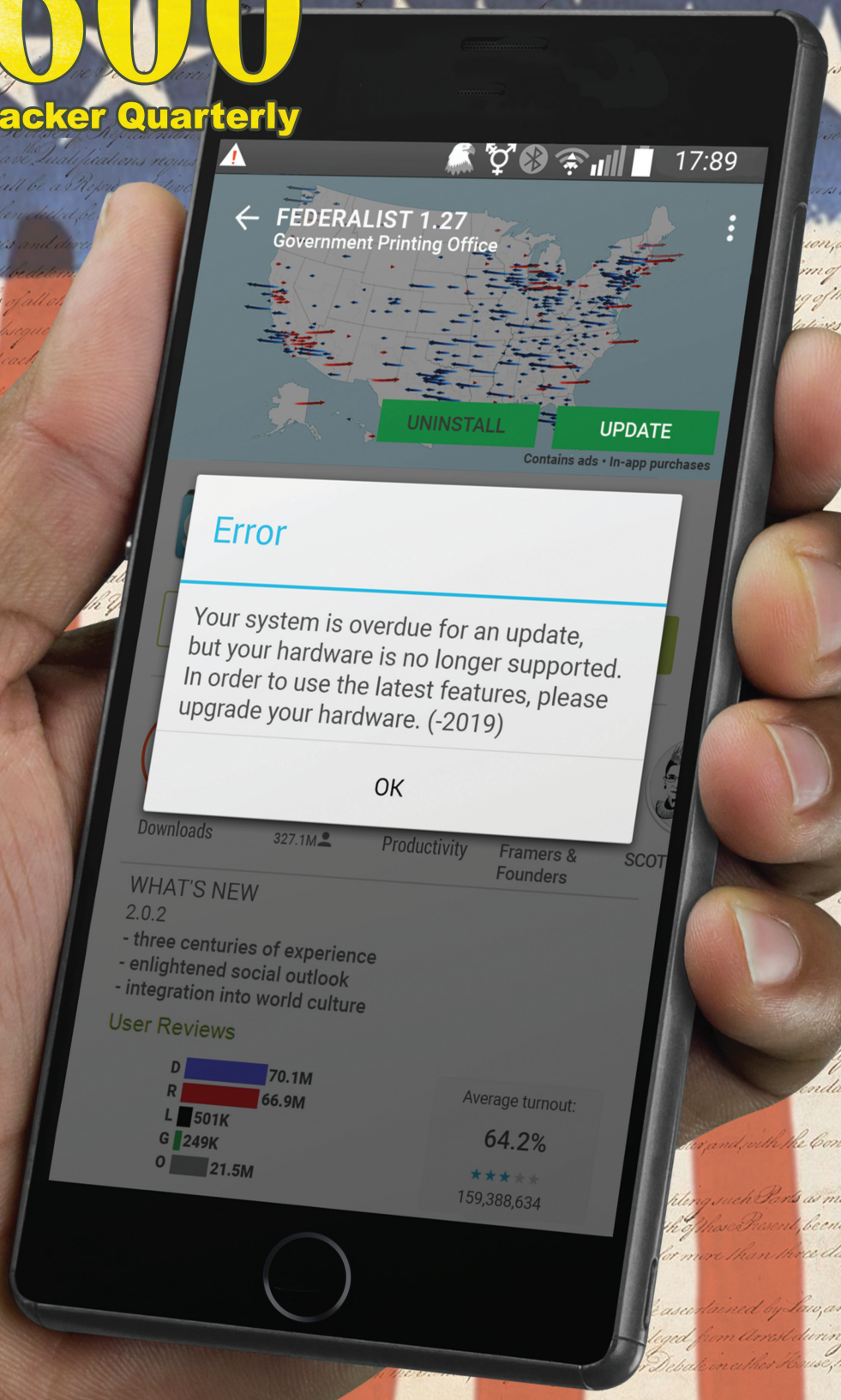
Volume Thirty-Five Number Four
DIGITAL EDITION Winter 2018-2019

2600

The Hacker Quarterly



FOREVER

Payphones with Coins

Russia. Found at the Museum of Soviet Arcade Machines in St. Petersburg. This isn't truly a working phone, as it's wired to call another phone in the museum and that's pretty much it. But it'll still take your coin if that's what you want.

Photo by Christina Dill

Peru. This neat little model was simply hung on the wall outside a shop in Cusco. Someone apparently spent a lot of time trying to get rid of the instructions.

