as used by area codes. However, this forced a change to dialing patterns: eleven-digit dialing became required for all long distance calls (1-NPA-NXX-XXXX). You should have heard the howls of protest from owners of fax machines that this decision caused in the business office, but it allowed us to conserve the 206 area code for much longer than would otherwise have been possible. Moving to 11-digit dialing for all long distance calls further enabled the adoption of area codes without a 0 or 1 in the middle, so area codes like 360, 253, and 425 (three of the four area codes currently in use in western Washington, along with the 564 overlay) became possible.

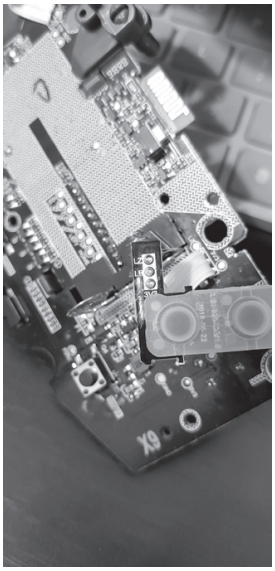
There is another problem that can be solved by conservation: filthy CLECs and tiny providers wasting entire exchanges on a handful of customers. The Telecommunications Act of 1996 created a massive explosion of companies who were allowed to ask for number assignments from NANPA. Naturally, it was almost free to get these, and there was no requirement to have any real subscribers, so every CLEC, paging company, mobile phone company, VoIP provider, and who knows what else snapped up exchanges for their potential (but nonexistent) customers, quickly exhausting area codes. Limiting assignment to "thousands block," where numbers are assigned by NPA-NXX-NXXX instead of NPA-NXX-XXXX meant that instead of wasting 10,000 numbers, small providers would "only" waste 1,000 numbers.

Number conservation, however, only goes so far and eventually the growth does require either a geographic split or an overlay. What's an overlay? That's what we are doing with area code 564. It's just an additional area code for the same geographic territory, meaning that nobody has to change their existing phone number. When the 360 area code is eventually exhausted (it's very close to exhaustion, but has been managed closely with number conservation procedures), telephone service providers will start assigning new numbers in the 564 area code. However, this creates another problem: seven-digit dialing doesn't work anymore because local calls can be in both area codes. In 2017, 10-digit dialing was mandated in the 360 area code to enable the 564 overlay. This created fewer problems than expected because it had been *supported* for years prior, and these days, most subscribers are calling on mobile phones (which require 10-digit dialing) instead of land lines. Although area code splits are still possible, the loss of seven-digit dialing is far less of an issue for subscribers than it once was. Many state public utility commissions, in fact, have mandated that future area code introductions *must* be performed as an overlay.

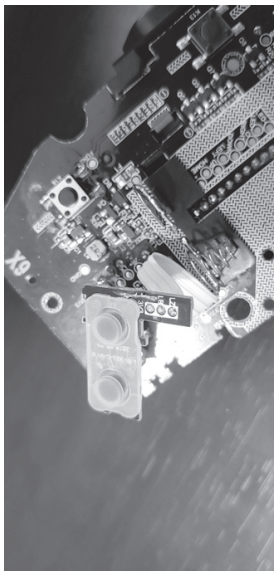
And with that, my test just passed, and my "service monitoring" just revealed that another friend is heading to the hospital. I won't be visiting - but HIPAA be damned, I'll be calling from a land line phone! Stay healthy this spring, and the next time a call doesn't work from a land line by dialing only seven digits, you'll know why!

Hackerspace School

Broken



Ready to fix



Fixed!

by RAMGarden

After reading the letter in the Summer 2018 edition of *2600* about having to hack Blackboard software just to get around the rigid structure of school and the curriculum to match the student's learning style, I came up with this idea. Instead of fighting the system to change it, why not supplement your learning after and outside of school? The best place I can think of is at your nearest hackerspace or makerspace. They usually have free classes that are totally unstructured or at least slightly formal in that there is definitely a set topic. The main idea with learning at a hackerspace is that everyone is basically learning from each other all the time even if not in a specific class or lesson. If you see someone is working on a project and welding something together, you can ask them to teach you how to weld. You don't want to stop them in the middle of their work, but they will most likely explain what they are doing as they go. You can then set up a different time later for them to show you and let you weld some scrap metal to get the hang of it.

If you see someone working on 3D printing, you can ask them to show you how to design something in CAD and print it. Or, in my most recent real world case, I dropped my Nintendo Switch wireless controller and it landed on the trigger button. That button no longer worked and of course it was out of warranty. So, instead of throwing it away and buying a new one, I went to my local makerspace and got some help from some of the electrical engineering members. We took it apart and found that the shoulder button and trigger press buttons on a small printed circuit board. The edge of the plastic trigger had cracked the edge of the PCB and broken the copper trace that connected the LZ button to the hole where the wire was soldered into that connected the small PCB to the main board. They taught me how to use a knife to scratch the coating (solder mask) off the top of the trace to expose the copper underneath. I then soldered a very small scrap wire across the broken gap.

Another great part of a makerspace is having scrap wires and parts like that on hand. They also taught me how to use the multi-meter to test the continuity between the connection points. After pinching on some alligator clips and pressing the little button on the small PCB, I could hear the meter beep each time I pressed the button. Screwing it all back together and testing it out proved it was indeed working great again!

I was able to not only learn a new skill and fix my own broken controller, but it was all free and I didn't have to sign up for any class or other structured lesson!

To pay it forward, I help teach others how to program and build desktop, web, and mobile applications and games during our weekly Code Jam events every Saturday. Free and open to the public! I also help with our Coder Dojo (`coderdojo.org`) where we teach kids how to program and some-

times even make robots (melbournemaker➥space.org/2018/12/coder-dojo-➥robotics-class-recap/).

By simply hanging out at your local hackerspace, you can accidentally learn new skills and things you would never learn at school. I would recommend to anyone who's not getting what they need from school to do their assigned homework and do the normal school stuff but *also* hang out at the hackerspace after school and on weekends to learn the other cool stuff.

I also learned how to use the sewing machine to make the curtains for our house at my local makerspace. Then I was able to use the sewing machine to make simple costumes for a sixties-themed party. Since I broke the sewing machine by trying to sew through too many layers, I also learned how to *fix* the sewing machine after you break it! The next thing on my list to learn is how to use the metal forge to melt metal into molds to make my own custom metal parts to replace broken ones or create brand new parts for robots and other projects.

In conclusion, I highly recommend visiting your local hackerspace to learn new things - especially if you aren't getting enough from your structured schooling. And if you don't have a local hackerspace, you can find a few other like-minded individuals on meetup.➥com or other social websites and start your own!

The worldwide wiki for all hackerspaces can be found at wiki.hackerspaces.➥org/.

Learning Programming Through Hacking AOL
A Journey Through Hazy Middle School Memories of Discovering the Joy of Code

by Scott Stahl

My first taste of programming came in middle school. Middle school for me coincided with the mid 1990s, which was a bizarre time. *Hackers* was released in 1995, and was a land of unimaginable techno coolness to us suburban, basement-dwelling, NES-obsessed weirdos. *The Net* had also been recently released, and Sandra Bullock was playing *Wolfenstein 3D* and outhacking her pursuers. People were prefixing "cyber" in front of everything, and it actually seemed cool. I learned from the pop culture of the day that floppy disks were a portable currency, and I imagined carrying around a set of programs in my pocket like a Swiss army knife. *The Matrix* and the actual coolness it would bring to the Internet were an eternity away in 1999.

I had cajoled and convinced my parents to get a PC by around 1996, and we had that dangerous entrance to the Internet known as AOL by around 1997. Now I had access to the world, and I imagined myself a Kevin Mitnick or a Zer0 C0ol. Of course, I didn't know the first thing about what I was actually doing, but I had drive and a mischievous intuition. I quickly found my way into various chat rooms, which led to deeper chat rooms, which showed people passing around pirated programs, known as warez, which I had always pronounced like Juarez but I'm pretty sure in hindsight was probably like a merchant's wares but with a z for cool factor. And in this scene, you were surrounded by magical little Windows applications known as proggiez or progz.

Proggiez were typically written in Visual Basic, with names like AOHell, HaVoK, and Fate-X. They were the Swiss army knife on a floppy disk I had always hoped for. Progz had many uses, very few of them legitimate. There were phishing tools to try to trick users into giving you their passwords or billing info, there were scrollers that would flood chatrooms with text or ASCII art, there were chatroom responder bots, there were mass spam mailers, and there were punters. Punters sent HTML strings that would overload the poorly-written HTML parser in the receiver's AOL instance and kick them offline. Being kicked offline in the 1990s was a big deal. It took several minutes to open up AOL again and log back in, even with a top of the line 56k modem. Soon enough, progz would also come with anti-punters to neuter incoming punt strings. It was an arms race.

Once I stumbled upon this subculture, I became obsessed. I downloaded every prog I could find, evaluating them functionally and aesthetically. I was a prog snob. As 1990s fashion itself evolved from neon to black, progz evolved from big ugly flame-graphic buttons with 30 second intro videos by guys named XxHaCKeRxX to minimal cold blues and purples by lowercase unicode guys named

dárk råïn or whatever. I was in love with every piece, and I wanted to be a part of it.

Visual Basic 6.0 Enterprise seemed to be constantly available on warez sites, so I figured I'd give it a shot. I wanted to build badly enough that having no idea how to write code was not going to stop me. Like all warez, it came in 30-40 sequential RAR files that unzipped into a single install with a registration crack. I found myself a library of basic proggie functions that other people had written and distributed. All I had to do was deconstruct this bizarre language and figure out how to make things work. I spent hours every day during that summer of 1998 decrypting the obscure language in these VB files, figuring out how everything worked, and translating it into building my own prog. I was designing my perfect UI, I was implementing and tweaking functions from .bas libraries; I was building a prog of my own. I even put several encrypted passwords on it for higher access functions. Of course, no one but me ever used this application, but I was damn sure to build in five levels of security and ensured that I was the only one who would ever get full admin access. I was the admin of my own prog, and I could punt people with my own custom HTML strings. I tweaked the scroller for hours until I found the fastest possible speed you could send text before you got rate limited and booted offline yourself. And I felt invulnerable.

Did I almost get my family banned from AOL for life? Sure, several times. Did I end up talking my way out of it every time? Also yes. Like everyone else, our way out of AOL's walled garden was by choice, spurred on by the wide availability of broadband.

All the learning I would do on this journey would set me on the course I ended up on later in life. With the right tools and free time, I was able to skate just above the line of getting in real trouble while learning core programming skills. Fundamentally, I'm still doing the same thing today as I did with those VB building blocks: start with something someone smarter than me built, reverse-engineer it until I understand it, and go off on my own. I'll be forever thankful for the access and freedom I had in those days, and will treasure that time I spent learning and making mischief.

Major shoutouts:

- To this post by digital, the best reminiscence I've found of the progz scene and an inspiration to his post - `www.digital5k.com/aol-progz-a-digital-throw-back-to-aol-1995/`
- To this info dump of screenshots and information from that era - `justinakapaste.com/`
- To this list of progz, the closest thing I've found to a full list. Download at your own risk, though I'm doubtful any of the links even work. The names are definitely all real. `www.angelfire.com/ky/peschel/punters.html`
- To this technical walkthrough detailing writing progz in Visual Basic 3.0. Seeing that old VB code and UI is bracing. `charlesleifer.com/blog/a-stroll-down-memory-lane-scripting-aol/`

I recommend using `archive.org` to investigate broken links from the above.

Has Your Password Been Pwned?

by Jan Markowski, livetrue@pm.me

Passwords are a headache and, if you're anything like me, you have a handful with various degrees of complexity that you use, depending on the service. Lame-o subscription? Throwaway account with weak password. Bank account? Secure account with strong password.

Either way, how can you tell if your password, especially if you believe it's a strong password, hasn't been compromised?

Your first instinct may be to do a search, upon which you stumble across haveibebeenpwned.com, a service that allows you test if your password exists in a password list somewhere. But, it requires you to submit your precious "strong and secure" password... to a service you're not sure you can trust.... If you're like me, you're completely hesitant to do this. After all, how can you trust that the service, catered to non-technical folk, is not storing your password which then gets added to a compromised list or who knows what else? What if it's adding it to some insecure password database which risks becoming compromised itself? The honest truth is unless you're part of their security team maintaining the website, you can't be completely sure.

The good news is that there's another way! What if I said that you can test whether your password's been compromised without having to submit your password online?

The original author and owner of haveibeenpwned.com, Troy Hunt, has actually acknowledged that there are many people who share the privacy concerns over submitting their passwords using his online service. Paranoid folks rejoice! You are not alone!

So, to alleviate this concern, Troy has developed an online API that allows anyone, anonymously, to test their password using a method known as "k-Anonymity range search".

The basic premise is this: If you generate a SHA1 hash of your precious password, and then submit just the first five characters of this hash to the API, the API will respond with all the compromised passwords, in SHA1 form, that share those same first five characters.

Typically, you'll get back a SHA1 list of about 500 pwned passwords.

Using this list of about 500 hashed, pwned, passwords, you may now check to see if your precious SHA1 password appears (identically) anywhere in the list. If you do find an identical match, then you know that your password is not safe, and thus, not so precious! If your password's SHA1 does not appear in the list, then you can celebrate because you hold the secret sauce to a password that has not yet been pwned.

To save you the trouble, I've written a simple Linux bash script that uses the API and allows you to test your passwords:

```
#!/bin/sh

# Store the first argument
#with a name
password=$1

# Store the 40 character SHA1 hash
sha1=$(echo -n "$password"
➥| sha1sum | cut -c 1-40)

# Save the first 5 and last 35 SHA1
#chunks in separate variables
sha1_a=${sha1:0:5}
sha1_b=${sha1:5:40}

# Use the k-Anonymity API to
#fetch a collection of pwned
#passwords that share the same
#5 characters of the SHA1
sha1list=$(wget -q -O - https://
➥api.pwnedpasswords.com/range/
➥$sha1_a)

# Does our password's 35 character
#SHA1 chunk match any in the list?
echo $sha1list | grep --ignore-
➥case --quiet $sha1_b
rc=$?

if [ $rc -eq 0 ]; then
    echo "\"$password\" has
➥been pwned! Do not use!"
else
    echo "\"$password\" is safe :)"
fi
```

Save this file as "testpass.sh" and mark it executable:

```
$ chmod a+x testpass.sh
```

In a prompt, you can test your password by feeding it a password as an argument. For example:

```
$ ./testpass.sh MyPassword
"MyPassword" has been
➥pwned! Do not use!
```

or

```
$ ./testpass.sh 2600reader
"2600reader" is safe :)
```

Note that if you're using this script in your shell, the only issue is that it will exist in your shell history. You may be interested in purging your bash history as follows:

```
$ cat /dev/null > ~/.bash_
➥history && history -c && exit
```

Hopefully, this helps you with creating strong, uncompromised passwords, or otherwise gives you the much needed sleep knowing that the strong password you've been using over the past ten years hasn't (yet!) been pwned. Just remember to test your passwords every now and again!

Antique Malware Can Still Bite You
Investigating Malware in an Old File Format

by KoreyYoung

Many security analysts wouldn't think twice about ignoring and passing over a file with an antiquated file extension attached to an email. Many "ordinary" people would probably just ignore the file if they didn't recognize the extension. But your curious clickers might still try to open the file; and if they are on an old system, it could still detonate and cause damage. Now you might think that there is no chance that there are still old enough systems around to be able to open these antiquated files, but you would be surprised how many ancient systems are still hanging around to do a critical function that cannot run on an up-to-date system. So how would you, the part-time malware analyst, analyze an antiquated file if one got in and executed on your old, critical use computer? I say part-time malware analyst because a malware reverse engineer would still be able to easily dig into an antique file's binary to see what it does. But many cyber security teams do not have a malware reverse engineer on staff, and instead have to rely on malware sandboxes or visual inspection of the file's contents in a text editor.

The subject of this analysis is a .pif file that came into my email sandbox. Being a relatively young person, I had to look up what a .pif file was, because my Windows 10 computer did not recognize the file format. I found out that a .pif is an MS-DOS shortcut file, and it could be opened with MS-DOS's text editor application. I tried to open it in my Windows 10 Notepad application, but I got an error saying that it was too big to be opened in Notepad and asked if I wanted to open the file in another application. That was my first insight that this was not just a regular MS-DOS shortcut file, because MS-DOS shortcut files are ordinarily small files. I allowed the file to open in WordPad on my Windows 10 machine and was greeted with many weird characters, like you would see if you opened a binary file in a text editor. So I figured that I needed MS-DOS's text editor application to properly view the shortcut file.

The problem was that, like many part-time malware analysts, I didn't have old analysis operating systems laying around. I searched around the Internet and eventually found an MS-DOS emulator called DOSBox. I installed DOSBox on my analysis machine, got folder sharing working between DOSBox and my base operating system, and was able to get my .pif file listed in a directory listing in DOSBox. I then tried to view the .pif file's contents using MS-DOS's text editor program "edit," but was again greeted by the weird text symbolizing a binary file. I was beginning to see that this file was not just an MS-DOS shortcut, because the shortcut files normally just contain plain text, not binary. I didn't want to try to execute the .pif file, because I was only in an emulator and any malicious changes would persist.

I wanted to view the "shortcut" properties in a GUI. MS-DOS is command line only, so I would need to view the file in a more recent operating system. I happened to have a Windows 98 disk lying around, and the

Internet told me that Windows 98 was able to handle MS-DOS files. So I installed Windows 98 in a virtual machine and set the vm to non-persistent so any changes the malware made would not linger past shutdown.

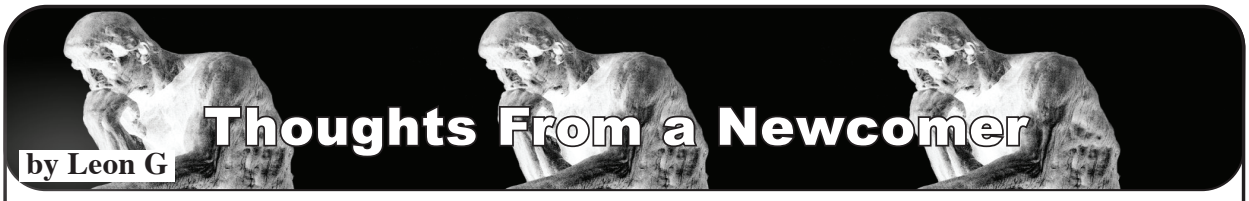
Windows 98 did indeed recognize the .pif file as an MS-DOS shortcut file, and I was able to view its properties. But unfortunately, the properties gave little information other than the fact that it was a shortcut file; it did not show what the shortcut would try to open or do. When I viewed the .pif contents in WordPad in Windows 98, I was again greeted with the weird characters of binary file content. I also tried to view the .pif file shortcut properties in a Windows XP vm to see if the properties view in Windows XP gave more information; but it too only said that the file was an MS-DOS shortcut without any information about what the shortcut did. Windows 7 offered even less help, as it did not recognize the .pif file format at all.

At this point, I had exhausted all of the manual analysis options, short of binary reverse engineering the apparent binary file. The next step a part-time malware analyst would take is to analyze the file with a malware sandbox. There are several options available online: Hybrid Analysis, ANY.RUN, VirusTotal, etc.. Hybrid Analysis and ANY.RUN will actually try to run your file, whereas VirusTotal just runs many antivirus engines against your file to see if there are any virus signature hits.

I uploaded the .pif file to Hybrid Analysis and ANY.RUN. But even just seeing their configuration options told me that they would not be able to successfully run the file because neither Hybrid Analysis or ANY.RUN offer an analysis environment below Windows 7. I don't blame them for this because hopefully very few people are still running operating systems earlier than Windows 7. But this restriction eliminates the automated sandbox analysis option when you are investigating an ancient file. It would be nice if they at least still supported Windows XP, since there are still a considerable number of XP machines out there, many running antiquated but critical processes. Plus, with XP support, you would have the ability to analyze DOS files. As predicted, both Hybrid Analysis and ANY.RUN failed to execute the .pif file. Hybrid Analysis just said the sandbox analysis failed, although it did show three hits for antivirus flagging the .pif file as potentially bad. ANY.RUN gave a screenshot of Windows 7 presenting a popup window immediately after launching the .pif file, saying that 16 bit files were not supported. This is why Windows 7 and above did not even recognize the file as an MS-DOS shortcut, because only Windows XP and below support 16 bit files.

VirusTotal was actually a bit helpful in analyzing this antique file, identifying the .pif file as potentially malicious. Five of VirusTotal's 55 antivirus engines flagged the file as bad, although only three showed red in the antivirus results list. And one of the three red results remained in the "undetected" state, because it only flagged the .pif file as Adware. Only Avast and ClamAV were fully confident that the file was malicious. Avast flagged it as a rootkit and ClamAV flagged it as a generic Trojan.

So, we have finally finished the journey of finding out if an ancient file is malicious or not. We went through five different versions of operating systems, several sandboxes, and a bunch of antivirus engines. I don't blame the sandboxes or antivirus vendors for not having support or definitions to detect these old file formats. After all, it is very, very low probability that an old enough machine would be exposed to a malware attack. However, there are still quite a bit of Windows XP machines out there, so it is interesting that the malware sandboxes do not still offer a Windows XP analysis environment. When an ancient file attack does happen, malware analysts need to be able to quickly analyze the file; and it might be very hard to find the necessary old operating systems or equipment to perform the analysis.