Photo by Matthew Searle

Singapore. We don't know exactly what a "multicoin phone" is, but here's one that was discovered in Tampines. And don't even ask about the Ikea pencils.

Photo by David M.

Ukraine. Spotted in Odessa, we suspect this might also be part of a museum collection. In a sense, we may be looking at the future.

Photo by Jason Lenny

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 (Do not send us links as photos must be previously unpublished.)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

40.749080,
-73.956008

specifics

Taking Back Ownership	4
1979 Plus 40 Years	6
AV1: One Giant Leap for Video-Kind	8
YITM	9
Social Engineering from Prison	10
A Brief Tunneling Tutorial	12
TELECOM INFORMER	13
Quantum Computers and Privacy	15
Hacking the School System	22
A Reading of the AI Hype Meter	24
HACKER PERSPECTIVE	26
Thumbcache.db Primer	29
Sorting It All Out: The Long Lost Bastard Children of the United States Postal Service	31
Configuration Negligence: Who is Responsible?	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
Facts About Honesty/Integrity Tests and Interviews	47
Book Review: Surveillance Valley: The Secret Military History of the Internet	50
Book Review: Ten Arguments for Deleting Your Social Media Accounts Right Now	50
Modem and Me: The Loose Ends	51
CITIZEN ENGINEER	52
A Fork() in the Road	54
Making an Informed Business Decision Using Public Financial Records	55
To the Unknown Hacker	57
Hacking in a Slow Job Market	58
Fiction: Hacking the Naked Princess 0x16	59
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Taking Back Ownership

There is a disturbing trend many of us have noticed in recent years, one that seems to affect an increasingly significant part of our lives. Little by little, we're losing control over much that we once took for granted.

The concept of ownership is still not an alien one. But it seems to be in danger. In the past, if we bought a book or a record, that was considered an item that we indisputably owned. We were free to do with it whatever we wished, bring it anywhere we wanted, and say with confidence that we, in fact, *owned* that tangible object.

Those days are threatened on a number of fronts. Books give us a great example. A digital copy may be more convenient and allow us to carry more works around with greater ease. But it can also be taken away at a moment's notice when someone in control decides that we should no longer have access, whether it's because we didn't pay a fee or we simply moved to a different part of the world. Or something entirely unrelated to us could change the circumstances. There was a dramatic instance of this back in 2009 when - of all authors - George Orwell had his works quietly deleted from Amazon Kindles due to a rights issue. Overnight, copies of *1984* literally disappeared as if they had never been there. Naturally, the cost of the books was refunded to the customers, but that's not the point. This kind of an action would have been inconceivable with a "real" book, regardless of copyright issues that are of no interest to the consumer.

We see similar scenarios regarding music and video. Increasingly, we opt for digital over analog and cloud over local collections. While there are significant advantages, specifically content availability and ease of access, none of this comes without relinquishing significant degrees of control. Recordings can be removed if terms change as outlined above, our entire collection can disappear if the hosting company goes out of business, and our viewing/listening habits can be analyzed and shared by third parties and even law enforcement. Maintaining an account that isn't tied to an actual identity is a concept that's beyond the imagination of most people, meaning the days of anonymously viewing and listening have ended for many. Sadly, they may never even know why that was important.

It's also becoming increasingly difficult to buy major pieces of software for local installation on our own machine(s). Instead, subscriptions to cloud versions are pushed and, in more and more cases, are the only option left. Again, there are advantages: the latest version, customer support, lower initial cost. But, once more, control is sacrificed. We lose the ability to experiment with the software, we're dependent on connectivity and the availability of the remote host, it becomes more difficult to compare with competing software, and there's no way out of continually paying for something. Remember: we don't actually own the software - we're simply leasing a license, a license that goes away once we stop paying. And, of course, the privacy issues persist.

The trend continues into the world of hardware - from computers to cars and well beyond. The latest trend in operating systems is to exist in the cloud, leaving our local machine a lot closer to a dumb terminal than to a sophisticated computer. But it's clearly more convenient (and cheaper) since there's no longer any need to worry about maintenance and updates. And if you've bought a car in recent years, then you know that it's become next to impossible for just "any" mechanic to service it. We need licenses, codes, and access in order to get the proper permissions to maintain newer vehicles, something our local car dealership is happy to be the exclusive supplier of. The convenience aspect here is a bit more subtle, as this form of technology has more of a history of independence and do-it-yourself repairs. But for quite a few people, not having the "hassle" of choice is actually an advantage. Not for everyone, though. And the issue of control couldn't be clearer.