Thoughts From a Newcomer

by Leon G

When I got my first computer for my eleventh birthday in 2014, I didn't immediately understand how to fully utilize the access to the machine I had just gotten. I had vague notions of learning how to program, and setting up *Minecraft* servers for my friends and me to play on. That is to say that I'm a relatively new player in this game, and am writing naively and idealistically about one of the only interests I've held for more than six months.

Firstly: the whiny part where I say it's not as easy for us as it was for the early guys. The biggest obstacle that I have found is just all the baggage information that exists, which is both a blessing and a curse. When I say us, I mean the newcomers, the people my age, growing up in the current climate of the walled gardens and popular culture's stifling of exploratory computing.

We are no longer pioneers and must follow in someone else's path to l33tdom. The mainstays of the culture have been formed and for the most part agreed upon years before our parents even met. In a way, we are lucky. I can associate myself with people and ideas that have been tested. I am not taking as many risks as the early hackers were. However, the stories of glory and the connotations picked up by popular culture have strengthened. In essence, like every other person that has participated in culture of any kind, we (the newcomers) must learn how to process the old cultural material (be that music, old files, etc.), but also learn how to move forwards and define the hacking experience for ourselves.

My second point is related to my first, and it is essentially this: the muddiness introduced by old cultural material is offset by how inclusive and willing to share and collaborate most of the hacking community is. Publications like *2600* and online groups provide an entering point with anyone willing to put in some hours and contribute. And that is one of the most important parts of the hacking community to me: it's a place where I can share ideas and projects that the people around me at school and family do not necessarily appreciate themselves.

Out of the school of 2000 kids I go to, only two have shown even a slight interest in the kind of geekery I subject them to on a daily basis. However online, I show milk12345 my bad character heuristic implementation, and they'll actually respond with enthusiasm. It's an awesome feeling. *2600*, hackerspaces, and all the other places physical and not, make this world more inclusive, and safer for us.

Hackerdom is a culture of seeing-what's-around-the-corner and creativity, a palace of free-thinking built on the foundation of inclusiveness and being passionate about what one does.

Thank you all so much.

Why Is the DoD on My APN?

by ThoughtCrimes

I was recently doing some research of cellular networks and how public IP addresses change when moving from tower to tower when I came across an interesting discovery. It seems that my Android mobile phone was reporting two different public IP addresses. When I would use third-party tools like free websites to check my WAN IP, the results would always come back as expected and point to my existing carrier's network. However, when I dug through some of the internal menus in Android settings, I discovered a second IP public address which I did not recognize. This seemed odd as it was a completely different network than my carrier.. Being a little curious, I ran a whois query against the second IP and the results were astonishing. It turns out that this second IP was tagged as belonging to a Department of Defense network based in Columbus, Ohio.

At first, I thought this was funny but also a little scary. Frankly, I wasn't too worried about it as I'm not all that interesting nor was I committing any crimes that would warrant direct surveillance by the most powerful country on Earth. However, I do consider myself to be a privacy conscious individual and use VPN whenever possible, have very little social media presence, use an encrypted email provider, and use encrypted messaging for SMS. Based on this and some of the things I'd read in the Snowden dumps, it wasn't improbable that I was deemed interesting for those reasons.

At any rate, I decided to investigate further to try and determine if this was just a fluke or something targeted at me specifically. To begin, I rebooted my device and then installed a couple of network monitoring apps. Each time I'd reboot the device, the same pattern of behavior occurred. My external IP showed as belonging to my cellular provider, but a second "Carrier IP" was showing up. I continued by disabling and enabling my cellular connection to refresh the IPs and began recording what addresses I was receiving. I then began looking each of these IP addresses up to determine who owned them. To my astonishment, four out of five times, this "Carrier IP" was coming back as belonging to the DoD network. In some instances, however, the IPs were showing up as coming from the United Kingdom's Ministry of Defence. That was obviously strange considering that I was in the USA at the time. Another weird fact was, depending on what system I used to look up the IP addresses, some were reporting as not available and others were throwing warnings with detailed legal language stating that I wasn't allowed to query the whois records except for specific purposes.

To investigate further, I looked at the phones of friends and family members that were using the same carrier I was. The weird thing was that none of their devices showed this second IP address the way that mine did.... Now I was getting a little worried, but still thought it was worth digging a little deeper. So I tethered my phone to my laptop and began sniffing some of the traffic and running traceroutes to determine what was happening. Turned out that the DoD/MoD addresses were in fact showing as belonging to my device (only one hop away and only a few milliseconds of latency). An odd thing that occurred whenever I tethered the phone to my laptop, however, was that a third public IP address began showing up in some of the network analysis apps I had installed on my device. This third IP also showed as belonging to a DoD or MoD network. When I disabled my Wi-Fi hotspot, this IP would disappear, and when the hotspot was enabled, it would again reappear.

One thing that stood out about my friends' and family's devices as different than mine was that their devices were all showing an IPv6 address, whereas mine was an IPv4. I then began to compare the APN settings on my device to theirs, and that is when things got really interesting. I was using an Android device with a prepaid mobile virtual network operator (MVNO) that piggybacks on top of T-Mobile. When I set the phone up for this carrier, I followed their instructions and installed the APN as detailed in their onboarding guide. Some of my friends were using the exact same carrier as I was, but didn't bother setting up the APN that the carrier recommended we use; instead, they were using T-Mobile's default APN that automatically populated when inserting the SIM card. I tried setting up this APN on their devices and discovered that as soon as I did, the DoD IP addresses began showing up.

So at this point, I felt pretty confident that this mysterious APN was likely the culprit. To investigate further, I began entering several new APNs with slightly different settings in each to see what kind of IP addresses I'd receive. Well, it turned out that T-Mobile would only allow me to connect using IPv6 whereas the prepaid MVNO would allow IPv4 or IPv6 connections. If I connected to the MVNO using an IPv6 connection, everything looked almost identical to what I'd get with the T-Mobile APN. None of the DoD/MoD IP addresses were showing up when I connected over IPv6, however they would *always* show up when I connected using IPv4. This seemed odd to me, especially since the MVNO's instructions explicitly called out using IPv4.

I then took to the web to search on the APN settings that my carrier was recommending. It turned out that at least five other prepaid phone carriers were providing instructions to use the exact same APN settings as my carrier. Upon further investigation,

it seemed that all of them were using T-Mobile as the underlying network. Another interesting fact was that all of these carriers were providing prepaid SIM cards which didn't require any registration. Many of them were targeted at people traveling to the USA from abroad who wanted a SIM card to use while on vacation. Others were providing SIMs for use in alarm systems and GPS tracking equipment. Based on this, it seems probable that this APN may in fact be routing cellular traffic through a DoD network. I could be wrong, but if others have any possible explanations, I'd love to hear them.

I obviously can't say this with 100 percent certainty, but based on the research I did, it seemed to support the theory that this APN may in fact be used for surveillance purposes. In the end, I felt my initial assumptions were probably correct: I'm not really all that interesting. Rather, it seems that I may have stumbled onto something bigger than I had initially expected. I'll include some of the research I did to help get interested parties started to investigate further, but in conclusion, if that conspiracy theorist friend of yours claims the government is spying on them, they might not be as crazy as you think they are....

DoD APN?

```
Cellular Data
Name - Ultra
APN - Wholesale
Proxy - (leave blank)
Port - 8080
Username & Password - (leave blank)
Server - (leave blank)
MMS
MMSC - http://wholesale.mmsmvno.com/mms/wapenc
MMS Proxy - (leave blank)
MMS Port - (leave blank)
MCC - 310
MNC - 260
Authentication Type - (leave blank)
APN Type - default,supl,mms
```

Carriers That Use this APN

```
Ting
Ultra
SpeedTalk
ZipSIM
Roam
Mint
AlarmSIM
```

IP Addresses

```
HOST IP --> 25.175.94.2, 21.250.106.162, 21.250.111.204, 26.194.83.43, 25.175.83.43
GATEWAY IP --> 25.175.94.1, 21.250.106.161, 21.250.111.205
External IP --> 172.58.35.148, 172.58.35.199, 172.58.38.251
HOTSPOT IP --> 26.194.57.144, 25.175.65.232, 25.175.205.29, 26.195.248.156,
25.174.65.239, 21.251.115.224
```

WHOIS Query - Network 1

```
whois 26.194.83.43

NetRange:       26.0.0.0 - 26.255.255.255
CIDR:           26.0.0.0/8
NetName:        DISANET26
NetHandle:      NET-26-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1995-05-01
Updated:        2009-06-19
Ref:            https://rdap.arin.net/registry/ip/26.0.0.0

OrgName:        DoD Network Information Center
OrgId:          DNIC
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:
Updated:        2011-08-17
Ref:            https://rdap.arin.net/registry/entity/DNIC

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName:   Registration
OrgAbusePhone:  +1-844-347-2457
OrgAbuseEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
```

```
OrgAbuseRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN
OrgTechHandle: REGIS10-ARIN
OrgTechName:   Registration
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName:   Network DoD
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/MIL-HSTMST-ARIN
```

Whois Query - Network 2

```
IP Location      United Kingdom United Kingdom London Uk Ministry Of Defence
Whois Server     whois.ripe.net
IP Address       25.175.83.43
% Abuse contact for '25.0.0.0 - 25.255.255.255' is ''

inetnum:        25.0.0.0 - 25.255.255.255
netname:        UK-MOD-19850128
country:        GB
org:            ORG-DMoD1-RIPE
admin-c:        MN1891-RIPE
tech-c:         MN1891-RIPE
status:         LEGACY
notify:
mnt-by:         UK-MOD-MNT
mnt-domains:    UK-MOD-MNT
mnt-routes:     UK-MOD-MNT
mnt-by:         RIPE-NCC-LEGACY-MNT
created:        2005-08-23T10:27:23Z
last-modified:  2016-04-14T09:56:26Z
source:         RIPE

organisation:   ORG-DMoD1-RIPE
org-name:       UK Ministry of Defence
org-type:       LIR
address:        Not Published
address:        Not Published
address:        Not Published
address:        UNITED KINGDOM
phone:          +44(0)3067700816
e-mail:
admin-c:        MN1891-RIPE
abuse-c:        MH12763-RIPE
mnt-ref:        RIPE-NCC-HM-MNT
mnt-ref:        UK-MOD-MNT
mnt-by:         RIPE-NCC-HM-MNT
mnt-by:         UK-MOD-MNT
created:        2004-04-17T12:18:23Z
last-modified:  2016-10-06T11:09:40Z
source:         RIPE

person:         Mathew Newton
address:        ISS Design Directorate, Joint Forces Command
address:        UK Ministry of Defence
phone:          +44 (0)30 677 00816
e-mail:
notify:
nic-hdl:        MN1891-RIPE
created:        2005-03-18T10:42:04Z
last-modified:  2017-10-30T21:46:39Z
source:         RIPE
mnt-by:         UK-MOD-MNT
```

WHOIS Query - Network 3

```
NetRange:       172.32.0.0 - 172.63.255.255
CIDR:           172.32.0.0/11
NetName:        TMO9
NetHandle:      NET-172-32-0-0-1
Parent:         NET172 (NET-172-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS21928
Organization:   T-Mobile USA, Inc. (TMOBI)
RegDate:        2012-09-18
Updated:        2012-09-18
Ref:            https://rdap.arin.net/registry/ip/172.32.0.0
```

```
OrgName:        T-Mobile USA, Inc.
OrgId:          TMOBI
Address:        12920 SE 38th Street
City:           Bellevue
StateProv:      WA
PostalCode:     98006
Country:        US
RegDate:        2003-01-02
Updated:        2017-01-28
Ref:            https://rdap.arin.net/registry/entity/TMOBI

OrgTechHandle: DNSAD11-ARIN
OrgTechName:   DNS Administrators
OrgTechPhone:  +1-888-662-4662
OrgTechEmail:  ARINtechcontact@t-mobile.com
OrgTechRef:    https://rdap.arin.net/registry/entity/DNSAD11-ARIN

OrgAbuseHandle: ABUSE4857-ARIN
OrgAbuseName:   abuse
OrgAbusePhone:  +1-888-662-4662
OrgAbuseEmail:  abuse@t-mobile.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE4857-ARIN
```

Whois Query - Network 4

```
NetRange:       21.0.0.0 - 21.255.255.255
CIDR:           21.0.0.0/8
NetName:        DNIC-SNET-021
NetHandle:      NET-21-0-0-0-1
Parent:          ()
NetType:        Direct Allocation
OriginAS:
Organization:   DoD Network Information Center (DNIC)
RegDate:        1991-07-01
Updated:        2009-06-19
Ref:            https://rdap.arin.net/registry/ip/21.0.0.0

OrgName:        DoD Network Information Center
OrgId:          DNIC
Address:        3990 E. Broad Street
City:           Columbus
StateProv:      OH
PostalCode:     43218
Country:        US
RegDate:
Updated:        2011-08-17
Ref:            https://rdap.arin.net/registry/entity/DNIC

OrgAbuseHandle: REGIS10-ARIN
OrgAbuseName:   Registration
OrgAbusePhone:  +1-844-347-2457
OrgAbuseEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgAbuseRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN

OrgTechHandle: MIL-HSTMST-ARIN
OrgTechName:   Network DoD
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.hostmaster-dod-nic@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/MIL-HSTMST-ARIN

OrgTechHandle: REGIS10-ARIN
OrgTechName:   Registration
OrgTechPhone:  +1-844-347-2457
OrgTechEmail:  disa.columbus.ns.mbx.arin-registrations@mail.mil
OrgTechRef:    https://rdap.arin.net/registry/entity/REGIS10-ARIN
```

The Hacker Perspective

by shadoe

"Are you a hacker?"

Any time someone asks me that question, I pause to reflect on what they mean. Do they want me to pirate software for them? Do they want to know if I can fix some problem for them that resides in some faceless back-end? Do they envision me in some shadowy, confined space up at all hours of the night relentlessly smashing keys in pursuit of some locked away gem of knowledge? Or do they have a genuine interest in my abilities as a problem finder/solver?

I usually respond in the affirmative and wait for the next question, but sometimes I can tell already what it will be. I definitely don't pirate software for people (anymore), break into protected systems (anymore), and I think my home office is fairly well-lit and decently sized. The locked away gems I hunt are those that still reside in my own mind, waiting to be seized. So, if I peg someone as the type whose follow-up is likely on one of those veins, I just shrug and say "nah, not really."

In reality, yes, of course, I am a hacker. But, it was many years before I became comfortable self-labeling as such without feeling like an impostor. When I was a pre-teen, the hacker persona I envisioned could do amazing things like break through any password-protected software on the fly, cause money to spit out of ATMs, and bring us all to the brink of nuclear war (thanks a lot, *WarGames*!). I could do exactly zero of these when I began my journey.

I began a typical 80s kid's route to hackerdom by dialing up to various local BBSes and playing games, downloading piles of docs on all kinds of interesting subjects (yeah, you had to print them out if you wanted to realistically reference or share them), messaging other users, and learning about "warez" and the trading of them.

My first hack struck a blow against Corporate America. I had a Commodore 128 and a 1200 baud modem at that time (prior, my rig was the workhorse VIC-20 and its screaming 300 baud acoustic coupler). It occurred to me that the 2400 baud modem and mine were pretty much the same size, being cartridges and all. So, I purchased a brand new 2400 baud modem from a nationwide toy store chain, took it home, popped open the cartridges, and switched the guts. If I recall correctly, I had to make some small modification to (read: melted a hole in) the 2400's case for it to fit back together. Armed with my receipt and recently swapped guts, I returned to the store where I made the purchase and approached the return counter. I was extremely paranoid that I was going to be busted. I was only 12 and had no idea how closely it would be examined. To my adrenaline-enhanced elation, I succeeded!

Soon, I began looking into disk copying software that eliminated copy protection and shoplifting games from another, more software-focused national chain. My technique was pretty good: walk in the store with a bag from another retail establishment (in the same mall, no big deal), grab two copies of the target software and hold them as one with one in front of the other, position things so that I could hold the bag open, and drop the back box in. I could crack the games and use them for currency to download other warez or, if that particular title was already cracked, I could sell a copy to my classmates for less than they would pay retail. When *Pools of Radiance* came out with its code wheel encryption, I had my first success using a hex editor to remove the check all on my own (shout out to Bandit's Hideout in the 817)!

I wasn't always breaking the law. One of my favorite hardware hacks to date was one I made when I was in junior high school. That

Christmas, I received a gift that was essentially an answering machine for your locker. It came with two whistles that you could give to friends, and the idea was that they could go to your locker (where you would hang this recorder inside), blow the whistle to activate it, and talk to the ventilation holes (where you would tape the microphone) to leave messages. For me, it had limited utility as my friend count was quite low and, of that number, none of them were really interested in my toy beyond an initial test. I also had an old hanging door knob alarm that I had liberated from a box of old electronics my grandfather was tossing. I decided that I would see if I could somehow merge the functionality of "touch the doorknob to do X" and "blow the whistle to do Y" and I spent an evening following wires and leads from microphone to controller board of the tape recorder and weird insulated wire loop to controller board of the alarm. When I was satisfied that there was no harm in trying and thought I had a good idea of how the change should go, I cut some leads and soldered the right bits to their new places. I fully expected failure, but it worked! I was able to touch the wire and make the tape recorder turn on. I essentially had eliminated the hard limit of two users without resorting to paying for more whistles and struck another blow to Corporate America!

Eventually, retail security started tightening up and I abandoned the physical theft game. I turned back to the BBSes and piles of docs I had accumulated and started exploring the phreaking side of things. One box, two box, red box, blue box... there is no way I can get into the history of boxes in this article. Just imagine a world where payphones were plentiful (COCOTs were also fairly easy to find) and you could make free phone calls to anywhere at will if you spent a little money and some time with a soldering iron. The best part of that? Being one of very few people on your college campus that knew this stuff and making some spending money selling non-resident students the magic box that let them call back home to their parents, significant others, or anyone. Oh, and of course, giving Corporate America as many paper cuts as possible.

I think one of the most important skills for the general hacker is social engineering. Social engineering is fun. Once, my then-girlfriend and a few of her friends were looking for a place to rent when the semester was finished. She had an idea that I was a "hacker" (though I wasn't embracing it fully at the time) and "good with phones" and asked if there was anything I could do to help make sure nobody got in touch with the person renting out this particular place. I called up Bell and posed as the mark, and was able to add remote call-forwarding to his list of services. Then, I simply forwarded his calls to an unused PBX extension on our dorm floor and waited for the girls to tell me they had it.

My college years were incredibly enlightening. Until 1991, I had never heard of the Internet. Once I learned some initial Unix commands for the school's workstations, I began learning about how the systems on the network communicated, what services they offered, and how to chat with people all over the world. Instead of IRC, I fell hard into the MUD that was being hosted on one of the university's Suns. I fell so hard, in fact, that my academic life suffered to the point that I was unable to continue my education. It was a depressing time. I had finally figured out that I wanted to be "in computers," likely a programmer of some kind, but I had just shot myself in the foot by dropping out of college.

To avoid the humiliation of returning to my hometown as a failure, I moved in with some roommates to save expenses and I took on temporary jobs, making pitiful hourly wages. I wanted to stay because it was 1994 and things were starting to heat up around everyday consumers and the Internet. I needed to get "in" somehow. During this period, I was still accessing my old university account to play the MUD. When we didn't have phone service at the apartment, I would splice a neighbor's line at the junction block while they were at work or sleeping. When the university disabled my login, I went to the lab and I found a way to

get MUD access from the dumb terminals without needing to log in at all. It wasn't magic, it was CTRL-C telnet. And, if you are thinking, "Wow, I could do some serious SMTP exploitation with unlogged access to telnet," you are right! I had some fun with that, for sure. I never did anything stupid, like a friend of mine who used his work machine to spoof a threatening letter to President Clinton. Seriously, he got walked out by Secret Service agents and everything.

By this time, I had gathered various bits of knowledge across a number of domains. I had also made the jump in the temporary labor market to "knows DOS" contracts. At last, a foot in the door! I slowly began the long slog through the path of low-level IT/support grunt, to permanent positions doing "level 2" support, then to freelance work around the products I had been supporting, to returning to Corporate Land as a technical and sales-enablement trainer.

I came to view hacking as more of a life ethic than an activity. I am always looking for ways to poke at the squishy edges of things. I do it to further my knowledge about that thing - or how that thing, used in a manner that it wasn't originally intended, might help me discover more squishy edges of another thing or things. Hacking is not confined to the world of software or computer hardware or phones. If you can envision any process as a diagram or flow of individual component pieces, you can come up with attack vectors that can help you gain advantages or control outcomes.