With every example cited, we find ourselves on a tighter leash and, whether this bill of goods is sold with the promise of convenience or the threat of danger and all sorts of problems if we resist, we have less and less control. We no longer actually *own* our technology; we are but an end user. If we want to remain on the system, we have to follow the rules.

This is not the kind of environment that hackers enjoy. Convenience and control are for consumers who don't see the magic and beauty in the technology they use. They have no desire to take it all apart and see how it works. They just want a tool. And this is fine for their purposes. Ours are different and always will be. Knowing how things actually function is how we learn to make them function even better. It's how we find the flaws and occasional privacy violations hidden within. And, of course, breaking things is the first step in learning how to fix them. Without all this, we simply wind up blindly accepting updates and upgrades, losing features, accepting others without question, and allowing ourselves to be shaped by technology, rather than the other way around.

There's clearly a huge difference between the insides of an old rotary phone and a smartphone. But that doesn't mean we can't still learn how each of them works. The first is pretty straightforward while the second is far more complex and intricate. All that means is that we need more sophisticated methods of experimenting, not discouragement from playing around with something we've bought.

We obviously can't go around disassembling intricate and tiny pieces of technology in the same manner that we can with something built by human hands. But we also don't have to relegate ourselves to user status. Taking apart a watch is different than taking apart a clock. But there are still concepts and parallels we can apply to each. That doesn't have to disappear as our technology becomes more complex. We simply need to adjust *how* we learn.

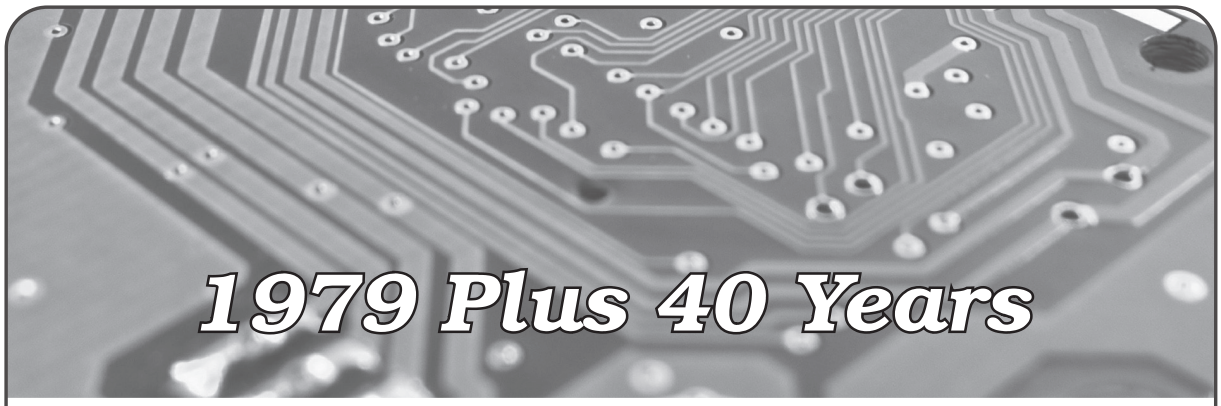
This is a gap that must be bridged or we risk some very unpleasant scenarios. We can reject the newer technology and only use that which we have full control over, losing out on all of the advancements and advantages coming out every day. Or we can fully embrace all that is new and be spoon-fed for the rest of our lives without any real understanding of how any of it is even possible. Clearly, we need something in the middle. It's foolish to discard old technology; even if there's no practical use for it, there is still the very real possibility that its functionality can teach newcomers about theory in ways that more advanced applications simply can't. It's equally nonsensical to reject new technology outright since everyone deserves to benefit from the advancements made possible through our continuing evolution.

By putting forth the idea that none of this actually belongs to us and that we're all just licensed to use the technology from month to month, we not only lose the ownership and control we've always valued, we lose our rightful place in the development and growth of technology. If we can't open it up and see how it ticks, it becomes nothing more than a magical product that somehow works. We never get to ask: How? We never get the joy of seeing it come together. It just is. And that may be enough for many. For us, we're always going to want a bit more.

In our rush to take advantage of modern bells and whistles, we often forget to add in our own values, the effects of which may not be readily apparent. For example, we increasingly see that it's not so easy to give digital items we "own" as gifts or to bequeath them for future generations to enjoy. We've all been to garage sales or secondhand stores where we peruse old record and book collections. That just doesn't work with a Kindle or a collection of MP3s, at least not in the same way. The digital files are a convenience, but the loss of a physical object is quite tangible.