I was finally able to jump from the IT side of technology to the creator/programmer side about seven years ago. I had been dabbling with web development as applications on smartphones and it turned out I was pretty adept at it. I made a few apps, then a little money. Then, like before, I freelanced some work making apps for other people. I became involved in the online community and the IRC channel that grew around the ecosystem. At one point, I approached the smartphone manufacturer about a cryptic tweet they had made regarding a position that seemed perfect for me (minus the part about having no professional programming experience or computer science degree). They asked me to describe what I thought the position would entail. They practically plagiarized my response when they made the official posting! I decided I would take my chances, since I felt I was at the pinnacle of my career path at that point. I still had major reservations about being exposed as a fraud, but I made it through the initial phone screen, then another, then a face-to-face where I had to do some of the hardest things I've ever done in an interview. I was honest about the perception I had of myself as not strictly a web developer, but as a consummate troubleshooter and asked questions of each of my interviewers that let them know I was engaged and serious about learning the things I couldn't answer. In short, I relied on every piece of experience I had gained to that point and used it to hack my way through each bit of that hiring process to land the position.

So, yeah, I'm a hacker and I'm damned proud of what I have accomplished. It doesn't matter that I'm not stealing corporate secrets from competitors or fixing parking tickets for people. What matters is that I know I can always approach problems from an angle that is slightly different than people who don't care about the why. If you understand the why of something, you can most times deduce the how of subverting it. If you are just starting your journey, don't get discouraged by not knowing everything (or anything!).

Keep hacking at things and, over time, experience will improve your technique. Stay safe, smart, and secure!

Who knows what mediocrity lurks in the hearts of software? shadoe knows... and likes to tell everyone about it until they're sick of listening.

HACKER PERSPECTIVE *submissions have closed again.*

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

Finding Email Addresses

by Michael Ravnitzky

Sending an email directly to the CEO of a company - to share your customer experience, either positive or negative - can be a powerful and remarkably effective communications tool, if used judiciously. But first, you need their email address. To avoid unsolicited emails, many individuals no longer publish their personal or professional emails online. There are, however, a set of simple techniques that can help you find (or predict) the email address of almost anyone.

Organizational IT policies mean that many email addresses can be accurately predicted. The "prefix" of an email - the part that precedes the at sign (@) - typically follows a pattern based on the person's name. The "domain" - the part that follows the @ is often (but not always) the same as the primary web domain of the CEO's company, such as ibm.com, walmart.com, exxonmobil.com, etc.

Since emails are part of a company's communications interchange, email addresses and organizational email formats are hard to keep totally private and show up in a variety of places, including email chains.

Search Engine Strategies

Your first step should be to conduct an online search for the person's name to see if an email address shows up. In some cases, however, the individual's name, mailing address, and phone number appear, but not his/her email address. However, beyond this simple search, there are several other tools available to you.

Some social media accounts (especially Twitter), for example, may include email contacts in the section about the person, or clues to affiliations that may provide a potential email domain. You can also try searching for the individual's name, such as Mary Smith, and the word "email" or "contact." You can also try conducting a domain site-specific search for the person's first name, last name, or both. For example, `site:domain.com "Mary Smith"`.

Finding the email pattern for an organization is also productive. You can search for the domain name and the word "email" to identify formats used for that domain's email accounts. This will help you determine if the email domain differs from the primary website domain. Or you can do a site-specific search, for example, `site:domain.com email`.

Another tool to identify alternate email domains is a WHOIS search for the web domain, which may provide organizational contact email formats.

You can use organization online directories in that industry, or conference attendance lists, to identify the email format for the person's organization.

News database searches can help identify relevant data to predict the individual's email address. Publications written by the person or even their colleagues may provide useful email data.

Most Organizational Email Assignments Are Formulaic and Predictable

Many emails can be predicted accurately because organizational IT staff are notoriously unimaginative in selecting/designating email address formats, and their operating procedures dictate a standard format for email addresses. Usually, the email address is assigned using a standard organization-wide pattern.

There are exceptions, of course. For example, one prominent news organization has been creative in assigning email addresses, often adding serialized numbers over time to deter spam.

Let's use the name John Q. Public at *2600* as a sample. The most frequent organizational email patterns are these:

```
First dot Last: John.Public@2600.com
First Last: JohnPublic@2600.com
First Initial dot Last:
➥J.Public@2600.com
First Initial Last: JPublic@2600.com
Last First Initial: PublicJ@2600.com
```

Less commonly, other email address patterns may be used:

```
John.P@2600.com
JohnP@2600.com
Public.J@2600.com
Public.John@2600.com
John@2600.com
Public@2600.com
JQP@2600.com
```

Sometimes, an underscore or a hyphen is used instead of a dot. For example:

```
John_Public@2600.com
```

In other cases, a middle initial is included in the prefix, such as:

John.Q.Public@2600.com

Or possibly:

JQPublic@2600.com

Email address assignments to individuals with a hyphenated name can vary, making it harder to predict the address.

Though less common today, for some years, many email frameworks limited the prefix to a fixed number of letters, usually eight, after which the rest of the name is truncated. Therefore, if their name had been Teddy Roosevelt, their email might be written as trooseve@2600.com.

The email pattern formats will surface across the organization, making it straightforward to predict the applicable email address.

Nicknames

In some cases, the email address follows the individual's formal given name, but the person commonly uses a nickname. That can sometimes cause an additional complication in predicting an email address.

BCC Can Be a Great Email Finding Tool

If you have several potential email address candidates and you know the domain name, you can send the message with all the potential email addresses as BCC (blind carbon copy) to suss out the correct address. This may include some or all of the permutations described in Rule 1.

BCC messages with incorrect email addresses usually don't get delivered and don't bother anyone, yet they provide valuable information on the correct email address format.

Most of the emails will bounce back, but the one that doesn't bounce is likely to be the correct email address. The bounce message or an "out of office" message can often provide valuable extra formatting or other information.

If the email format is the "John.Q.Public@2600.com" type, requiring a middle initial, you can either conduct a web search to help locate the individual's middle initial or check an online telephone directory (such as anywho.com). Alternatively, you can send the email in all 26 variants, using BCC, for all 26 middle initial combinations, one for each letter of the alphabet. The correct email will go through; the rest will bounce or be ignored, or may possibly be received by a person with the same name but different middle initial.

Often, individuals who do not have a middle name, or prefer not to use their middle name, may be included in the system with an X as a default middle initial. Some women may use a previous surname for their middle name.

Deliberate Bounces

Apart from incidental bounces, sending a deliberately defective email to the email domain may trigger an error message that contains useful email address formatting information.

Assume Gmail

Sometimes searching for the individual's name with a series of commercial email domains (especially gmail.com) may pull useful search results to the top.

CVs

In an academic environment, a curriculum vitae or CV is likely to contain email contact information. Therefore, you can search for the individual's name plus CV (or resumé) to identify these types of documents.

Email Aliases

While some people use shorter or more casual versions of the organizational email address, these are usually aliases, and the full pattern email also will successfully deliver the message. The exception is for top leadership, who sometimes may receive nonstandard email addresses.

Email Pinging

While a full discussion of email pinging is beyond the scope of this article, it is worth mentioning.

Pinging an email address is the act of verifying that the address is a real email address, but without sending an actual message. Pinging an email address is something you can do yourself. Instructions on how to accomplish this can be found at:

tools.verifyemailaddress.io/➥Articles/Ping/How_To_Ping_Email_➥Address

But many SMTP servers block email address pinging, so this might be increasingly difficult to do.

However, there are a number of online services that make it easy to ping an email address to determine whether it is active. Some of them include:

- verify-email.org/
- tools.verifyemailaddress.io/
- mailtester.com/testmail.php
- www.emailhippo.com

This allows testing of email addresses without using the BCC method. While possible in some cases, email pinging does not always produce a conclusive result. Some email addresses cannot be pinged due to limitations placed on remote mail servers.

Contacting an Assistant

Sometimes it is better to reach out to the administrative assistant or executive assistant, whose email address may be easier to locate. The message can explicitly recognize the gatekeeping process while enlisting the gatekeeper as an ally who can send the message directly to the intended recipient. Sometimes this works as well, or even better, than direct outreach to the boss. In some cases, you can mention that you'd like to send the boss an email and ask for his or her email address, but the assistant is more likely to be receptive if you simply ask that your email be forwarded to the CEO.

Worthwhile Tools

For years, RocketMail provided a cursory pattern analysis on an organization's email by collecting examples of emails with the domain name. For a particular domain, RocketMail showed the most common email patterns by percentage. If you subscribed to the service, it would provide the actual email for a given individual.

Better tools are now available.

`VoilaNorbert` is an email-locator tool; some access is free, but frequent use requires a subscription.

`Hunter.io` is another subscription email locator tool that provides all email addresses from a given domain name. But you can use it for free to identify email patterning for a domain.

`BuzzStream` is another email finder and social media page finder.

`Email Permutator` is a Google Docs sheet created by Rob Ousbey of Distilled.net. This tool takes a person's name and creates all the typical email permutations for that name for a given domain. You can then either send a message using the permutations in BCC, or else verify the email address using email pinging.

With this variety of helpful techniques and a little effort, it is not difficult to find a person's email address.

More Advanced Processors, Greater Privacy Intrusions

by Diana

One thing that makes me happy is that a TI-99/4 emulator still exists for me to develop and explore privately; the ability to think of a game or even to write a simple random color abstract portrait maker. All without having to worry about viruses, pop-ups, and even snooping.

The abstract random color portrait program is:

```
5 call clear
10 Print "Abstract Color
➥ Portrait Program"
20 Print "By Diana - 1980-2019
➥ - Use Allowed Under Creative
➥ Commons (Citation)"
30 Print
40 For i= 1 to 15
50 call color(i, I, I)
60 next I
70 For i=1 to 24
80 For j=1 to 32
90 idx=int(rnd*14+1)
100 call hchar(i,j,32+idx*8)
110 next j
120 next I
```

This program is a simple program and when it runs on a TI-99/4, no data is sent to Google, no data is sent to Microsoft, no one else logs any time of information at all; it is private to you. Or, private to who you are showing the computer screen to at your home.

The TI was around from 1978 to the early 1980s. I actually had a TI-99/4 and like the 99/4 more than the 4A. It was a hybrid 8/16 bit processor with 16MB of addressable memory via bank switching along with movable graphics called "sprites," the first computer to have it.

An advanced processor, but, no Wi-Fi or modem component that was built into the chip, which could be turned on by outside sources. So, if a computer was built like the TI-99/4, then you would not need to put a piece of paper over the camera to avoid outside images of you being seen without your permission; what you write or program is private, no world data log on a data farm for all of perpetuity (the right to be forgotten).

There was no price of admission for the TI-99/4 as compared to Web 2.0 and other advanced processors developed after 1995, the advent of Windows 95.

What is one to do? For me, when I

heard about Linux in '96, I jumped on and installed my first Slackware distribution into my 16MB Leading Edge and always prefer Linux with my 64 bit laptops. The issue of privacy still remains.

With the TI-99/4 and my trusted Osborne 1, there was great privacy even up to 2005. The reason it was trusted was because the connecting modem was a separate component that was not part of the chip or the main computer board. By not being part of the chip or the main computer board, it meant that the only access by the outside world to your computer was by that box. You decided when and where; no one could access your computer from the outside world without the box. Also, the firmware of the TI-99/4 on system and on cartridges was such that it followed a privacy practice too. No embedded modem or Wi-Fi chips; so, again, total privacy without data logging or snooping. With the Osborne 1, the same thing.

In 2000, there was a short-lived TV series that discussed the fourth generation of a chip which had a modem and Wi-Fi embedded on a chip and a group was trying to warn people about misuse. The misuse now is greater than in 2000; think about the aspects of social media.

In the 1990s up to the early 2000s, many of us participated in chat rooms and we knew that chat room logs were gone quickly. No permanence - you could chat. For many coming out, the privacy due to lack of permanence allowed many to first do this on the Internet. In many communities today, there are still harsh consequences for those who do come out.

Again, when faced with the question of privacy - older designs of computers that were made for fun and development while practicing full privacy in contrast to those made by advertisers and marketers who want to sell your information, I like the older design better. It is a reason why I have one laptop I compose and develop on that is not part of the Internet and why I use a "sneaker network" to transfer my data via flash drive (again never used on the Internet).

Isn't it time that we design computers, laptops, and games again where we have our privacy like the old retro systems? I feel comfortable and better using a system where I know that my keystrokes are not logged, even if it means I have to use a second system to access the Internet.

Given the amount of over-commercialization which has made others concerned about privacy and having their data sold, what about restarting the old BBS networks where no data-farming is allowed and no private data is kept?

WRITERS NEEDED!

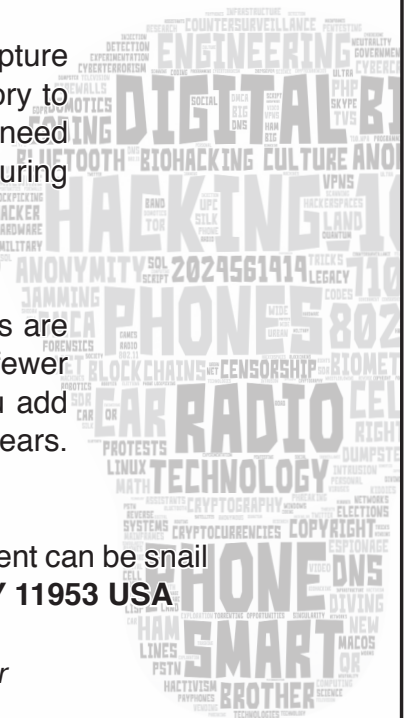
There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

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

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

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

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



Printers: The Overlooked Security Concerns

by Matt Muse, Independent Security Researcher

How much consideration is given to the security of network printers on any given network? Do you view printers as a threat to your network? Growing research shows that network printers are a major risk, and with time we can expect more and more attackers leveraging printers as an attack vector.

Consider this possible scenario as an example. An attacker wants to exfiltrate information from John. John works in a critical government setting where his PC is locked down with secure passwords as mandated and his device is fully encrypted. However, when scanning the network, the attacker notices many network printers. Simply visiting the IP address of any of these printers will bring you to the device's login page. What a surprise, default credentials were used as most organizations don't follow any sort of security practices when it comes to printers, no matter how secure the rest of their devices may be! In this case, the attacker only needs to enter the contacts/address book and remap the scanning/email profiles for John to send to the attacker's own email address, and John will begin sending potentially confidential information directly to the attacker's inbox.

Another fairly recent attack method has been spoofing these multifunction devices (which is rather easy) and sending an email with a malicious attachment to users and making it appear to originate from their office copier, which they trust blindly of course. How many users are going to carefully check emails that are sent from the copy machine that they use every day? If IT professionals don't take the risk seriously, how can the end user possibly be expected to avoid the threat?

Yet another example in recent memory is "HackerGiraffe" abusing port 9100 to print messages to support PewDiePie, a popular streamer, on 50,000 printers worldwide. According to "HackerGiraffe," the whole exploit took him about 30 minutes from first hearing about port 9100 to writing the script he used. A worldwide hack was pulled off by someone who described himself as bored while playing *Overwatch*.

So just how bad is the risk posed by network printers? In 2017, Spiceworks did a study on printer security and determined that only 41 percent of printers have any kind of security controls applied. What is even more alarming is that only 16 percent of IT support professionals view a network printer as an attack vector. This can only be described as total negligence in an age where security has become a critical component of modern corporate settings. Like any other endpoint on a network, the weakest link puts the entire network at risk for being compromised. Attackers will always look for the easiest point of entry and the data is there to show that printers are not being taken seriously when it comes to securing them on networks. If IT professionals don't stop viewing printers as basic tools, and start viewing them as networked low security computers that can also print, we will continue to see a rise in printers being used as easy targets.

CERTAINTIES

Inquiries

Dear *2600*:

Do you offer services such as locating a bank account for a judgment so I can levy it? Thank you.

D

You've confused us with a private detective agency, which we're not. That's not to say we don't know people with these abilities. Perhaps the best way to find such individuals is through our free Marketplace service or at a local monthly meeting. Good luck with the levying.

Dear *2600*:

Will Club-Mate be available to order again?

Nathan

Most definitely - and especially at HOPE.

Dear *2600*:

I would like to start by letting you know that I love your magazine ever since I found it in the 1990s - and your magazine is partially responsible for the career path change from psychology to IT, and now security.

Well, that's enough geeking out for one letter. The reason for my writing is because I would like to contribute with an article and I wanted to know what the guidelines are and do you have a specific template or style that the articles should be submitted in.

The other question is could the article be an IT story on hacking or social engineering?

Thank you for your time and have a great evening.

Sorry for the long letter - here's a cat picture for your troubles.

Darkcast

No need to send us cat pictures, though they're always appreciated. In short, yes, you can certainly send us articles on these topics. As you will see from perusing our pages, we welcome all sorts of styles and viewpoints. Don't worry about fitting in - just send us something that shares your interests and uses your background and experiences to tell the story. And never apologize for writing a long letter (which this wasn't, by the way).

Dear *2600*:

Hello, long time fan, first time writer. I have a question. I had a problem with a scammer and a con person, not to get into too much detail. Can anyone help to find justice from this con person trash? I truly appreciate if anyone write me back.

Arturo

We don't get involved in such projects, other than to share information on what can be done and what you should never do. We exist for the details. So please write us back and tell us what happened, so we can offer advice in these pages and help others prevent this from happening to them, and perhaps help you to get some justice. Whatever has happened to you is something we guarantee has happened to others.

Dear *2600*:

Would you be interested in selling 2600.com for US$30k?

I noticed that you already own 2600.org which would also be a great alternative domain to host the *2600 Magazine* site from.

If you could let me know either way, that would be great.

Richard

For one million dollars, we'll switch to 2600.org. But we also want to know what you intend to use 2600.com for. We don't intend to sell to just anyone, after all.

Dear *2600*:

Just wondering when the next quarterly issue is coming out?

amber

Right about now. Next question?

Dear *2600*:

I teach technology at a Brooklyn elementary school. Are there any suitable hacking simulator online games or apps that could work for fourth or fifth grade?

Lee

It really depends on how you're defining hacking. There are plenty of "good versus evil" games out there, like "Cyberchase" which is based on the PBS show that demonizes hackers. We suspect you're looking for something a bit more enlightened, and for that we suggest anything that encourages puzzle solving and thinking outside the box. It doesn't have to specifically be about hacking at this early stage, as the goal is to get kids to awaken their hacker mindsets and apply them to various scenarios. Computers and technology are just outlets to use the skills that are developed here. Remember, rigid adherence to rules and discouraging a lot of questions are precisely how you don't *develop a hacker mentality. Mindless video games that simply rely on repetitive actions also don't do much for that part of the brain. We'd love to hear what parents and teachers suggest here, as long as conformity isn't the goal, creative thinking is encouraged, and the skills developed are appreciated as good things.*

Dear *2600*:

I recently bought some *2600* back issues from the 1990s and saw a number of references to a tape you used to sell back then, the coveted "Dutch hacker" video. I know there are rips of the tape on YouTube, but would you ever consider selling it again? It's a pretty cool and rare piece of hacker history!

Mai

While it's certainly a piece of history, there are so many reasons not to sell it and we can't believe we're the ones who have to point this out. It's old information (we really hope the U.S. military has

patched those security holes by now), it's not the best quality, it's already available on YouTube and elsewhere, nobody uses VHS anymore, etc. But thanks for making us think of it again.

Induction

Dear *2600*:

Excited to read about hacking. I've always been interested... but never took any steps (besides an intro to computer science class where I learned to bounce a red ball from one side of a box to the other) to teach myself. But I find it super interesting. Your magazine is on J.T. Patten's "currently reading" list on *Goodreads*, it piqued my interest and... here I am! Thanks for compiling knowledge for the rest of us. Looking forward to reading it.

Amy

Welcome to the journey.

Dear *2600*:

I am a wanabe hacker. Am looking for ways to learn hacking, I want to have a super power which is The Ability to make the computer and the world to do whatever I want it to do.

Please I need help, my thirst for Cyber Tech is unquenchable. I will really appreciate if I can get a response.

Fikayo

Oh Lord. Here we go again. We don't know if you're six or 60, but you've undoubtedly been sucked into the fantasy world of the media and technophobes who believe hackers control all technology by magic and are currently living in every electronic device they own. That world doesn't exist. And hopefully the world that you want to make do whatever you want also will never exist. You want to get a super power? Strive for knowledge. Learn all you can about what you're interested in through reading, conversations, and experimentation of all sorts. Get rid of these notions of control and dominance. That's a one-way dead end. You will never know or control everything which is why you will never run out of things to do and learn about. And if that's not good enough for you, then hacking isn't your field. Unlike on television, there are few quick payoffs and lots of long nights figuring out things that often don't matter to anyone else. And we wouldn't have it any other way.

Correction

Dear *2600*:

On your payphone archive at www.2600.com/payphones, concerning Photo 4 /1023, I'm pretty sure that is the outline of Ireland, not Iceland. I've been to both, don't remember the payphones in either. But that outline....

Paul

You are correct and we have made the change. Thanks for noticing!

Observations

Dear *2600*:

This Bell truck toy is currently available locally, saw it, and immediately thought about buying it and making my own miniature *2600* truck.

Thanks a ton for all that you do! I was sad to learn there is no 2020 calendar.

Brad

Hopefully you bought one of those trucks since they're no longer available. We would love to build up a fleet. And if we're able to find a way to print the calendars cheaper, we'll be happy to resume production.

Dear *2600*:

I'm not sure if this was bad timing or if surveillance is getting this bad, but I was listening to Spotify and a kid walked into class jokingly offering a Sprite Cranberry. Before you know it, the next ad on Spotify was an ad for a Sprite Cranberry!! Crazy coincidence? I'm not sure. Voice surveillance, maybe?

Anyways, thanks for the great digest!

_hazy

We are really sick of the "Wanna Sprite Cranberry?" meme, but this brings it to a new level. While such surveillance sophistication isn't likely at this stage in humanity's decline, it certainly is something we could envision in the fairly near future. The more likely scenario is that everyone just has Sprite Cranberry on their minds.

Dear *2600*:

I bring offerings and prospect of a new subculture! It has a little bit of everything in there - but in a new, never-before-seen order of Wise Logical Scientific Rites and Living Images. Hacking could even be construed as being part of it - like, for example, when the Festival discusses, makes and uses super-fine alterations to UV Positrons for co-creating a semi-back-door to anything really - by making a concentrated biological form of: decrease of Positrons and Increase of Potential Energy (Bose Einstein Condensate) - being more equal with Net Positive Charge and Ecliptic - than any other thing can really become - and in a super organized and usable way - without disrupting the system it is working with. This is similar to how 600 Hertz causes UV Positron projections to be contained by a Plasmon - and how 2000 Hertz causes the taking in of single Neutrinos - to be contained by an Electron - which effectively causes a whole array of frequencies to be controlled by single Plasmons and Electrons.

But that is just a small fraction of this new subculture - which even delves into High-tech Permaculture Design - as well as other things.

I am basically asking for help spreading information of - and maybe even help preforming this Festival - or even testing parts of it within a window of time separate from the proposed 16 Months to complete all steps. It might prove to be fun and very useful.

I will leave an attachment of a PDF file about the Festival - all Parts and Formulas for how it is to be carried out. Please write me back - and let me know of your guy's stance on this! Also it is all Legal! As of yet. If reading the attached paper - I would read it in order from beginning to end. For some reason, it becomes almost entirely useless if read in any other order - causing too many preconceived ideas.

Thank you all - and Joy and Health to You!!!

Kody

We were going to read the file from the middle and then fan out from there in two directions simultaneously. Beginning to end is definitely better - thanks for the advice. In all of the 22 pages, however, we didn't find any actual details of this so-called festival, other than the fact that it should be taking place at Serpentinite-Rock Endemic areas and apparently lasts 16 months. Sounds like a real blast. But evidently, space and time don't really work the same way in your world.

Dear *2600*:

I have an update on your map: First and Pike Books in Seattle closed on January 1, 2020. Very sad news. It's where I picked up my *2600*.

jesse

We're very sorry to hear this. Yet another example of the challenges facing retail outlets and printed publications. Fortunately, we have other outlets in Seattle where you can find our issues, but this is one that we really valued. (You can see a full listing of U.S. stores that sell our magazine at www.2600.com/stores.)

Dear *2600*:

I'm the production coordinator of a cyberpunk show being developed. The show is about a ragtag group of losers who get roped into stealing an AI that was designed by a secret society of corporate overlords to regulate the stock market in their favor. Only problem is to protect the data, they split it up in pieces and started storing it on the most efficient storage possible: DNA.

Now an escapism obsessed hacker, his ex, a cybersex worker, and a former corporate security PMC with a bomb in his head do the bidding of one turncoat in the shadowy secret society of the ultra rich and powerful.

The creator wants to know if he could use a shot of one of your covers in the pilot episode.

Morgan

How can we turn down the creator? We get loads of questions like this and the answer is always yes. We don't think you should have to ask permission to show the cover of a magazine sold to the public. But that's us.

Dear *2600*:

I'm not looking for a fight. But you absolutely lost your mind after Trump was elected.

It was a pleasure to read stories about many things. The deranged ramblings about Trump were not one of them and they were so overbearing in the four Kindle issues I own, I chose to cancel my subscription.

Maybe you guys lightened up, but I'll never know.

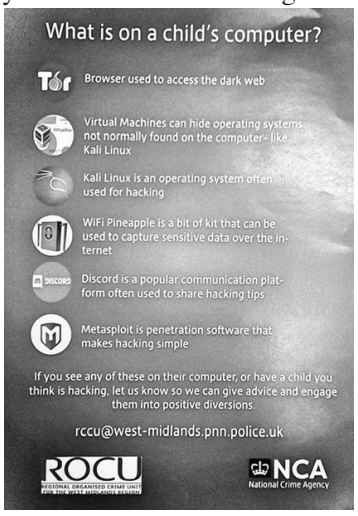
Oliver

Since you won't read these words, let us hold this up to others as an example of where many of us find ourselves today. We choose to stop listening and simply surround ourselves with material that doesn't challenge our beliefs. We live in a world of social media where news is shaped to our liking, regardless of the realities that say otherwise. But for those who decide to keep us around, expect to read content that doesn't always line up with your way of seeing things. After all, we expect that every day from our own readers and writers.

For that reason, we have always been a thorn in the side of any administration that finds itself in charge of our country, just as we are for any major corporation that handles our private data or otherwise affects our lives with or without our approval. Those who threaten us or otherwise try to silence us (or others standing up for individual rights) will find themselves the focus of even more of our attention. That's not politics. That's justice.

Dear *2600*:

I knew you'd find this interesting.



Mike the 0tt3r

We certainly did and have received this item a number of times from various people. We're slightly offended that there was nothing about us on that list, but it's funny enough regardless. Incidentally, the National Crime Agency (who we assume is against *crime) disavowed all knowledge of this once it became public and super embarrassing. But it was great publicity for the Tor Browser, Metasploit, Wi-Fi Pineapple, and Discord. And the folks at Kali Linux really got into the spirit,*

tweeting "Have to admit it's sort of nice they give kids a roadmap on where to get started. We all know the easiest way to get a kid to do something is to tell them they can't or should not, then they list specific item not to do. Too bad they did not link to kali.training." (That's the link, by the way.)

Dear *2600*:

This is not a letter meant for publication, but just information.

On page 44 of your latest issue (36:4), you said you would like to know more about using amateur radio transmissions to control satellites. These are just amateur radio satellites, of which there have been 106 since 1961. Some of these do telemetry, but most are used as repeaters. You should go to amsat.org.

I also note that some crew members on the International Space Station sometimes will make amateur radio contacts in their spare time (typically to a school class, by pre-arrangement). See www.ariss.org.

M

As it happens, information is exactly what the purpose of our letters section is. We took care to obliterate any identifying information, however. Thanks for sharing.

Dear *2600*:

Do you know what happened to HackerStickers? They used to be one of the biggest booths in the Defcon vendor's room. They had all of the cool merch, fancy lockpicks, everything a budding hacker could want. But recently, it seems they've disappeared into the night. They last tweeted in 2018 - I tried viewing their website after not seeing them at Defcon 27, but it was already dead, way back in August. I figured they had folded, but with no public word about it, it seemed a bit odd. To top off the weirdness, *2600* 36:4 (Winter 2019-2020) still had an ad for them in the marketplace section!

Are they really dead? Is it just that their ad placement with *2600* hasn't expired yet, like they prepaid for a certain number of ads? I'm very curious to know what happened.

Your Local Curious Hacker

Our ads are free, so there was no prepayment. But it does appear as if they're not active, so we'll make sure that ad doesn't appear again until that changes. Thanks for letting us know.

Dear *2600*:

Heads up, aspiring Intel techs!

If you fancy yourself a position at Intel, a new (cough, cough, really?) nationwide policy will allow Intel campus "security" to catch, record, and review license plate info as well as facial recognition. This was reported to be with "legitimate interest" so that suspected individuals could be "coached into better driving habits." Although this may at first seem like a legitimate reason to do so in hindsight of the automotive accidents that often occur on Intel campuses, this is far from likely the only reason.

Tldr; if you're going to work for Intel, expect to be catalogued. But that in itself is nothing new.

Failsom

We were able to verify the existence of this program via the "license plate recognition privacy notice" at intel.com. It's amazing how they make this seem so much in the interest of whoever happens to be driving on one of their campuses by saying things like "maintain... safety and security," monitor "unsafe behavior," "optimize resources," or "locate an individual... in an emergency" when what they're really doing is monitoring everyone's movements simply because they can. People reading this in the future will probably wonder why we're making a fuss over it. Trust us... privacy used to mean something.

Dear *2600*:

Hello, lifetime subscriber here, love the magazine, but I have a few questions and concerns I'd like to raise. First, it takes me a very long time to actually start reading the magazine because of the payphone pictures, notably, the "more photos on back" and "see more on the front." You never add an IF statement to define whether one already came from the front, and one can get stuck in an infinite loop without this instruction. I usually get exhausted and fall asleep, and sometimes, if I'm lucky, it falls open to an interior page and I can bypass the loop. Second, regarding what we get if you use our submissions, I have a serious concern. You state that we're entitled to "a free one-year subscription (or back issues)." This seems a bit extreme to me as, since I already am a lifetime subscriber, I have to choose between double copies or physical pain? And how will these back issues be enforced? Do you send a group of hooded goons to beat me up and billy club my spine? I already have knee problems, I don't want any more issues. I'm sure there are other problems with this publication, but these are the most glaring. I hope you guys can stop resorting to mind games and threats of physical pain - the contents are good enough without this trickery.

Shouts to Niebers. Loretto is fail.

Token

An all too tiny look at what we have to contend with on a daily basis.

Dear *2600*:

Hey there!

I noticed you are the owner of hackerquarterly.com. Are you interested in hackersquarterly.com? Let me know and I will send you more info.

I wish you a nice day!

Killinger

We actually forgot we owned that domain in the first place, so thanks for the reminder and for helping us realize we're wasting money on domains we don't use. So the last thing we want right now is another one.

Dear *2600*:

I was looking for the newest edition of *2600* at Barnes and Noble (which, it turned out, wasn't available at this particular one yet), but was having trouble finding the current *2600* where I usually do. It wasn't in the technology section like it normally is, and I couldn't find it on any of the

other main magazine racks. I was beginning to be worried that they stopped carrying it or something, but *then* I found it. Right where it should have been, of course! Off on a portable rack, in the holiday decorating section, almost a month after Christmas, nestled in with some health magazines! Glad to see your influence is reaching into so many other areas!

D

Now that's respect. (We'll look into why it took the new issue so long to show up.)

First Friday Fun

Dear *2600*:

I am writing this letter to ask permission to start a *2600* group that covers Manila and Metro Manila, Philippines. I would also like to ask the requirements to start this meeting group.

Luci

We've sent you the meeting guidelines, which are also published on our website for anyone else who might be interested in starting up a meeting. In addition, we've alerted you to the fact that there's already a meeting in that very area, a fact you can hopefully verify. If you feel you have a better location, please let us (and the existing meeting attendees) know and we'll be happy to post updates.

Dear *2600*:

Our latest monthly meeting for Wenatchee (Washington) had eight attendees.

We've gone into giving some structure to our meetings. We meet with the same schedule as typical *2600* meetings (5 to 8 pm, first Friday of the month). We've been wanting to incorporate some structure, but found that many people tend to take their time showing up, and at around 6 we are at expected population. So we have an open gather / talk / getfood / getdrink time before the structure (5 to 6 pm), which coincides with the brewery's happy hour.

Starting at 6 pm, we begin a structured meeting that ensures that we read the rules aloud, get the opportunity for everyone to introduce themselves (or pass if they wish) in a round table fashion, mention community technology events and volunteer opportunities, mention personal projects and provide a springboard for individuals to request help on their projects from others in the group, and finally, we go into a 20-30 minute presentation. Anyone can present, but we ask that they contact us via our email contact address (provided at meetings), or our local Facebook group page three days before the event so that we can make sure that we have arranged materials needed (power, projectors, etc.) with the establishment.

This month's presentation was a demonstration of RasPwnOS, a Raspberry Pi based Damn Vulnerable Linux with a variety of vulnerable web applications pre-installed. Its ease of deployment, low cost, and portability make it an ideal addition to our meetings and a decent first start for anyone looking to build a quick, dirt-cheap vuln testing lab. The structure only lasts about an hour, leaving us with 7 to 8 pm to intermingle and discuss.

Ian

While this structured format doesn't work for every meeting, you seem to be having success at it, which is great to hear. We do ask that attendees not feel compelled to participate, since our goal is to be as inclusive as possible. And, on that note, we assume that the meeting taking place in a brewery doesn't mean that those under 21 aren't welcome to attend, as that's an extremely important part of any meeting. We'd love to hear what other meetings are trying out.

Dear *2600*:

I'm not sure if the San Diego meeting at Regents Pizza meets anymore. The last two times I went, I didn't find anyone. I'm wondering if I should start a new meeting.

Zen Paralysis

Unless that particular location is unsuitable, the best move would be to breathe new life into the already publicized venue, since anyone who ever went to previous meetings will undoubtedly think of going there first. Also, a great way to attract attendees is to leave little notes in or around copies of our magazines in local stores.

Dear *2600*:

First meeting with more than one person in Lisbon! Two nationalities, how crazy is that? Myself and a fellow hacker from Russia. Good thing the meeting has been around *2600* for a while and that I was on Twitter - we were sitting back to back before meeting!

Talked about software development, SDR, and the demo scene. Had no clue the demo scene was so much alive. Will definitely be going to St. Petersburg sometime soon.

Happy hacking!

billk3ls0

This is a great example of how being determined pays off and can result in true magic. We hope there are many more such encounters. And for anyone in (or passing through) Portugal, this seems like a

great way to spend a Friday evening.

Dear *2600*:

Just an update, our meetings here in Penngrove (California) have been going great with a great showing and a Discord channel to communicate projects. We moved our location from Starbucks to Caprara's Pizza and now call ourselves *2600* North Bay. We welcome all hackers and those interested in the culture and technology involved. Hack the Planet!!

Mad Glitcher

Dear *2600*:

What time does the Manhattan meeting in New York start - 5 or 6 pm, please?

David

Unless otherwise noted (as this meeting isn't), meetings start at 5 pm on the first Friday of the month. But that doesn't mean everyone shows up at that time. People tend to trickle in throughout the evening. There are no penalties for being late.

Dear *2600*:

So, one is just supposed to go and show at these meetings? No sign-up list?

Al Xbert

Nothing of the sort. Your identity is yours to do with as you wish.

Dear *2600*:

Smaller turnout this month in Raleigh, North Carolina, but any non-zero number still counts as a successful meeting.

arcane

That's a great attitude to have, and not just for meetings.

Dear *2600*:

Concerning the meeting in Stockholm, Sweden, me and Quik made some real efforts to promote it this time.

I managed to claim the old @2600se account and tweeted out: "Stockholm Hackers! The *2600* meeting is on again! This Friday (Dec 6th) 17:00 (local time aka CET) @ Starbucks Stockholm Central Station. #2600 #2600se #hacking #phreaking #hacktheplanet - greets to @2600 @SEC_T_org @0xFFse @sakpodcasten - special greets to Quik"

The tweet was spread through IT security channels and some famous hackers in Sweden started to follow the Twitter account.

We were hopeful.

Only me and Quik turned up at the meeting at 17:00 sharp. We were a bit downhearted by this, but I reminded him that we had a 100 percent increase since the last meeting I went to. As far as we know, no other hackers were present. The train station was really crowded and noisy, but the Starbucks was not overly full. We sat at a table with a neon green pi-top, with a white antenna hanging out of it. On our table there were two miniature keyboards and a Sun Microsystems mouse. I'm sure that if anyone was looking for the *2600* meeting, they would have found us.

We clicked around in the Kali menus for a while and Quik said, "This just feels like work, using Kali." The coffee (long double espresso) and fudge cake were unusually good and after an hour we both agreed that we were old and tired after a long day's work, so we left at 18:00.

We hope more will come to the next meeting. I wouldn't be surprised if more showed up, but I must admit, I wouldn't be surprised if I was alone either.

/Psychad

It's not easy to get meetings started or to breathe new life into meetings that have seen better days. But you're doing everything right. And being in a busy place is a great way to snag some curious people who just happened to be passing by. We hope you continue to show up, publicize the meetings, and spread enthusiasm. The payoff is almost never immediate, but your efforts will undoubtedly have a positive effect on others if you keep at it. Good luck.

Dear *2600*:

Is the Madison, Wisconsin meeting currently active? I've been wanting to check it out for a while, but they don't seem to have much interaction with IRC, Discord, Reddit, or Facebook.

I'm a little socially anxious by nature. I just have a bit of a fear that I'm going to show up and nobody will be there or it'll be a few close-knit dudes working on something way beyond my skill level and I'll just be the awkward girl sitting and watching. Is there anyone who attends that you can connect me with?

ll

We don't share any contact info for privacy reasons. We understand your hesitation, but hope you give it a shot. You can always just pass by without revealing any interest to scope out the scene. For those currently involved in meetings, we ask that you pay particular attention to these types of concerns, as they're not at all uncommon. We need to make sure we're doing all we can to create a welcoming environment for newcomers.

Dear *2600*:

I'd like to start a meeting in Fort Worth (Texas). What information do you need from me?

Chad

We don't require any information, other than regular updates from the meeting once it gets started. The guidelines have been sent to you and are always available on our website. But this may be a case where there are too many meetings in the area already. Addison, Dallas, and Plano are all within an hour of Fort Worth. While we don't want to discourage anyone, four meetings in such a close area will likely drive down attendance. It's best to coordinate with the others if they're this close together.

Dear *2600*:

I wanted to start a chapter of 2600 in Bangalore, India. There is a lot of interest among the hacking community here. Also, I have several venue options, which may have to be cycled through as per availability. Can you let me know how to get started?

Karan

We sent you the guidelines and we look forward

to hearing how it's going. We get that it can take some time to find a place that works, but it's important that your location remain constant. So please choose carefully, as our listings are only updated for each printed issue to avoid conflicting info. Not everyone seems to get this, as seen below.

Dear *2600*:

Weeks ago I reported a change of venue for the Titusvulle (Florida) meeting. *This Friday is the meeting date for February.* For those people who will check the online listings, I *insist* you update the meeting page. If you need me to take over the official meeting page to provide updates faster than *2600* staff, *please* contact me to discuss the matter. I would be happy to volunteer to do so.

The Cheshire Catalyst

We appreciate your enthusiasm, but this is the sixth time in four years you've changed the venue - three of those times in the last six months! If you're looking to confuse people, that's precisely how to do it. You need to pick a venue and stick with it. Since we're seeing this meeting going back to previous locations, this doesn't look like a situation where businesses are closing and forcing you to move. The meetings don't exist so you can decide from month to month what the most convenient location for you is. Communities are built on consistency. And on that subject, we need to be consistent in what locations are being publicized at the same time. That's why we only update the listings when there's a corresponding issue. Otherwise, the issue would say one thing while the online listing would say another. If a last minute change occurs, a local web page for the meeting (that we link to) can address that issue. But that should be the exception, not the rule.

We won't be changing this location again unless the current meeting place goes out of business or enough time has gone by where hearing the name Titusville doesn't make our staff try to jump out windows.

Dear *2600*:

This is a keep-alive report of the *2600* meeting in Buenos Aires in Bodegon Bellagamba. I was there in the last part of 2019 and hopefully it's very active and many assistants are coming.

To my surprise, there were many new faces. Young people are joining this meeting point and finding a place to share knowledge and stories - and to learn from old school hacking. Most of the new people came from the Ekoparty Security Conference that has been going on in Buenos Aires since the year 2005. Thanks for sharing! Keep calm and drink mate.

Pablo 0

Buenos Aires, Argentina

Great to hear. Please keep up the good work!

Interesting Stuff

Dear *2600*:

I am not looking for anything in particular, however I just found *2600* and I think I'll let you know what I'm up to. My background is in engineering - chemical and materials science engineering. I started working in IT - Accenture in 2014 because I couldn't find a job in the chemical industry.

I'm not bullshitting when I say this, but I've made the alethiometer (golden compass). It is a fabled device from a fictional novel (*His Dark Materials*). HBO made a series adaptation recently which shows how it's supposed to be used. Anyway, I made it, and it was taken off the market for the second time. I think it's big news in engineering history. Aside from it being the first prototype of the alethiometer, I think it can be adapted to allow for mass communications across cultural borders and bring world peace pretty fast. I am currently working on making a few adjustments and raising money for it through the form of grants. I am letting you know because I will probably need support in the future if it ever grows big from the likes of hackers.

Mudib

Be sure to send us a prototype so we can review it.

Dear *2600*:

Help. I called 2600.com ten years ago and I told you I would need your help and maybe your listeners' help as well. Deep fakes have come out. And I have only one video on the Internet drinking a swig of vodka. I need your help - this is a temporary email. Which could be gone like me without help. I want to call in but not live. Give me a number and a convenient time - and we just talk first.

Bill

We often wonder just how much more interesting our lives would be if only we had more time to follow up on letters like this one. We've been kept up nights wondering if this writer is the victim of a deep fake video or the perpetrator of one. And how does the swig of vodka tie into all of this?

One thing is certain: once these deep fakes become prevalent, these kinds of interactions will seem completely normal. There are some fun times ahead.