As mentioned already, privacy issues are a big concern, something we don't think about nearly enough. Having systems in place where there's an ongoing log of what book or article we've read, what movie we've watched, the exact software we've used, or where and when we've gone on a drive should be a *huge* red flag, regardless of whether or not we think we have anything to hide. We never would have accepted that level of surveillance in the analog world and we shouldn't accept it now. And it's most certainly *not* necessary in order to have the things we want. It's just something thrown in by the designers - and those who want more control.

We are at a true crossroads in so many ways. We want to embrace all of the new developments and help to apply creativity and imagination to them. To do that, we cannot be restricted or told we're simply users and that we're not permitted to access, experiment, and take things apart - even when the very definitions of those concepts have changed. Because what *hasn't* changed is our desire to keep learning.



1979 Plus 40 Years

by Diana

A friend and I were talking about the year 1979. My friend observed that we were paid less than what others are paid now. However, we had more money and ability to participate and do activities. Thinking of this idea, I decided to think about what it is like for someone to buy a computer now without credit cards. As in 1979, most people had department store credit cards with about a $500 limit and would ask to have their limit increased to $1,000. This is how my dad was able to buy my first home computer: a TI-99/4.

Even at that time, the concept of working in the computer revolution meant a better society in the future; it did not mean the concept of an information worker who is like someone working in fast food, having to work long hours for low pay, hoping to get food stamps, and trying to keep their head above water without being evicted or becoming homeless due to emergency expenses.

This future of 40 years since 1979 is not the future many of us envisioned. There is something wrong; even in my undergraduate years, all of us graduated without student debt and were able to drive, go to movies more than once a week, and most importantly, have fun. It was not a cycle of study, work, and sleep.

What I and Others Expected

We expected that the future would allow all to enjoy benefits of being able to create, explore, recreate, and try something new. The ability to create like we did in 1979, try half-baked ideas without the permanent social media record keeping, and the ability to fail privately. There is a benefit to being able to fail privately because when one feels they are always under surveillance, it does create a group think or herd mentality. An ability to explore privately as when one goes outdoors or develops without an Internet link. Exploring privately means that the exploration is not a race, it is a drive and positive benefit like exercise. To play rather than using the term recreate, an informal rather than clinical term.

Play is something that was done a lot in 1979. It meant we would meet and decide what we wanted to do, whether we wanted to show each other what we did with our TIs, Ataris, Commodores, Ohio Scientifics, and others. Also, it meant that coding was not our whole life. We would have activities other than coding. We could afford to have many activities rather trying very hard to keep one activity or hobby.

As we witness the development of the low-wage economy, even in the computer field, it becomes apparent that we need to stop this trend. No one in 1979 would have thought like someone knowing how to program a computer, or use what would become the Internet, or develop a web page as a commodity worker, someone who would work the hardest for the lowest pay and least stable work environment. What was thought in 1979 was the dream of Adam Osborne, David H. Ahl, Steve Jobs, Steve Wozniak... a vision where your idea would help lift the quality of life higher for others and for yourself.

At one time, the Silicon Valley actually included those who designed, built, and marketed new ideas and computers, very different from an area where the livability index is way high and prototype and building is done by IT production workers in other countries who have mental health issues while making a computer or table that cost $2.50 in production and is sold in the U.S. or other countries for $2,500.

The original spirit of the computer revolution that existed in 1979 still exists in open source, other forums, and in universities that allow for students to explore half-baked

ideas, and fail privately without a permanent log on social media or server farms. It is also comprised of those who still speak of social issues like older magazines such as *Creative Computing* and *Byte* used to do, along with code.

Computer science was very different when I started in my undergraduate year. It meant strictly business computing, no AI, no half-baked ideas, no real-time running of code. Computer science then, which included parts of computer engineering, meant learning how to make your CPU from chips. For us, it meant making a four-bit CPU using MSI and VLSI chips like 7400 and 74138, along with a clock chip.

Even at my old university, I don't see much of the actual hardware balance along with software like when I started in 1982, majoring in pre-med and applied computer science with a breadth of knowledge in art and history. In a way, it was a joy to see the old computer display in the building where computer and engineering sciences were together. Yet, it's a bittersweet memory, and I wonder if the current students would know what I was talking about when I say one project was to built a four-bit CPU from 74xx and 74xxx series chips. Would the student be able to complete the same project today? I hope they could.