Dear *2600*:

I just signed the petition "Clemency for Ross Ulbricht: Condemned to Die in Prison for a Website" and wanted to see if you could help by adding your name.

Our goal is to reach 300,000 signatures and we need more support. You can read more and sign the petition here: chng.it/xFMz9XrxFQ. Thanks!

Michelle

At press time, it looks like you'll have no trouble reaching 300,000.

History

Dear *2600*:

After a long career in the phone business and a longtime subscriber/newsstand reader, I need to write about an amusing story dealing with 2600 - the hertz variety.

We had long used *2600 Magazine* in our business

and in our research labs to keep tabs on what the public was fooling around with and were always amazed at the ingenuity and curiosity of some people with too much time on their hands trying to see what would happen when you did random things to your telephone. The era of the blue box was certainly an eye opener for us all on how we designed our equipment to keep it relatively safe and secure.

I was responsible for putting the first Nortel DMS in service in Ottawa, Canada in the 1970s and one of the maintenance features was all types of audible and visual and paper alarm indications. The alarms were staged into three levels - minor, major, and critical - each with its own buzzer/bell that you could hear anywhere on the floor over the background noise of the telephone equipment.

Another maintenance feature was that in order to communicate with support people in case of problems, one telephone line was sourced from another switch in case your switch was off the air.

During the testing stages, bells going off was a continuous happening and no one paid too much attention to them as the commissioning of the switch got closer to the in-service date.

While talking to the labs and support groups on the phone, we occasionally kept getting cut off. It happened to me too often and I kept trying to figure out what the cause and effect was and finally figured out that when the critical alarm bell started to ring and I was on the phone to the labs, I would get cut off.

Now this was the time of blue boxes and Captain Crunch whistles being fairly popular and I finally figured out that the trunk I was talking to the labs on was using in-band signaling (which used 2600 hertz) and a harmonic of the critical bell must have been 2600 hertz, thus telling the trunk to disconnect.. Sure enough, after drilling a couple of holes in the bell to change its frequency, the call cutoffs were eliminated.

I always give credit to your magazine for helping me figure it out. I am sure you already know that a lot of folks in the telecommunication/computer/software business read the magazines as well.

Keep up the good work.

Jack Jordan

If this took place before 1984, then it was before our time. But the spirit of hackers and phone phreaks existed long before we were around and will survive whatever lies ahead. Thanks for sharing a great story!

Dear *2600*:

I saw the recent letter about Central Office in Tacoma, but I also noticed there was no mention of the Telephone Museum in Cle Elum, Washington. Located at 221 East First Street, it was the site of the last operator-assisted switchboard run by the Pacific Northwest Bell system. If you're in the area between Memorial Day and Labor Day, it's a lovely place to spend a couple of hours. More information can be found on their website: kittitashistory.com/sites/telephone-museum/.

Squeeling Sheep

It seems these museums are everywhere! Thanks for sharing. We look forward to hearing about even more, perhaps some in other countries as well?

Responses

Dear *2600*:

This has got to be a better letter than the one I wrote prior, in which I complained about a missing driver, only to suddenly realize that I missed the dongle-like bit on the web cam cable that controlled the light, and there never was "software control" for them. This letter is in response to Ruikmuir (36:4).

The issue of people that are "fake" because they claim a different gender or orientation is something I do know about, and his comment probably pissed me off as much as it did you. Not just because the very idea that people need to be "normal," and they are somehow ruining the world by challenging those ideals, but his assertion that his version of normal is "science based" is factually incorrect right from the start. I refer everyone to this article, from a college professor named PZ Myers: freethoughtblogs.com/pharyngula/2014/03/11/pathways-to-sex/.

Another article on sexual morphology goes into much greater detail and is stated to also be an incomplete list of all the things that affect physical sexual development, but it shows the network of things that need to go "right" for everything to end up as the XX/XY pairings are "supposed to" work that contain at least 13 different gene interactions, and an explanation in the linked article and chart regarding all the thing that change as a result: freethoughtblogs.com/pharyngula/2017/09/18/building-a-sex-is-harder-than-most-people-imagine/.

And, remember, this is known to be an "incomplete" list of things that have an impact. It's a complex series of interactions that *must* happen for someone to end up with the right sex organs, and literally *anything* can go wrong in this process, resulting in someone with drastically different physical characteristics than their apparent "genes."

We see clear, obvious, and undeniable pathways to development of "physical" differences which do not conform to Mr. Ruikmuir's simplistic "normal," but also that, when it comes to how the brain wires even the most basic and simplest characteristics, with regard to gender identity and sexual orientation, we, by comparison, know almost nothing. We literally don't even know what most, never mind all, of the genes involved are, how they interact, what the expected result is supposed to even be, never mind what the deviations are, never mind why, how, or even when, they happen. This, by the way, to push the point home, actually includes cases of over-sensitivity, or insensitivity to estrogen, or testosterone. If you don't "react," starting in early development because the

mechanisms that interact with one or both of these do not work right, it is one of the things that can, despite "every other thing about your genes saying the opposite," end up producing a body that has the wrong anatomy. Because, funny thing, not "reacting" to, or "overreacting to" either of these things causes the development of the "opposite parts."

There are, ironically, plenty of people who seem perfectly happy to acknowledge that genes can do things they shouldn't, or have errors, which results in everything from abnormally large anatomy in both men and women, as well as a complete lack of those characteristics and just about every feasible result in between. Yet these same people, despite the existence of *known* developmental errors which affect the brain on drastic and profound levels, are flat out unwilling to allow for the same thing "in" that brain, as happens with physical gender - i.e., an otherwise totally normal person with no apparent dysfunctions, who, nevertheless, has a wide range of sizes, to their physical sexual traits, all based on some, simplistic XX or XY comparison, proclaiming, "The brain is somehow exempt from all these things, even though we know almost nothing about how its genetics determine sexual attraction, or perceived gender."

This is tantamount, despite the often flawed nature of such comparisons, of some clown claiming that you can change the "hardware" in a computer, and that it can contain variations in design and function, but it's impossible to alter Linux and install a version that does something different than what is "normal" for that piece of hardware.

It's not even a logical argument. The brain is affected by genes just as much as everything else that has to go through stages to form in a body - and, in the case of the brain, our definition of normal comes not from its genetics, or even facts, but more often than not from religions and "social rules" about what is "normal." In reality, when it comes to what the brain is even doing when you look at someone or something and get aroused, this is still utterly opaque to us. We can track the bits and bytes, as it were, but we haven't even started to crack open the "chips" and look at why the bits and bytes do what they do, never mind how much of it is because someone installed "Social norms 1.2355.67.1971.dat" in there instead of "Social norms 4.25.62243.2020.dat".

But, one thing is absolutely certain. "Science" rejects the idea that "gender" and "sexual orientation" are some sort of simple switches built directly into the hardware instead of, at minimum, an entire 64-bit integer full of flags and values, any or all of which might be "flipped" to just the right state if you want to produce 100 percent pure male or 100 percent pure female.

Patrick

It's incredible how one uninformed statement can lead to a whole lot of intelligent discourse. This is what makes the science of hacking so universally interesting. Every day we learn that there's something new to discover, explore, and question.

Dear *2600*:

What I had hoped was that *direct* communication between readers could be further facilitated somehow without the need for anything to be published. It is unfortunate that you don't have something like an online discussion forum (independent of social media). If I had the skills and the know-how, I would happily build it and moderate it for you. Something Reddit-style perhaps. I know it's not a suggestion you are likely to take, but just wanted to throw it out there anyway. Thank you, as always, for your time and consideration.

Emily S.

While we love communication, this just isn't something we're set up for. If writers wish to communicate with readers and/or other writers, they can make themselves easy to find through various search methods - or even include contact info along with their chosen byline. However, if they don't want that, it should be just as easy to remain private. We already have a whole bunch of social media options for the magazine on top of all of the magazine stuff. So we're quite happy with where we are communication-wise. We'll continue to help connect people together whenever that's possible and desirable.

Dear *2600*:

I've enjoyed *2600* for many years, despite being neither a hacker nor much of a computer expert. Thank you for what you do.

Your 36:4 issue contained a letter (page 44) about Google Street View being used by stalkers. You responded by essentially "hoping" that Big Tech would be more responsible. That's so sad, but understandable; it's certainly the majority opinion. Big Tech counts on that naivety.

But there are two relevant legal issues that I think your readers may appreciate.

One is the unique aspect of the United States in that it is based on a written document (not a person) and that document structures a decentralized government, a structure based on a healthy, and historically accurate, inherent distrust of government. As one example, the federal government was only given 18 enumerated powers (Article I), whereas states retained all general powers, but for some exceptions. Courts were given no enforcement power, no power over the states, no power over any other branch. Founders determined that unelected judges, in office for life, were the most prone to tyranny.

The fact that we now labor under a monster that is nothing like a decentralized federal government is the cause of most every national U.S. crisis today - the very type of crisis that our founders anticipated and drafted a constitution to prevent, using decentralization.

U.S. states still have more power than the federal government in all but those 18 enumerated

areas. But they are cowed into non-action by naive politicians who believe the feds can do anything, thanks to politicians' erroneous understanding of the "supremacy clause." Politicians have never been the sharpest crayons in the box, but they're enabled by a naive populace and fed by a media that benefits from constant headline-creating crisis and division, not from solutions.

And this leads to point two, which is the answer to your dilemma about Big Tech's irresponsibility: States can stop it.

Here's just one example, relative to the Big Tech issue. The general civil law of every U.S. state but Louisiana was based on English common law - developed over hundreds of years and followed successfully in the U.S. until the late 1900s. Under that common law, there is a right to stop someone from invading our privacy. This comes in four types: 1) misappropriating a name or a "person;" 2) intrusion upon someone's seclusion; 3) describing someone falsely; 4) publicly disclosing private facts. Each state has details that differ and there are other related principles, but that's a core of the claims, for our example.

Big Tech intentionally violates these, billions of times every second. Why does not anyone do anything about it? If you go to a lawyer and say, for example, "Google is using detailed satellite photos of my backyard and showing the entire world, including stalkers and burglars who want to case my house, and taxing authorities, who penalize me for not telling them I installed a pool!" Isn't this "intrusion upon seclusion?" Or you mention facial recognition or selling a composite of your most personal information, or....

In response, today's well-trained lawyer chuckles and then dutifully explains that, thanks to the supremacy clause, state common law takes a back seat to federal laws, and the feds have legislated in the Internet area. They rule, that's that. Run along now, you right-wing, racist, extremist you.

That lawyer is, understandably, relying on federal court opinions, judges that have every motivation to increase their own relevance, regardless of what the Constitution says, and no longer checked by the states or by a public educated on the limits of the federal government.

Fortunately, it's getting easier for Joe and Buffy Mass Public to understand these limits, thanks to marijuana states and the sanctuary city movement (both immigration and Second Amendment types).

Let's say a privacy suit against Big Tech is filed in state court. That judge will, erroneously but understandably, just like the lawyer, send it over to federal court and that judge will dismiss it all with a chuckle and call everyone racist right-wingers, hoping it gets picked up by the press, so that judge appears heroic for the gratuitous speech about morality (from a government official, too, hmmm). She might even sanction everyone for having the "audacity" to challenge "settled precedent" - as if some sole federal judge's opinion deserves more respect than the written U.S. Constitution, ratified by state legislators. (Yes, federal judges do think that way, which is why the founders gave them so little actual power, if you read the actual document.)

But aha, a courageous state leader, maybe the attorney general, someone who has read the Constitution, someone who does consider it more weighty than a judge, intervenes. He sees no grounds under Article I for federal jurisdiction over the issue of when strangers can sell people's private data (no, it's not the "commerce clause," which would gut all of Article I, indeed the entire Constitution, if it was ever meant to be read the way that today's federal judges do) and asks the state supreme court to weigh in. If those judges "get it" (and don't give up, they are "getting it" as they see more citizens waking up on this, too), they keep the case in state court, where the parties can go forward on the privacy issue, as it should be.

If a jury agrees, a verdict is reached and a state court judgment is rendered against Big Tech, based on the common law. The feds swarm on it like angry bees, frothy at the mouth that anyone would be so audacious as to follow the old, written Constitution ("Hey, wasn't it written by dead white guys anyway? I thought we came down there and burned their churches and shot their cows. They're losing their respect!") and issue an injunction. State officials ignore it, as they would an injunction from Angola or Greece. State officials, as sovereign entities under the U.S. Constitution, move to enforce the judgment against Big Tech, whose leaders are by now shaking in their fruity designer duds and spilling their $10 coffees, angry and frightened that their protective shield of naivety no longer works. They use their massive social media databases in blackmail attempts against state officials and attempt to warp the news and sentiment about this issue. No?

Another idea is for states to do what Illinois (and Texas) did with a Biometric Information Privacy Act, a weak emasculated version of what they could do, but effective, as witnessed by Facebook's recent $550 million settlement and, more importantly, its plunge in stock price, as investors think, "uh-oh, states are waking up to the scam."

Like the "sanctuary" principle, states have simply refused to enforce George Bush's unconstitutional "Real-ID Act." Hoorah.

Way back in 1854, the Wisconsin Supreme Court rightfully declared that the Federal Fugitive Slave Act - passed by the U.S. Congress, not some redneck racist Southern states, as Hollywood tells us - was unconstitutional. It actually rewarded bounty hunters to find black people, assume they had "escaped," kidnap them, and bring them back to their owners, without due process, lawyers, or anything. The whole U.S. considered black people to be mere property, as the U.S. Supreme Court (again, feds, not the south) unanimously determined, in that case, and again with the more

famous Dred Scott decision. But Wisconsin not only refused to enforce it, they made it a crime for anyone to try to enforce that law, including federal employees. Yes, states can do that. They could make it a crime for anyone, including Big Tech employees or federal agents, to do anything inside their states that is not exclusively within federal authority. Protecting state citizens is a state's responsibility, not the feds' (it's not in Article I, so feds have no right to go there).

Long shot? Maybe. And it's time. What else, we just give up? We do have an answer, there is a solution, written into our founding documents, integrated into the country's OS. The remedy starts with telling people how our constitution gives us decentralized remedies. Once we start applying pressure to state officials, it will fix. But that's where our focus should be, not on the seething swamp of DC.

2600 could greatly assist this long shot by first informing folks of the anti-tyranny decentralized nature of the U.S. Constitution (as opposed to how the general public thinks) and further by letting them know that their own states have the answer.

Jack

We'll leave the bulk of this for legal minds to ponder, but we need to weigh in on a couple of key points here. You seem to have missed much of the news in recent years, where this right wing group of states' rights advocates you believe in has become really quiet. They (or their allies) are the ones appointing the federal judges now. States are currently fighting the feds on a number of issues and those fights, some of which you cite, are no longer being led by those on the right wing. It's quite the opposite, in fact.

People who believe as strongly as you do in the Constitution should always take that side, not simply when politics dictates. What a difference that simple adherence to values would have made over the past few years.

Of course, that doesn't mean the states always act correctly. The civil rights movement is a clear example of how racist state policies needed to be taken down. And, sure, there were plenty of racist laws and policies on the federal level as well, but to gloss over state responsibility, as you seem to, is irresponsible and horribly misleading.

Human rights (including freedom of speech, privacy issues, a free press, etc.) cannot be trampled upon by either state or federal authorities and, when that happens, systems need to kick in to correct the error. If the Constitution fixes that, then it's still relevant. But if it locks us into a perpetual stalemate, then we need some upgrades.

Finally, the letter you reference concerned an incident that took place in Japan. While you may see the Constitution as the ultimate arbiter, it has no power at all in other countries, which is where a lot of Big Tech happens to live. So we need to work together with people all over the world and also learn how to protect ourselves as individuals. Nothing else is going to work.

HOPE 2020

Dear *2600*:

Are there any age restrictions for attendees for HOPE?

B1u_De4D

We don't want a bunch of toddlers showing up unattended. Other than that, it's all common sense. And obviously, underage people can't book hotel rooms, but that's not anything we have control over.

Dear *2600*:

Over the years, I've attended nearly all of the HOPE conferences. In fact, the first one I attended was at the Puck Building (the second HOPE conference).

I know that you're excited about your new location, but I want you to know something... I'm *not*.

I live in Brooklyn and there's no way that I'm going to take a very long subway ride out to somewhere in Queens and then take a bus to get to the conference, and then do the same thing in reverse to get home.

I suppose if you live on Long Island, holding the conference in Queens at a college that has plenty of rooms and plenty of space is a great idea, especially if you travel by car and value something called parking. But for someone like myself who doesn't own a car, I can't bear the hassles of a long commute.

I know the cost of holding a convention in Manhattan must be exorbitant, but what your final attendance numbers will be, at least for now, is anyone's guess. I wish you the best, but I do hope that you'll bring the convention back to Manhattan two years from now.

Even Jersey City would be better than Queens. (I can't believe I actually said that.)

David

You're not the only one expressing concern, though perhaps you're the most passionate. But Queens is not nearly as inaccessible as you fear (a common and ironic misconception for people in the neighboring borough of Brooklyn). We don't know what part of Brooklyn you're in, but we doubt it's much harder for you to get to Queens than it is to get to midtown Manhattan or even New Jersey.

For one thing, there are ways of greatly speeding up the trip. For instance, the Long Island Railroad's "city ticket" is only slightly more than a subway fare and gets you from Brooklyn to Queens in around 20 minutes. The bus connection from that point isn't long at all.

We know this is different from how it was before, but how much time did it really take to get from Brooklyn to Hotel Pennsylvania in Manhattan by subway? We estimate it would be at least half an hour. So all of this comes down to a couple of dollars and ten extra minutes to make HOPE happen for you. We're hackers - we can handle a little bit of change.

(Incidentally, for those of you who can't bear to depart from our traditional home of Hotel Pennsylvania in Manhattan, they've actually

stepped up to offer a special rate to conference attendees - even though the conference is no longer in their hotel! Getting to the conference from there is super easy - just walk across the street and take the Long Island Railroad one stop to Jamaica where you catch the bus to the conference. Full details are up at www.hope.net.)

WTF?

Dear *2600*:

In the instance that I have a form of technological terrorism being waged against me, say for example... hackers attempting to tap nanotech in my brain to run algorithms... how would you go about solving this? They are literally using Daisy Ridley's identity in my head with a bunch of fucking pop-ups to try to antagonize me. I'm getting a lot of bribes and shit.... I've already contacted a few three-letter acronyms and the like, with little response if any. I talk about some unusual and contentious things on my wall only because I'm forced to.

Ryan

Wow, where do we even begin here? Over the years, we've received so many letters like this, the only variation being the type of technology exploited for these nefarious purposes. As science evolves, so too does the sophistication of those entities attempting to reprogram our brains. We're now at the nanotech stage. However, we don't believe any evil scientists are yet at the point of being able to hack into people's heads. Will that happen someday? If the science allows it, absolutely. There is no evil that's off limits. But that's still science fiction, at least at the time of printing. As for other methods of driving people insane, they certainly exist and are used by the most sophisticated intelligence organizations, as well as hostile neighbors who simply want to drive their enemies batshit crazy. The most important ability is to be able to identify which is which. It's unlikely an intelligence agency is trying to get into the head of someone who isn't pretty high up on the totem pole, which eliminates the vast majority of us. And if a neighbor (seen or unseen) is giving you the impression that they are controlling you, they're not, other than planting that idea in your head and convincing you that everything that happens naturally is a result of their efforts. It's a surprisingly effective technique and, when dealing with technological issues like failing Internet connections or weird sounds, it's easy to believe that they have mystical powers. Of course, your infrastructure could still be compromised at any time by anyone with knowledge and a degree of skill. That's why it's so important to pay attention and be aware of what the risks are and how to stay in control.

Dear *2600*:

Hello again,

Thank you for your reply and happy to hear you're interested.

Here are a few things we ideally need from our side that I am obligated to state, but we're flexible about them so don't be overwhelmed.

1. We request that our post not be labeled as "sponsored content," but rather as a regular post or guest post.

2. We'll want to include up to three do-follow links in the article (some of them will be authoritative links).

3. The article must stay on the site indefinitely (we don't do yearly fees).

4. We prefer to pay in EUR via PayPal; we don't cover the transaction fees nor pay in cryptocurrencies.

Once the article is live and indexed, send us a PayPal request for payment and we'll pay as soon as possible.

Please let me know if we are good to proceed.

Cheers,

Alex

Who are you?

Dear *2600*:

As one of the very few contributors to *2600*, why the fuck have I been banned from the Facebook page? Get your admins into shape or you'll never get another donation or subscription again. Cheeky talentless morons with a power complex because they have Facebook status.

I've canceled my one percent of income after (corporate) tax BTC donations, the next subscription payment to you for my team will fail, I've canceled it.

Why are you protecting idiots while some of us are actually working hard helping people to get into tech work? You're working against everything I worked towards after being inspired by you. It's a joke.

Fix it please.

Rob

With such a pleasant demeanor, how could this have ever happened?

Dear *2600*:

Dear Hackers:

I received an email from "Hacker" so I knew it was you guys. It says "I see all your passwords, pictures and documents. If you don't pay me 50$ with Bitcoin I will expose everything."

So, I have only one question. Should I send $50 equivalent in Bitcoin, or 50 bitcoins? I await your answer.

D1vr0c

Do what feels right. Keep in mind we have all your passwords, so we can always correct you if you do something wrong.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.

As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

Who Has Your Face?

by Jason Kelley

Without your knowledge or consent, chances are high that a photo of you is in a government facial recognition database, right now. That could give access to government agencies like the FBI, Immigration and Customs Enforcement, and local and state law enforcement to compare your photo against photos of people suspected of committing crimes, potentially putting you at risk of being misidentified and invading your privacy. And perhaps the worst part: right now, it's nearly impossible to know for sure which databases you're in and which agencies can access them.

How did we end up here - and how did you end up in a facial recognition database? It's a version of the same story that privacy advocates and technologists have been telling for decades, often beginning with the implementation of a fairly unknown technology with supposedly benign intentions. In this case, DMVs began using facial recognition software, in some states more than a decade ago, ostensibly to catch fraud. The DMVs initially used the technology to compare photos of new license or ID applicants to those already in the database. But soon, other agencies came knocking. Requiring the collection of data on so many people, and implementing a way to search through it to supposedly limit crime, helped open up the door for other agencies to do the same. This is an important reminder that often all it takes for a technology to endanger a person or a group of people is to change who has access to it - and this is why it's so important to consider who has that access, and who could potentially obtain access in the future.

Fast forward a decade or so to now and, depending on which state issued your ID, you may or may not be in one of these facial recognition databases. Various agencies may have unfettered, direct access to the system itself, or they may submit images and expect the DMV to return potential matches. And this violation doesn't just happen at DMVs. Similar types of sharing occur with the photos used for passports and visas as well, and is also planned for trusted traveler programs like TSA's PreCheck. But because these agencies aren't up front about who they share access to their databases with and because they are all run differently, it's difficult, if not impossible, for the public to review their use.

Limitations differ across states as well: Georgia's DMV requires only that the agency requesting use of facial recognition be conducting a criminal investigation. Utah's DMV only requires that agencies provide an official case or report number. In contrast, Florida's Face Analysis Comparison and Examination System (FACES), the oldest facial recognition system in the country, shares access to at least 273 partner agencies (as of 2019), including 17 federal agencies. Not all DMVs allow access, and not all DMVs even have the technology: New Hampshire's DMV is prohibited by state law from using facial recognition. Oklahoma hasn't implemented it either. Depending on who issued your ID, you may be protected - for now.

To help you figure out where you fall by explaining what happens in each state, and to help put a stop to government use of the technology, EFF has launched two new websites: `WhoHasYourFace.org` and `AboutFaceNow.org`.

At WhoHasYourFace.org, you can take a short quiz that will give you a better idea of which agencies may be using your image for facial recognition. After you figure out who has your face and how they share it, you can visit AboutFaceNow.org to put a stop to government face surveillance in your community. Working with our partners in the Electronic Frontier Alliance and other local grassroots organizations, we're collecting signatures in towns all across America, and each time a multiple of 100 supporters in your area sign on, we'll deliver the message to your local lawmakers. If you live outside of the United States, you'll see other information about how U.S. government use of facial recognition may affect you, and learn how you can fight back.

And we must fight back. As more and more government agencies gain access to these databases, it becomes effortless for them to search through photos of hundreds of millions of innocent people. Once the collection of biometrics and use of this technology is standardized, it becomes much easier to locate and track someone across all aspects of their life. The problems with this are serious: this technology can be prone to error and is particularly bad at recognizing women, young people, and people with darker skin. At a time when public protest is widespread and the federal government is scrutinizing immigrant communities and criminalizing activists, law enforcement and government use of face surveillance chills free speech and threatens First Amendment-protected activity like public protest. This technology invades the privacy of everyone inside the database, and amplifies historical biases in our criminal system.

But face recognition doesn't just mean you could be mistaken for a suspect after an algorithm claims your face resembles a face in a grainy security photo. It also means that your government doesn't trust you. The FBI has scanned these driver's license databases a total of 390,000 times since 2011, according to a report from the Government Accountability Office. How many times has your face been scanned without your knowledge and despite no evidence of wrongdoing?

Thankfully, there are now more bans on government and law enforcement use of facial recognition than ever. While hundreds of millions of innocent Americans are currently subjected to facial recognition searches without ever having had the chance to opt out, we can fight back. Visit WhoHasYourFace.org and AboutFaceNow.org to take a stand.

The USPS Informed Delivery Service as a Phishing Data Source

by ~Me

In 2017, the U.S. Postal Service announced a new program called "Informed Delivery." This program would provide access to images of mail pieces being delivered along with tracking information for that specific address. It is limited to those pieces that are of letter-sized mailpieces and processed through USPS automated equipment.

To create an account, you go to `informeddelivery.usps.com/`. You start by entering an address, accepting terms and conditions that look like something from Microsoft, "warrant and represent that I am eligible to receive mail" at this address, and create your account. Account creation is the standard process: ID, password, security questions and answers, email address, phone number, and opt-in for communications from USPS and partners. They validate the email address through the common process of sending an email and having you sign into a specific URL.

What is not included in the process is any actual validation of your identity, name, address, or phone number. In other words, anyone can sign up for the service for any physical address using any email. There is nothing preventing "me" for signing up for the Informed Delivery service for "your" house.

I signed up, not because I want to track the mail coming to my house, but because I wanted to prevent anyone else from grabbing it. One nice feature is the ability to flag non-receipt of specific pieces, but I have no information about what USPS actually does about the reports. After having the service for a bit of time, and checking it only infrequently, I started thinking about the information that could be derived for social engineering from this source.

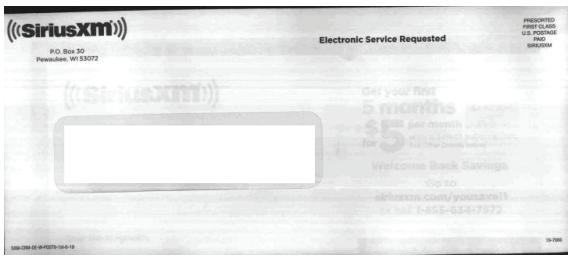
Since I already know a lot about the mail I receive, I worked with a trusted friend to access their information. They set up the account but provided access. I spent the next eight months summarizing and logging all the mail items they received to determine what I could learn about them.

What Did I Learn?

I learned a few interesting facts about the service itself:

- Newspapers and magazines are not scanned
- Full sheet (8.5 x 11 inches), even first class, are not scanned
- Online only provides information for the last seven days (including today, even if Sunday)
- About ten percent of images have "bleed through" where you can read some of the contents through the envelope.
- The online service will report "There are 3 mailpieces for which we do not currently have images that are included in today's mail." This information is not included in the daily digest email.
- The USPS recognizes certain advertisers and will include a URL for that advertiser or in competition

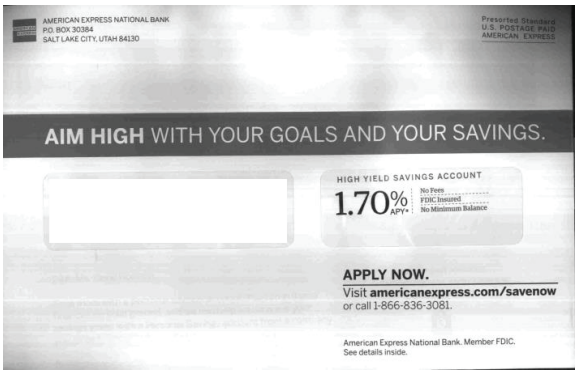
The last bullet is a little scary. Somehow USPS is interpreting the mail you are receiving and connecting that with web content. I do not know if USPS is OCR-interpreting corporate names or just simple image recognition based on feeds from those advertisers. I only hope that data is not leaking in the other direction.



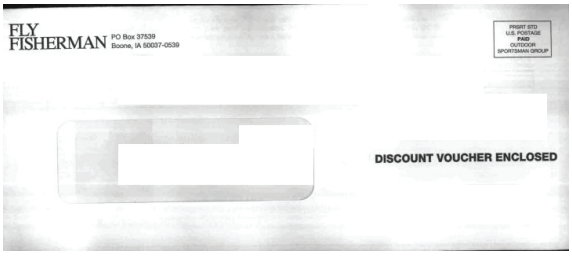
The above SiriusXM envelope is a good example of the bleed through. I used this as an example because it is safe as an advertisement - it discloses no information about my friend other than that they owned a satellite radio at one time and the account has expired. While the SiriusXM information is totally benign, other examples of bleed through leaked more sensitive information.

I learned many things about my friend. I learned that most of the couple's debt was individual - they had their own credit cards. They had several cards, each from different providers - and different affinities. This was easy to figure out from the envelopes - the affinity and provider are often on the envelope, and the creditor name is in the address window.

Their big credit was joint names - like home and vehicle - but with different banks. Their automobile and home insurance policies were with the same company.



They seem to be creditworthy, in that they get a lot of advertisements for credit. Based on this envelope, an advertisement for high-yield savings accounts, American Express thinks they have some money to place in savings - and be willing to bank online.



Based on the affinity cards, magazine subscription statements, and memberships, I know a lot about the interests, hobbies, and favored causes. Based on this envelope, a discount voucher for *Fly Fisherman* (magazine, I presume), I conclude they have some interest in the outdoors, possibly fly fishing in particular.

I also know that there was some change with their cellular service this year - they no longer receive statements in the mail. The exact change is not obvious - they could have switched to electronic delivery or a different provider.

They seem to have a few investments, based on the different mailings they get from one financial advisor firm with different fund names on the envelopes. They also seem to have multiple investments (like 401K) and accounts at multiple banks. I even know the name of their actual financial advisor and their assistants.

I know the names of some of their closer friends - based on the receipt of cards. Cards are easy to figure out based on size, pretty envelopes, and handwritten addresses.

I also know a bit about their medical conditions - at least the specialties of the medical professionals they visit (and how often).

I know who they work for - based on envelopes with the corporate name and tags along the line of "Important benefits information enclosed," "Your 401K," "Important Tax Information," and similar.

I also learned a bit about their tax situation. They get the real estate tax statements and get refunds on their income taxes. How the real estate taxes are paid or how much the refunds are, I do not know.

Based on the advertisements they receive, I can even conclude that they have a pool and a lawn, that they are over 50 years old, and that they have a bit of a lead foot (one item was a citation from an automated speed camera) - but not a *lot* of a lead foot because there was only one in eight months.

Granted, that is a lot of time to invest in research. But with the ease and low risk of that research, it is possible to have multiple targets at one time.

How Could I Use This Information?

The value of this information comes if I want to know what kind of accounts they have. It doesn't make sense to try to phish someone about a Chase credit card when they carry one from Bank of America. The same goes with regular bank accounts: someone who banks at TD isn't going to respond to a phish from Santander. Phishing over the phone is also enhanced because I know names of people who are important to my friend. I know the name of financial advisors, insurance agents, and close family/friends (based on holiday/ birthday cards).

This information also has value if I wanted to mailbox-dive or porch pirate. I can watch for specific checks (like from the IRS) or packages. Enough information is available to provide a cover story for the porch pirating - "I'm here to retrieve package with tracking number 123XYZ which was miss-delivered, here's the package."

Of course, all this information (and more, since not all mail ends up on Informed Delivery) is available by looking in someone's mailbox. But it is a lot more effort to go to a physical location on a regular basis and the risk of detection is much higher.

Disclaimers

I reviewed the disclosures in this article with the receipient. I have to conclude this article with a few disclaimers: It is illegal to misuse this service to access information about someone else. It is illegal to dig through someone's physical mail box. And, of course, it is illegal to use this information for social engineering and phishing purposes.

YAHOO GROUPS AND THE LEGACY OF INTERNET CONTENT

by Nathan Kiesman (nkizz)

Yahoo announced last year that they would be shutting down "Yahoo Groups" on December 14th, 2019. This service contains over 20 years of mailing list messages, photos, and other content that will be deleted after that date. This is just the latest of several rushed shutdowns of sites that Yahoo has become known for, the most infamous of which being GeoCities. GeoCities was the largest website host in the 1990s and early 2000s, and provided many people's first experiences with posting content on the Internet. However, it had stopped making Yahoo money, so it was unceremoniously shut down. Some particularly large sites that have been shut down include Megaupload, parts of Myspace and Tumblr, Google+, and hundreds of smaller services, sites, and web forums that make up a significant portion of the culture and history of the web.

Senator Ted Stevens is famous for saying "The Internet is a series of tubes." Although this quote is often mocked, it's actually accurate. All the Internet does is move bits from one place to another. To retrieve a web page, there has to be a server on the other end with enough disk space, electricity, and bandwidth to run it. All of these things cost money and effort to maintain. This is fine when the web page makes enough money to justify its upkeep, or it's maintained by an entity who's interested in its continued existence. However, when sites run out of money, this upkeep becomes an issue. Many will say that nothing is ever truly deleted from the Internet, however that's only true if someone is around to copy it. If the server running in someone's basement gets turned off, crashes, or the company maintaining them decides to shut them down, all the data is lost.

Barring situations like catastrophic hardware failure, web services are usually shut down because no one uses them anymore. Hosting costs outweigh the revenue from advertising, and the operator stops paying the hosting bill. So what if we can't access a bunch of web pages that haven't been updated since 2001? After all, if they're not making enough money to support themselves, than clearly not many people care about them. However, the erasure of these sites eliminates parts of the greatest trove of primary source documents that has ever existed. User content online, especially the exact kind of un-updated content that are on these legacy services, provide unprecedented snapshots of life in the late nineties and turn of the century that don't exist for any other time period. There are millions of web pages and posts created by regular people chronicling their lives, their loves, and their experiences. This may not seem like history now, but considering there are many people alive today who were born after that time period, like myself, it *is* history now. Additionally, there's a lot of knowledge stored on the "old Internet" that is still directly useful today. Every hobby imaginable most likely has 25 years of web forums, message groups, and websites with truly awful graphic design filled with advice and information that isn't available anywhere else.

However, I can't help but be optimistic. The same democratization of content creation that allowed all this content to exist also applies to preserving it. Most of the time, if content is still accessible, it's downloadable, and many people have dedicated themselves to doing so. The biggest player in this space is the aptly named Internet Archive. They maintain an archive of a staggering 330 billion web pages, and millions of videos, books, and audio recordings. They also digitize older media, like books, tapes, and records. Textfiles.com and Bitsavers.org are also archival projects with technical focuses like BBS and software archives. Archive Team is a group of volunteers who archive at risk content on online services.

As I write this, Yahoo Groups has officially shut down and even though Yahoo actively attempted to prevent archivists from accessing the site, Archive Team was able to save over 90 percent of the content on the site. Even large entities are getting into the game, like Google maintaining a Usenet archive and the Library of Congress keeping their own web archive. Many of these projects, like so many other online projects, rely on a combination of volunteers and employees, and are funded by donations from individuals and interested corporations. Also, like many other Internet projects, there are ways for individuals to help. You can upload media to the Internet Archive, nominate web pages to be archived, run "warrior" programs that download web pages, and donate to the various archive organizations. Additionally, for personal data, the GDPR requires sites to allow users to export their data, so people can backup their data before a site becomes defunct.

Like any other form of media, online media requires maintenance to preserve it. Digital preservation presents its own set of problems and challenges to archivists of the 21st century that we are still learning how to overcome. But as long as there are people creating, there will be people dedicated to preserving those creations too.

The Freephones of Whidbey Telecom

by Curtis Vaughan

Were it not for *2600,* I probably would have little interest in payphones. Now, whenever vacationing, any stray payphone garners my full attention. Whereas my travels almost never take me to exotic places, I'm sure most of the payphones I've discovered have already been featured in the magazine's inside flaps.

On a recent sojourn to Whidbey Island, just north of Seattle, an island across which surely many local 26-hundreders have wandered, I noticed some unique (at least to me) public phones. Their most peculiar aspect was that they were unmistakably not *pay* phones, as there was no method by which these phones could extract a payment from the user. No, these were truly public or, I'll venture to coin: freephones.

The first one I encountered was outside Langley City Hall. Although a very unpresumptuous telephone, it included a telephone book! An actual book with telephone numbers of local businesses and individuals, which is released annually. I was perplexed. Had I slipped into a TARDIS and been slingshotted back into another time?

Later that day I found yet another freephone at the Langley docks. This one, although denuded of a phonebook, enjoyed an appropriate seashell halo. These and numerous other phones are the property of the island's own Whidbey Telecom. In total, Whidbey Telecom reports that there are 34 such freephones. According to an article from 2012, WT decided to repurpose many of the payphones into free phones for local calls.

Of course, I had to check whether these phone actually worked. As I expected, when I tried calling my own cell phone (not a local number!), a recording explained that calls to mobile phones and numbers out of area could not be completed.

I was happy to find out that Whidbey Telecom intends to host a web page with a map of each freephone. We can only hope they will also have pictures of each freephone as some are apparently quite unique. For example, I only found out later that there is a phone booth in Langley that has been specially fitted with metal siding by a local metal works. Look it up on the web at `www.heavymetalworks.com/2008/07/phone-booth-make-over.html`. Pretty cool.

POINT OF SALE SHENANIGANS: AUTHORIZED UNAUTHORIZED TRANSACTIONS

by Ryan Clarke

The Defense Commissary Agency operates the commissaries on U.S. military bases. For those unfamiliar, the commissary is the supermarket on a base. An important difference between a commissary and a civilian supermarket is that the baggers are volunteers. The baggers will also offer to bring your newly purchased groceries to your car and it is normal to tip them a few dollars for their efforts.

Considering most people do not carry cash on their person these days, it is common for a customer to ask for cash back during the transaction in order to tip the baggers. Many times the customer wants to use a credit or charge card, because don't we all want those points? Unfortunately, the point of sale (POS) system does not allow cash back on anything except debit cards. You must notify the cashier to split the transaction between a debit card for the cash back and a charge or credit card for the remainder of the total. Easy stuff.

Then it changed. Recently, the commissary at my local base changed their POS system to a newer version, and now the customer can request cash back themselves using the customer-facing terminal. I know, I know, this has existed for a long time, but the U.S. government is not always up to speed with modern systems.

Here is the glitch. I informed the cashier that I needed cash back for the tip, and she advised me of the new procedure. I placed my AMEX in the machine's chip reader to begin splitting the transaction. However, after reading the chip, the device asked me if the total transaction amount was correct. I selected "no," thinking it would allow me to then enter a new value. The computer canceled the transaction and asked for a new card. It irritated me slightly, but it was not a big deal and I got my debit card out of my wallet to place in the chip reader. I informed the cashier what happened, and she gave me a confused look, considering the receipt printer output a receipt. I told her that I canceled the transaction, and that I never entered my PIN or submitted a signature. She said it went through and handed me the receipt. There it was, a confirmed charge on my AMEX, seconded by my AMEX app chiming in with a notification of a new transaction. I walked away with my bagger, and I was utterly confused, but also curious.

Unfortunately, I am one of those people who doesn't carry cash. I had to sheepishly inform my bagger, walking with me to my car, that I could not tip her and that it would be unfair for me to allow her to unload my groceries into the car. Embarrassing, but I generally don't like them helping anyway; I'm perfectly capable of loading my car.

So there you have it. A POS system that allows a transaction to complete without proper PIN entry or signature input. I think the readers of this magazine could think of the nefarious shenanigans a ne'er-do-well could do if they had a card in their possession that they did not own and came upon a POS with the same flaw in its design. Of course, I also trust that no one reading this magazine would do such a thing. So, that begs the question: is the software problem unique to the commissary on my base, or does this work at other locations, specifically non-Department of Defense locations? Happy shopping.

lxa4rh3xy2s7cvfy.onion

That is our SecureDrop address where you can submit leaks, tips, and files of all sorts while maintaining your complete anonymity.

Here's how it works. Get the Tor browser (www.torproject.org) if you're not already using it and go to that .onion address above. Attach any documents you want us to see, and hit "Submit Documents" and we will receive them without any identifying info. You can also send us a message and we can reply back to you, again without us knowing anything about you!

We've already gotten some really interesting material. Please consider adding to the pile! Voice recordings, videos, tax returns... well, you get the idea.

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

CITIZEN ENGINEER

by pt, ladyada, and John Edgar Park

Controlling MagicLight Bluetooth Bulbs

Internet of Things devices are inexpensive, popular, and incredibly fun to hack! If you shop for IoT devices, there's about a 50/50 split between Wi-Fi and Bluetooth LE (BLE). In this article, we'll take you through the process of "hacking" a low-cost off-the-shelf BLE light bulb - all you need is an Android phone. If you must, you can also use an iOS device or even a desktop with Linux (using BlueZ) or Windows (using Microsoft's Bluetooth LE Explorer).

The BLE bulb we'll be exploring today screws into a common socket and can display any color when controlled with the app. But how does it all work? What if you do not trust their app? And what if we want to control the bulb ourselves? Say have the light act as an ambient indicator for our CI build status, network ping time, or when our favorite streamer comes online! We will be using the MagicLight Bluetooth bulbs: `www.magiclightbulbs.com/collections/bluetooth-bulbs` (about $20 just about everywhere).

Bluetooth LE has many terms that need to be understood so you can know what is talking to what, and how. Let's start with some BLE basics. The two modes of BLE devices are:

- *Broadcasting ("advertising") Mode* (also called GAP for Generic Access Profile).
- *Connected Device Mode* (also called GATT for Generic ATTribute Profile).

GAP Mode deals with broadcasting peripheral advertisements, such as "I'm a device named LEDBlue-19592CBC" as well as advertising information necessary to establish a dedicated device connection if desired. This mode has two device roles involved:

Peripheral - The low-power device that broadcasts advertisements. Examples of peripherals include heart rate monitor, smartwatch, fitness tracker, iBeacon, and a smart bulb.

Central - The host "computer" that listens to advertisements broadcast by peripherals. Central is often a mobile device such as a phone, tablet, desktop, or laptop.

Advertising is information sent by the peripheral *before a dedicated connection is established*. All nearby centrals can observe these advertisements. When a peripheral device advertises, it may be transmitting the name of the device, describing its capabilities, and/or some other piece of data. Central can look for advertising peripherals to connect to, and use that information to determine each peripheral's capabilities (or services offered - more on that below).

GATT Mode deals with communications between two devices once they are connected, such as between a heart monitor and a phone, or between your phone and a smart bulb. GATT mode also has two device roles:

Server - In connected mode, a device may take on a new role as a server, providing a service available to clients. It can now send and receive data packets as requested by the client device to which it now has a connection.

Client - In connected mode, a device may also take on a new role as client that can send requests to one or more of a server's available services to send and receive data packets.

A device in GATT mode can take on the role of both server and client while connected to another device. There are a few terms to be familiar with to get the information out and usable:

Profile - A predefined collection of services that a BLE device can provide. For example, the heart rate profile, or the cycling sensor (bike computer) profile. These profiles are defined by the Bluetooth Special Interest Group (SIG). For devices that don't fit into one of the predefined profiles, the manufacturer creates its profile. For example, there is not an official "smart bulb" profile, so the Magic Light manufacturer has created its unique one.

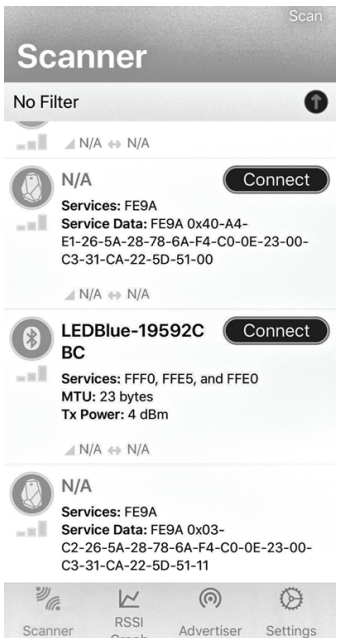
Service - A function the server provides. For example, a heart rate monitor armband may have separate services for device information, battery service, and heart rate itself. Each service comprises collections of information called characteristics. In the case of the heart rate service, the two characteristics

are “heart rate measurement” and “body sensor location.” The peripheral advertises its services in GAP mode.

Characteristic - A characteristic is a container for the value, or attribute, of a piece of data along with any associated metadata, such as a human-readable name. A characteristic may be readable, writable, or both. For example, the heart rate measurement characteristic can be served up to the client device and reports the heart rate measurement as a number, as well as the unit string “bpm” for beats-per-minute. The Magic Light server has a characteristic for the RGB value of the bulb, which can be written to by the central to change the color. Characteristics each have a Universal Unique Identifier (UUID), which is a 16-bit or 128-bit ID.

Packet - Data transmitted by a device. BLE devices and host computers transmit and receive data in small bursts called packets, much like other radio or networking protocols!

OK, now that we know the terminology, it’s time for reading and writing data to characteristics to Magic Light. An excellent way to get familiar with BLE is to read and write to individual characteristics using the Nordic nRF Connect app for Android and iOS (`play.google.com/store/apps/details?id=no.nordicsemi.android.mcp&hl=en_US`)



The Android version is much more feature-rich than the iOS version. That’s what we are using. Again, you can use different tools on desktop devices, such as Bluetooth LE Explorer (Windows 10) or BlueZ (Mac). Once you launch the app or scan within your program, you’ll see a list of BLE peripheral devices that are broadcasting their advertisements.

Screw the bulb into a standard lamp socket and turn it on, then re-scan/refresh until you see the LEDBlue device and click on the Connect or Pair button. (Make sure it’s not connected on your phone - only one central at a time can connect to the bulb peripheral!)

Once connected, look at the services available. There are three mysterious services, with codes 0xFFF0, 0xFFE5 and 0xFFE0. There isn’t much helpful info here about what these services are, so we’ll need to dig deeper into the characteristics to find what we need.

Click to explore the service with UUID of 0xFFE5. You’ll see that it contains five characteristics called red, green, blue, white, and RGBW. Bingo! Try writing values from 0x0~0xFF to each of the first four characteristics using the “Write Value” dialog box. You should see the bulb immediately change color. *Hacker voice: “I’m in.”*

In addition to a characteristic each for red, green, blue, and white, there is a combined characteristic for RGBW (although the white element is not enabled in this characteristic for some reason).

To write to the RGB combined attribute, use the characteristic UUID FFE9. The byte array looks like this: `56 FF FF FF 00 F0 AA`

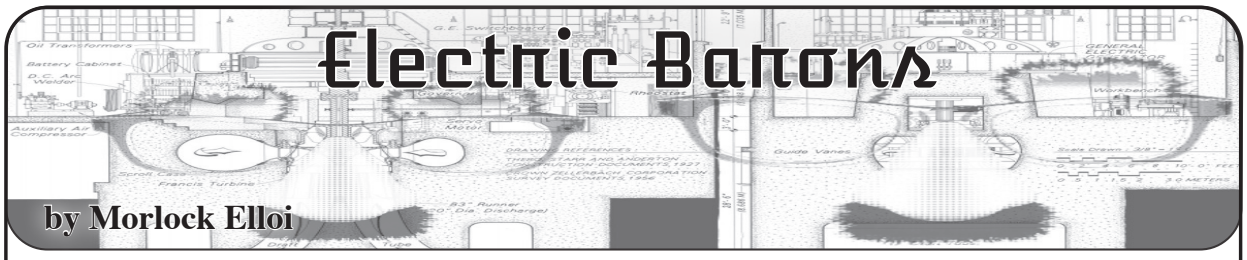
The first and last bytes are required (we figured these out by packet-sniffing the BLE connection from the app). You can set the red, green, and blue values in bytes 2-4 and the range is 00-FF (or 0-255 in decimal).

Now that you know how it works and how to control it, you can use open source BLE tools to connect to and control the light bulb with your computer acting as the central. JavaScript fans can use Web Bluetooth (available in Chrome). Python folks can try Bleak. Linux fans can use BlueZ.

Now that you know the basics of BLE, try scanning, connecting, and controlling other IoT devices you own to uncover their secrets!

Good night and good luck.

Electric Barons



by Morlock Elloi

Modern technology of computing machines provides plausible disguise for the ideology of power. This ideology permeates the infrastructure and its design methodology, disarming opponents with pseudo-technological excuses. The two need to be separated.

In the Name of the Infrastructure

If you live in San Francisco's Potrero Hill, there are several rational choices for getting to a Mission bar. Public transport - take 10 to SoMA, then 16 to Mission. Bicycle: down De Haro, then 17th. These choices frame your notion of "Mission bar." Going there is contingent on weather, available time, and mood. Some Mission bars are out of consideration - too hard to park, too far away from transport, too much feces on the sidewalk. Some are rather convenient and thus become the natural choice. Over time, the inconvenient ones are forgotten. You will never go to Dovre Club.

This happened because MUNI made particular decisions on bus routes, SFMTA determined parking availability, the city planners laid down streets as they are now, and the city politics resulted in the current sidewalk feces distribution. Your natural bar choice was engineered by many contributors over long time. This is how cities are, and we got used to it. Enabling efficient traffic requires choices to be made - by politicians, bureaucrats, city utilities, and services. One is free to use this infrastructure in many ways... that it allows one to use it. It is impossible to step out of the infrastructure, and this is why having a say in its workings is important. On your way to the convenient bar, you may consider all of this and perhaps table some thoughts for future actions.

Cities are shaped through constant clash between residents, real estate owners, investors, builders, politicians, parties, and action groups. Anyone vaguely familiar with city politics knows how hard and slow it is to change anything. When a MUNI bus stop is too far away from your destination, or your street has potholes, or there are too many cars, you will not argue with the bus driver, pavement contractors, or car drivers. You may contact your district supervisor to bring up the issue at the next SFCTA/SFMTA meetings. First, you need to find out that SFCTA and SFMTA exist, and what they do - it's all in the public record, and not so hard to figure out. Eventually, your intervention may bear fruit and you will have a drink at Dovre Club. Or you may decide to move to some other place, with more agreeable politics and infrastructure.

Different cities have different mentalities and have been influenced by different politics and development strategies. They all have one thing in common: city workings are observable. Changes in the city scene are obvious - construction sites, traffic jams, traffic enforcement, parking tickets, cops on the beat. The infrastructure is visible: streets in your neighborhood have bike lanes or they don't, they are congested or not, they are one-way or two-way. This visibility, in turn, means that one is in the position to make informed choices for the action.

What happens when another kind of traffic, communication between people, gets engineered by multiple interests? Our "natural" ways to communicate are verbal, visual, and touch - all physical and requiring proximity of the other person. Anything else requires some form of technology and infrastructure - from printed pages to fiber and satellite relays. Who are the builders, investors, real estate owners, politicians, action groups, utilities, and services companies for this infrastructure? What does the road map look like? How does one initiate the change?

This is important to know, because the state and the layout of *these* roads may affect you far more than the city traffic jams. It may determine who you will know, who your friends and adversaries will be, what education and job you will have, who your future family will be, and how you will die. It is important to be able to see and recognize this infrastructure the same way the traffic jam or sidewalk feces are recognized, because one should not trust PR departments and experts' claims that

these things are or are not there. Effective politics and activism happen only after one spots traffic jams and feces.

But communication and data processing infrastructure are not visible, and politics and ideologies of its builders are far from obvious. There are many reasons for it, but this article is not about the history. It will try to show that politics and ideology of this infrastructure do exist, and how they affect people.

The ideology of the infrastructure goes deep and is often invisible to the involved actors. The participants generally believe that they are doing the best possible job. What is specific to engineering is that the governing ideology is often internalized as a technical issue, and is so presented to the insiders and the outsiders. The presumed difficulty to understand technicalities is used as a barrier to shield the ideology from the outsiders. The baffling part is that it also works on the inside. It is extremely hard to penetrate this construct and separate the ideology from the technology: the amount of its inherent nonsense can shame any belief system known to man. Yet it must be done.

One aspect of this ideology is centralization. Centralization of traffic, directories, databases, personal information, you name it. That center is somewhere where you are not. People interfacing machines built under this ideology are called "users." This is telling, as those, for example, driving machines or being driven by machines are called differently - drivers, pilots, or passengers. The prospect of having millions obey machine instructions designed by the few is very seductive. In the previous times, only select novelists, directors, songwriters, and dictators enjoyed this replicative amplification of consequences, mostly for entertainment, enlightenment, and indoctrination of the audience. Today, the code determines conversations, money flows, employment, entertainment, and the rest of life.

Perhaps the most sinister aspect is that it captures the energy of activism, which adopts the ideological canons and builds the same dystopian constructs, on the premise that they are now operated by the good guys, as if an Open Source cage is anything but a cage. The underlying fallacy, that the power will be used only for good purposes, becomes obvious always too late, when the energy and trust have been exhausted. Thus, the useful idiots complete the ecosystem and seal it against the alternatives.

The infrastructural issues considered here are fundamental in nature, not about kinds of traffic on top of the infrastructure (social networks, search monopolies, etc.). The list is not exhaustive - only three examples scattered across a huge domain. It is about the constraints the infrastructure imposes and inertia against the change that it creates, pretending to have technological justification, and about the need for a major redesign. It is obvious that this is a huge problem and uphill struggle, but it is a lesser problem than continuing down the current path. And finally, this is not a Luddite argument against the machines. We do need the machines, but designed and operated under a different ideology. What that ideology shall be we should determine through the established social institutions. The present we experience is not a technical problem.

The Server Tax

Servers are computers living in large numbers in buildings where space, air conditioning, power, and bandwidth pipes are abundant. These are called "server farms" or "colocations" if servers are owned by multiple parties. Large enterprises own multiple farms. It's hard to estimate the total number of servers, but taking into account the 25 million annual server-class CPU chip sales, and using four years as a typical server life span, a round number of 100 million active servers is reached.

On the other hand, there are around 2.5 billion smartphones in the world, and at least as many other edge computing devices (PCs, tablets, smart TVs, IoT). Taking into account that the average server is ten to 100 times more "powerful" (in terms of CPU and storage) than a smartphone, it appears that the total edge computing power is likely greater than the total power of the servers, with trend favoring the edge. The "edge" here means all computers in the hands or homes of individuals, businesses, etc. The sheer weight of the edge silicon (metal from which chips are made) will be orders of magnitude higher than the weight of the total server silicon, if it is not already so. Still, as there are several billion edge equipment owners, and only a few million server owners, with less than a few hundred of the large ones, the server owners control computing power

thousands and millions of times over that of the average edge equipment owner.

Computing power-wise, servers do not appear to be a dominant component of the whole system. Yet today, servers control everything. Pretty much all edge devices talk directly only with servers. The centralization makes the traffic pattern look rather odd: as if residents of all 2612 San Francisco streets, when visiting another one, would all have to pass through the intersection of Market and Van Ness.

Almost every single "app" and "website" is based on this paradigm. There is a server and there are thousands/millions/billions of "clients." The underlying motivation is that the owner of the server has control over multitudes of clients. The edge equipment owners themselves do not need this centralization any more than San Francisco residents need to pass Market/Van Ness every time they go to the grocery store, but they have little choice. This is considered normal - from dreams of every startup that few will make and operate something that billions will use, to schools where engineers learn to make the servers work and to make the clients work.

Technical arguments for data storage concentration are weak. Today, the entire contents of Wikipedia can fit on a smartphone. Street maps of all places a person will visit in a lifetime are only a few gigabytes in size. The amount of the "new" content is relatively tiny. Yet servers insist on dishing out small crumbs of information from their centralized storage when it is required, enabling the server owners to know what edge devices are doing and when, almost like giving some change to a child to buy one ice cream from the store.

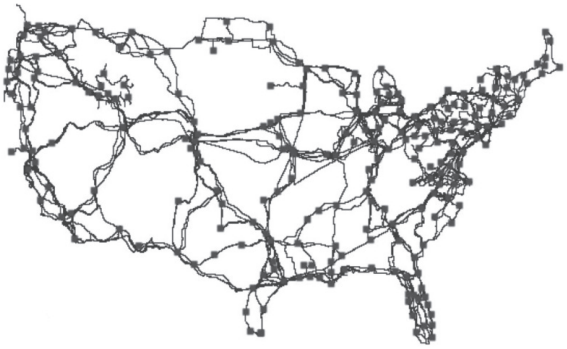
Can today's popular services exist with decentralized storage? The answer is yes, and there is empirical proof: as countries assert their sovereignty, the companies providing these services are compelled to move storage of data related to citizens to their respective countries, and make them subject to local laws. It doesn't seem that any of these services suffered because of this. What works on the country level will certainly work on any other level: city, municipality, household.

Technical arguments for computation centralization are even weaker. Edge devices do not benefit from it, for the simple reason that, per device, there is far more power in the edge device itself than in the tiny fraction of the server apportioned to the device.

On the technical side, there are solutions for distributed applications, naming, storage, resource discovery, and source routing, so interventions against the server canon are political. The edge has to become its own center. It involves regulating against faraway processing and storage. There are parallels in the urban politics world: road builders never managed to make everyone go through the single toll ramp, many cities built barriers to chain stores, exploiting and parasitizing on human social and other instincts is customarily regulated by law: there are very few places in the world with industrialized prostitution. Political instruments already exist.

Cyberslum Concierge

The communications infrastructure consists of long-haul backbone of fiber lines, which in the U.S. more or less follow roadway infrastructure, and of Internet Service Providers (ISPs) that provide "the last mile" connectivity between the backbone and individual participants. This is the layout of fiber in the continental U.S., from "InterTubes: A Study of the US Long-haul Fiber-optic Infrastructure," R. Durairajan et al 2015.



This looks more or less like the physical roadway infrastructure, where highways connect cities, each of which has its own street grid.

But there is a difference.

While you can get into your car in San Francisco and drive all the way to your friend's apartment building in New York, enter the elevator, and visit your friend, you cannot do the same with information packets for your friend. The information packet will be stopped at the building entrance. The desk clerk will check if you friend is expecting the packet. If your friend did not alert the desk one minute or less before the expected packet arrival, your

packet will be thrown out. In other words, you cannot send a surprise gift to your friend. The interesting question is how do you alert your friend? He cannot ask you, as your building has the same unsolicited packet policy. You two can never exchange packets directly. There have been numerous attempts to trick the entrance desk into letting unsolicited packets in, but they were never reliably successful, and thus never became the basis for widespread direct connectivity.

Fortunately, there is another business nearby that will accept packets from anyone. In the machine world it's called a server. Both you and your friend can send packets to the server. When you send a packet to the server, you alert your building desk clerk that you expect something back from this particular server. Your friend must do the same. In this way, the server acts as a meeting point to enable exchange between you and your friend. Needless to say, the server has to like both of you, and it is usually because it profits from each.

There are thousands of times fewer servers than apartments, and the initial technical rationale for this entrance triage and server middlemen was that there are not enough street addresses to cover everyone, so only servers get to have public entrances for themselves, while everyone else shares the building address and must deal with the desk clerk (by the way, the building street address itself changes, sometimes several times a day, so you cannot count on it being known). The server addresses do not change. You have no choice but to use the server as middleman if you want to communicate with others. Except that there is a choice, a new style of addressing, available since 1998, called IPv6. It is not catching on, which may have something to do with the lucrative server business. Even where IPv6 gets implemented, ISPs tend to cripple it or require, through contracts, that you will never receive unsolicited packets (in technical parlance, "run a server"). While you and your friend must use the intermediaries, server owners don't have this problem, so, for example, *The New York Times* is directly accessible because it has its own servers.

This two-tiered system - on one side the inability to accept information directly and to have its own permanent street address for ordinary people, and on the other side the privileged position for server operators - has deep influence both on edge participants and on the way edge computers are designed and used. The edge equipment owners acquire the mentality of a homeless person with no permanent address - and consider it normal. The edge computers must be tethered to various privileged servers, as they cannot communicate directly. This has shaped the minds of engineers and frameworks and tools that they use and design. This is where centralized social networks and email providers stem from. While this has not been a technical obstacle for 20 years now, it still defines the entire computing landscape.

The intervention is simple: lobby for unrestricted IPv6 and permanent addresses for everyone.

Celebrity-Based Security

During World War Two, Germans were using Enigma machines to encrypt worldwide military radio traffic, including the one between the central command and submarines. The Allies managed to break the Enigma encryption in 1941, but they didn't tell the Germans. Instead, they allowed some ships to be sunk, and in other cases the scout airplanes would "accidentally" spot the submarine whose position was known from decrypted traffic, so that the Germans would not suspect a broken cipher.

The Germans eventually found out about this in 1973, and had a hard time believing it. Many texts have been written on the topic of the hubris of Enigma designers. This three-decade gap between successful cryptanalysis and public learning about it is typical in cryptography, and should be accounted for when designing security methods. It does not make cryptography useless - the cryptanalysis will not be used against low value targets, and some ships can be sunk.

In general, the cryptanalysis (breaking a cipher) is as hard, if not harder, than the cipher design itself. It took the Allies considerable effort - many man years - to perform this cryptanalysis feat. One obvious way to stay ahead of the cryptanalytic curve is to keep introducing new ciphers. In World War Two, the machines executing both the encryption and the cryptanalysis were electromechanical and expensive to construct, so introducing new ciphers was a very slow process. Yet the Germans

modified their Enigma machine three times in ten years, once in the middle of the war.

One would think that today, when all cryptography is done in software that can run on any computer, this staying ahead of the curve principle is a norm. It is not. On the contrary, the ideology of cryptography preaches the exact opposite: never do custom cryptography, always use the standard one that's approved by the experts who know better than you. Like in every ideology, there is truth in this: designing strong ciphers and strong security systems is very hard. But it completely misses the balance of power relationships and threat models. It is also obvious that the cipher designer hubris is still a cryptographic constant.

While it is hard to estimate how many "licensed" experts participate in the design of ciphers, it is possible to estimate the upper boundary: the International Association for Cryptologic Research has about 2,000 members. On the other hand, the unverified lower estimate for the number of mathematicians working for just one state agency (NSA) is about 10,000, so we can assume that worldwide there are at least ten times more brains paid to cryptanalyze than engaged in designing ciphers, and this ratio could easily be 100 times. It gets worse: the total number of block ciphers widely used today ("approved by experts") is four (AES, Camellia, ARIA, ChaCha20-Poly1305 - all published between 1998 and 2007), and the total number of key exchange protocols deemed secure and widely used is also four (RSA, DH, EC, GOST - all published between 1976 and 2005). Compromise of either key exchange or block cipher compromises the whole system. At this point, tens of thousands of cryptanalysts had ten years to compromise four algorithms, designed by less than a dozen experts. The official mantra to use these four is part of the power equation mandating uniformity of the protective gear, and is permeating both academia and the industry. On the other side, no diplomatic service, military, or government communications appear to use any of these: "Serious countries (USA, UK, Germany, France) do not use foreign algorithms for high-security needs" (Eric Filiol, head of research at ESIEA).

Here again, we see the "few for many" principle rearing its ugly head, facilitating centralized control and related compromises.

Should everyone design their own ciphers, with millions of companies and individuals designing their own terribly weak ciphers, a new one every year? There is no automated way to cryptanalyze even naively weak ciphers (and many would make not so naive ones). Tens of thousands of cryptanalysts cannot begin to chip away even at the weak security of millions of new custom and unpublished ciphers every year. First, they would have to figure out what is the cipher, and then break it. It takes time, even if it is a variant of ROT-13.

What would happen is a leveling of the playing field, engaging brains against brains, on the scale that cryptanalysis could not keep up with. The targeted cryptanalytic approach would still work, but with a limited amount of targets, and would likely be no different in the overall amount of breaches than today's successful targeted hacking of computer systems. The mass snooping would cease to exist.

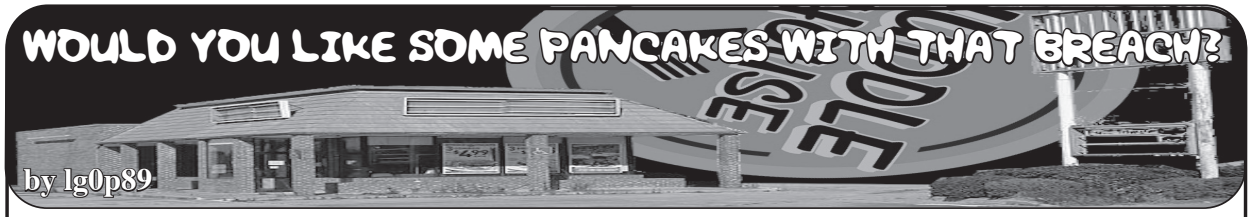
The compliance with the cryptographic ideology which forbids custom ciphers boggles the mind, as it prevents the only hope for changing the power imbalance: recruitment of raw brain power.

The intervention is straightforward: as different applications do unique things and have unique code, they should have unique ciphers, and change them often. The probability that your system will be broken into by targeted hacking will remain roughly the same, and the probability that your system is a continuously open book for the major adversaries goes down to zero.

What Can Be Done?

The luxury of not caring for the infrastructure and leaving it to the experts and industries involved must be abandoned. Efforts on superstructure levels (information monopolies, copyrights, data ownership and collection, freedom of speech, etc.) are pointless when the infrastructure embodies and petrifies diametrically opposite models. No amount of smoke and mirrors and assurances that the operators are honorable and law-abiding will ever change that. This infrastructure was successfully removed from the public view and it's time to do hard work and start looking at it.

WOULD YOU LIKE SOME PANCAKES WITH THAT BREACH?



by lg0p89

Seemingly, a restaurant or restaurant chain would not be a high value target placed near the top of the target list, as they don't have or retain any personally identifiable information or PII (e.g. name, Social Security number, medical records, and other confidential data). Curiously though, this industry has much the same data that others do, which is very sale-able. The primary data here for the attackers are the credit card numbers. These may be monetized in a few different ways which we have seen time and time again with bulk sales - or simply creating new physical credit cards via placing the data on the magnetic strip. One such restaurant that faced these difficulties in 2019 was Huddle House. Huddle House, headquartered in Atlanta, is a casual dining and fast food operation.

Attack

Huddle House was targeted for an attack which was very successful. They released a statement on the malware infection. The specific system breached was the point-of-sale (PoS) system, just like other retailers, which was infected with malware at various locations. The PoS system was a third party's. The malware was coded to allow attackers to steal credit card information used by Huddle House's clients (name, credit or debit card number, expiration date, cardholder verification number, and service code). With this data, you could have a great shopping experience on someone else's dime.

Unfortunately, the variant of malware was not disclosed. This would have been very useful, not only for research purposes, but also for other businesses to learn from. This would include what to watch for, how it worked, etc.

The malware delivery system was interesting, as the attackers gained remote access by exploiting the third party's assistance tools, allowing the third party to deploy the malware. This was done throughout every Huddle House, and made it to an estimated 341 locations. With the malware being spread across all of these locations, the reach was extended every time a client used their credit or debit card.

This was noticed after a bit of time had lapsed. The infection span was from August 1, 2018 to February 1, 2019. In essence, anyone using their card for the seven months during the infection probably had their credit card information at risk

Detected

Another interesting aspect to this is that Huddle House did not detect the malware. They perceived no indication of any issue. This was detected by law enforcement and Huddle House's credit card processor. Seemingly, Huddle House would have noticed something in the logs.

Post-Attack

After the notification, the investigation began. Initially, the business had no idea how many of their locations were involved or the number of customers affected. They contracted with a third party forensics company and worked with law enforcement within 24 hours of becoming aware.

The business notification was for their clients to monitor their credit card statements and possibly call the credit card companies to request new cards. While this is helpful yet obvious, this still created work for their clients now and in the future.

Lessons (Not) Learned (Still)

The Huddle House story is much like most other breaches - there is nothing really exciting. What does make this a bit more interesting is the attack itself. The old saying is you are only as strong as the weakest link. This continues to be the case. When a business allows another organizations (third parties) access to their network and/or data, the business is allowing not only the third party into the network, but also the baggage and issues with their system, which come along for the ride. These likewise have full access to all that the third party does, and much more.

There is a massive retailer with stores throughout the U.S. allowing third parties access to their network. They are allowed to use this authorized access to upload invoices or various other functions. As they connect and log in, any infection they have may be shared with that system.

This is the issue facing cybersecurity and supply chain management. While the business certainly has some level of transparency into their network, in general this is not prevalent with third parties. Gaining access to cybersecurity data for the third parties is difficult, as this is new ground for the vendors and, naturally, they don't want to tell others of their vulnerabilities for fear this information could be accessed by unauthorized parties and exploited. The System and Organization Controls (SOC) report (along with other reports) shows at a certain day and time what their vulnerable points were. This in the wrong hands could create a large issue.

As time passes and these requests become greater in number and frequency, the attitude

will slowly change. Until then, start and continue to ask for these and put them in your contracts. The business and the third party vendors have to understand this is a vulnerability attack point. If everyone continues keeping their heads in the sand hoping all will be well, all won't be well. Just ask the national retailer whose HVAC vendor introduced malware into their system which breached the PoS system just before the largest sales period of the year.

Also, it is notable that Huddle House had no idea there was a problem until they received the call. If an estimated 341 sites are affected and the credit card data is being sent to the command and control servers in small or large blocks of data, it would seem that the cybersecurity team would have been able to look at the logs and notice the activity due either to the amount of data or frequency. Granted, the data logs can be large, however, that's why they sell SIEMs. A program can also be coded to parse through this looking for trends.

Resources

Abrams, Lawrence. Huddle House Fast Food Chain Suffers Data Breach in POS System. www.bleepingcomputer.com/news/security/huddle-house-fast-food-chain-suffers-data-breach-in-pos-system/

CU Today. Restaurant Chain Announces Data Breach. www.cutoday.info/Fresh-Today/Restaurant-Chain-Announces-Data-Breach

Huddlehouse. Important Security and Personal Data Protection Notification. www.huddlehouse.com/data-protection-notification/

Muncaster, Phil. Huddle House Suffers POS Malware Breach. www.infosecurity-magazine.com/news/huddle-house-suffers-pos-malware

NNT. Huddle House Restaurant Chain Suffers POS Malware Breach. www.newnettechnologies.com/huddle-house-restaurant-chain-suffers-pos-malware-breach.html

The Paypers. Huddle House Announces Security Breach, POS System is Affected. www.thepaypers.com/digital-identity-security-online-fraud/huddle-house-announces-security-breach-pos-system-is-affected/777240-26

An Introduction to Chaff - an Anti-Forensics Method

by Andrew Ziem

For aircraft, chaff is a physical countermeasure that confuses radar by making it seem like there are additional aircraft in the sky. Chaff protects the aircraft by misdirecting radar-guided missiles.

Likewise, BleachBit Version 3 introduces a basic chaff system that creates files to confuse digital forensics. Think of it also like the metaphor of the needle in the haystack. The needle represents the files you want to keep private, and the chaff is the haystack that makes the needle difficult to find because the forensic investigator has more junk to sift through before finding all the needles.

Does this imply that using BleachBit to delete other data, such as browser history, is counterproductive? No. Use BleachBit to remove any private data you don't want found. However, there may be private data you decide to keep or forgot to clean, and chaff is one of an array of options to protect this private data. Of course, please also consider other options such as encryption!

BleachBit uses a statistical model called Markov chains to learn a document as inspiration and then uses it to generate random text that is difficult for an investigator to fingerprint. At a glance, the chaff files seem to be English, but a closer inspection reveals they are nonsense, so do not spend much time reading them looking for any wisdom.

BleachBit 3.0 comes with two statistical models. The first model was inspired by Hillary Clinton's emails as released by the United States Department of State. Please remember that FBI documents indicate Clinton's IT guy used BleachBit to wipe emails from her private server, and now BleachBit can also do the opposite: generate Clinton's emails.

The second model was inspired by *2600* to yield more interesting keywords that might show up on the forensic investigator's scans.

When making chaff files, either leave them undeleted or delete them without shredding them. Shredding them would remove any trace, which would be counterproductive, but deleting them without shredding can slow down the forensic investigator.

While BleachBit itself does not implement any steganography, a savvy user can consider hiding private data in the seemingly-useless chaff files. Just this possibility implies a thorough digital forensics investigation would require examining the contents of the chaff files rather than whitelisting them.

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.

April 24-26
Vintage Computer Festival East
InfoAge Science Center
Wall, New Jersey
vcfed.org

May 2-3
Maker Faire Kyoto
Keihanna Open Innovation Center
Seika, Japan
makezine.jp/event/mfk2020

May 5-6
RVAsec
University Student Commons
Virginia Commonwealth University
Richmond, Virginia
rvasec.com

May 8-9
THOTCON 0xB
Chicago, Illinois
thotcon.org

May 14-15
Converge 2020
Cobo Hall
Detroit, Michigan
convergeconference.org

May 15-17
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

May 21-24
GPN20
ZKM and HfG
Karlsruhe, Germany
entropia.de/GPN20

June 12-14
CircleCityCon 7.0
The Westin
Indianapolis, Indiana
circlecitycon.com

June 19-21
Teardown 2020
PCC Cascade Campus
Portland, Oregon
crowdsupply.com/teardown/portland-2020

July 9-12
Hackmeeting 0x17
CSOA Forte Prenestino
Rome, Italy
www.hackmeeting.org/hackit20

July 31-August 2
HOPE 2020
St. Johns University
Queens, New York
www.hope.net

August 6-9
DEF CON 28
Caesars Forum, Harrah's, Linq, Flamingo
Las Vegas, Nevada
www.defcon.org

August 11-18
BornHack
Funen, Denmark
bornhack.dk

September 25-27
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
2k20.balccon.org

October 8-9
Security B-Sides MSP
Water Street Inn
Stillwater, Minnesota
bsidesmsp.org

October 22-23
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.org

November 6-7
PhreakNIC24
Clarion Inn & Suites
Murfreesboro, Tennessee
phreaknic.info

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

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).

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. Retails 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 RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://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

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

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 community and earn money with freelance programming jobs. All hats welcome!

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.

Announcements

TOG IS DUBLIN'S HACKERSPACE. We run regular events in coding, lock picking, electronics, craft, cad, wikipedia editing, electronic music, brewing, science fiction book club, and monthly socials. We recently celebrated our 11th birthday! TOG is run and funded by volunteer members and we are always looking for new hackers. website: www.tog.ie email: info@tog.ie address: 22 Blackpitts, Dublin 8, D08 P3K4, Ireland.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! 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

BLACKSTONE LAW GROUP LLP. Unique among law firms, we have married the practice of law with the practice of information security. We are also the only law firm to offer bespoke threat intelligence. Designed to identify the hallmarks of impending cyberattacks (APT activity, phishing, credentials harvesting, etc.), with our own DNS monitoring and threat intel platform, OMNI, we have assisted hundreds of companies worldwide with the early detection, investigation, and termination of sophisticated cybersecurity threats before a breach or reputation damage occurs. Engineered for and by information security professionals, our DNS intel platform goes far beyond ordinary brand protection, safeguarding our clients full circle: from detection to takedown. Our lawyers have been the Chief Information Security Officer and Chief Compliance Officer of some of the world's most recognizable companies, have federal government experience in both intelligence and defense, and been partners in several Am Law 100 firms. At Blackstone Law Group, there is no lag time to "get the lawyers up to speed" on the technical issues surrounding an incident or investigation. Our combination of legal acumen and information security expertise results in great efficiencies that, by design, benefit our clients' bottom line. And perhaps most notably, one of our partners is Alex Urbelis who many readers will recognize from *Off The Hook*. Give us a ring or send Alex a note. We would be glad to speak to you confidentially about our threat intel and legal services. Blackstone Law Group LLP, alex@blackstone-law.com, 1201 Broadway, 9th Floor, New York, NY 10001, P: (212) 779 3070 x 101, https://blackstone-law.com.

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.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMES? Stand up for your rights! Be calm, cool, and collected: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember basic game theory and the Prisoner's Dilemma: nobody talks, everybody walks. Consult with a lawyer experienced in defending human beings facing computer-related charges in California and federal courts. Omar Figueroa is an aggressive Constitutional and freedom defense lawyer with experience representing persons accused of unauthorized access, misappropriation of trade secrets, and other cybercrimes. He is a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and is willing to contribute pro bono representation for whistleblowers and peaceful hacktivists. Past clients include Kevin Mitnick (million dollar bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure) and Vincent Kershaw, reported member of Anonymous indicted for his alleged participation in a DDOS action against Paypal. Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note I also specialize in cannabis legal compliance and can help you navigate a complex maze of marijuana-related laws and regulations. Please contact Omar Figueroa, at (415) 489-0420 or (707) 829-0215, at omar@alumni.stanford.edu, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

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/

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 18 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.

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).

ANTIQUE 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

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing 2600 promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

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!

Personals

LONGTIME HACKER "ALPHABITS" previously arrested in Operation Cybersnare doing time for another high tech escapade. Looking to hear from people in the free world. Jeremy Cushing #19763473, East Mesa Reentry Facility, 446 Alta Road, Suite #5200, San Diego, CA 92158-0002.

JUST TRYING TO STAY CURRENT WHILE INCARCERATED. Can you help by forwarding knowledge to a fellow tech enthusiast? I'm hoping to find an intelligent, curious few people with a hacker mentality, money making mind, and great sense of humor. I'm not looking for love! I'm married to the greatest woman in the world plus an old timer told me "if a woman is looking for a man in prison, there's something wrong with her." Some of my esteemed colleagues here are looking for love, so if you want me to play match maker, knock yourself out. Please write if you have any current hacking tech or science info. I can offer you humor, warped, semi-informed opinions, and of course plenty of prison and criminal war stories. My interests are far and wide so I look forward to hearing from you. I can be emailed using the jpay.com app. My DIN is 18A3614 or regular mail at: John Black 18A3614, Washington Correctional Facility, 72 Lock 11 Lane, PO Box 180, Comstock, NY 12821.

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 Summer issue: 5/21/20.

HOPE 2020

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

Featuring

- 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.

Get Involved

- Submit a talk or panel idea to speakers@hope.net
- Put together a workshop at workshops@hope.net
- Volunteer to help with the conference at volunteers@hope.net

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

"*This is the time. And this is the record of the time.*" - Laurie Anderson

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

S T A F F

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Kashtin, Iggy Pop, Negativland, Worlds of IF, Stormzy

Shout Outs: Tshiuetin Rail, Schefferville, CIBL, Wet'suwet'en, LCM+L, Henry Anderton

***2600* is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176) 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.
2000-2019 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**

MEETINGS

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 Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

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

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), 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

PORTUGAL

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

RUSSIA

Moscow: RNDM, Nastavnicheskiy 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: Krystal Hamburgers, 2914 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.

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. 6 pm
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

New Orleans: Z'otz Coffee House uptown, 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door. 6 pm

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston (Cambridge): Starbucks, 2nd floor, Harvard Square, 1380 Massachusetts Ave. 7 pm
Waltham: The Telephone Museum, 289 Moody St.

Michigan

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

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 Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm
Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm
Philadelphia: 30th St Station, food court outside Taco Bell. 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!

Phones as Art

England. This is actually a Thai payphone that somehow wound up in a bar in Oxford as some sort of an art display. Don't bet on getting a dial tone.

Photo by Toronto Phreak

United States. Spotted in Gorman, California (and you can spot it too if you look long enough), this is an example of the camouflage effect of graffiti. Most

Photo by German Rodriguez

Malaysia. This work of art was discovered on the island of Langkawi in the Cenang Beach area. If only every abandoned kiosk could look this nice. No dial tone, no receiver, and not even a phone here.

Photo by Sam Pursglove

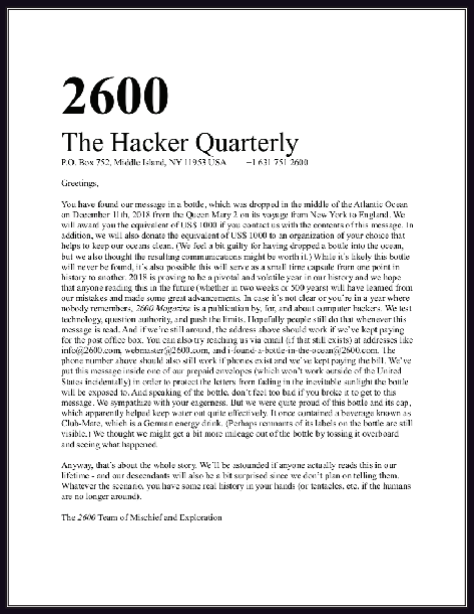
Japan. What makes this particularly artistic is the fact that this is still an actual functioning payphone, complete with rotary dial. Found in Hachioji. And just look at the great condition it's in!

Photo by Larry Washburn

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

2600 and the Club-Mate Bottle
A Transatlantic Saga

This is the bottle before it was dropped in the middle of the Atlantic Ocean on December 11, 2018.



2600

The Hacker Quarterly

P.O. Box 752, Middle Island, NY 11953 USA +1 631 751 2600

Greetings,

You have found our message in a bottle, which was dropped in the middle of the Atlantic Ocean on December 11th, 2018 from the Queen Mary 2 on its voyage from New York to England. We will award you the equivalent of US$ 1000 if you contact us with the contents of this message. In addition, we will also donate the equivalent of US$ 1000 to an organization of your choice that helps to keep our oceans clean. (We feel a bit guilty for having dropped a bottle into the ocean, but we also thought the resulting communications might be worth it.) While it's likely this bottle will never be found, it's also possible this will serve as a small time capsule from one point in history to another. 2018 is proving to be a pivotal and volatile year in our history and we hope that anyone reading this in the future (whether in two weeks or 500 years) will have learned from our mistakes and made some great advancements. In case it's not clear or you're in a year where nobody remembers, 2600 Magazine is a publication by, for, and about computer hackers. We test technology, question authority, and push the limits. Hopefully people still do that whenever this message is read. And if we're still around, the address above should work if we've kept paying for the post office box. You can also try reaching us via email (if that still exists) at addresses like info@2600.com, webmaster@2600.com, and i-found-a-bottle-in-the-ocean@2600.com. The phone number above should also still work if phones exist and we've kept paying the bill. We've put this message inside one of our prepaid envelopes (which won't work outside of the United States incidentally) in order to protect the letters from fading in the inevitable sunlight the bottle will be exposed to. And speaking of the bottle, don't feel too bad if you broke it to get to this message. We sympathize with your experiment. But we were quite proud of this bottle and its cap, which apparently helped keep water out quite effectively. It once contained a beverage known as Club-Mate, which is a German energy drink. (Perhaps remnants of its labels on the bottle are still visible.) We thought we might get a bit more mileage out of the bottle by tossing it overboard and seeing what happened.

Anyway, that's about the whole story. We'll be astounded if anyone actually reads this in our lifetime - and our descendants we'll also be a bit surprised since we don't plan on telling them. Whatever the scenario, you have some real history at your hands (or tentacles, etc. if the humans are no longer around).

The 2600 Team of Mischief and Exploration

This is the note that was stuffed inside.

Here is where the bottle was found on February 2, 2020 in the Bay of Littlelure, Shetland by **Henry Anderton**. The label had washed off but the glass bottle was otherwise unscathed and the contents completely dry.

In an unbelievable stroke of synchronicity, Henry is allocating his reward money to the restoration of this local phone booth left behind by British Telecom. An additional donation is being made by us to The Ocean Cleanup organization in Henry's name.

We will resume our regular back cover feature next issue.

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.