In the world of the information worker, when they lose the coveted position at a major firm, they become the worker who is faceless in the commodity work of the information worker - no matter where they work. However, the perks of having two cars, their own house, and being able to really play on the weekend disappear after they reach age 35 or 40. Remember the $65,000 student debt for an undergraduate computer science degree. So, from age 23 to 35, a life of expenses must be paid in 14 years whereas my generation had at least until age 50; we would move into another field without becoming a commodity worker, a field where one is a valued individual, compensated fully without having to ask the state for food stamps, health insurance, or help with rent.

Whatever happened to the boycott, like the #metoo movement and glass ceiling? The boycott does not work. One should not have to study harder than a medical doctor and be treated as a commodity worker. Even when I started to change careers, my parents said they would support me for obtaining an advanced degree, but not in science or technology because they felt the main aspect of how graduates were treated was as a commodity of who would work for the lowest compensation, longest time, and be the ball. This was in 1998 before the aspects of corporate welfare were fully known.

So, I went for an MBA as well as a doctoral degree in management and organizational behavior to start my own company and to continue the ideas of the computer revolution. One thing I did not do is seek venture capital because it is a sword and a delicate dance. Rather than public, set up a company as private. I see the idea of an initial coin offering (ICO) preferable to an IPO and hope that it will spur the benefits where all live fully and corporate welfare ends.

With regards to the idea of making a four-bit processor, even the concept of a simulation is not taught in computer science. The theory is, but I prefer code to learn. An example of the main engine is:

```
1.      Repeat
2.      Data = getMem(PC);
3.      Opcode = data and $0f;
4.      Case (opcode) of
5.      Pushv: doPushv(PC, data);
6.      Push: doPush(PC,data);
7.      Pop: doPop(PC, data);
8.      Call: doCall(PC, data);
9.      Cmp: doCompare(PC,Data);
10.     JMP: doJump(PC, Data);
11.     JNE: doJumpNE(PC,Data);
12.     JEQ: doJumpEQ(PC,Data);
13.     JLT: doJLT(PC,Data);
14.     JGT: doJumpGT(PC, Data);
15.     Skip: doSkip(PC, Data);
16.     Ret: doReturn(PC, data);
17.     End case;
18.     Until (opCocde = haltIns)
          or (pgmStop);
```

What is shown is a basic CPU simulator that supports the concepts of a program as sequence, control, and interaction.

We need to think about the future the way we did in 1979, not in what has become 1879 to many IT workers worldwide. This is the 21st century. We have to stop backsliding and once again start pushing the future in a positive way for all, so no underclass or people are treated as a commodity. All should be treated with full dignity and a full quality of life. That full quality of life is not a perk. It is a right.

AV1:
One Giant Leap for Video-Kind

by Ethan

Codecs aren't exactly the most exciting thing. But a new one, AV1, might actually change the way we watch videos, despite its relative obscurity, because it improves on its predecessors in pretty much every way.

The project itself is developed by the Alliance for Open Media (aka AOMedia), a nonprofit with a Who's Who in the tech community: the biggies like Google, Microsoft, Facebook, Amazon, Alibaba, Mozilla and Apple; chip manufacturers like Arm, AMD, Intel and Nvidia; and streaming providers like Netflix, Hulu, Vimeo, and the BBC, among others. This means that, for possibly the first time ever, there could actually be a standard supported by pretty much every major tech company from the very get-go.

The format is open source, and licensed under the BSD 2-clause license, alongside an explicit patent grant based on reciprocal license (basically, as long as you don't sue someone with your own patent over their use of AV1, you can use AV1 without worrying about being sued). Plus, since a big part of the format's development was patent review, it won't face problems like the rocky rollout of H.264, which, while now the most common video format on the Internet, was initially blocked from browsers like Firefox because of patent licensing issues. The situation is even worse for H.265, which five years in still isn't widely supported by any tech company but Apple, in large part because it has three separate patent licensors. (Side note: one of them asked for a percentage of streaming revenues, which was unanimously rebuffed. As one CTO put it, "no mainstream company is ever going to do that," which probably influenced the format's non-use.)

AV1 is even more efficient than the last available free codec, VP9, by at least 30 percent. When combined with the open audio format Opus, which is also the most efficient audio codec available, you can watch videos at the same quality while using 50 percent less data than H.264, according to Facebook's testing. The implications of this development are pretty wide reaching: with so much more efficient delivery, 4K and 8K content streaming may actually be within reach for those with slower Internet; high-quality streaming will be possible over low-speed cellular networks; and, even for those with good Internet, everything will look better.

The only problem: the format is so complex, it takes significantly longer to encode than any other format. As in, depending on the video, hundreds or thousands of times as long. But since the big tech companies don't have a lack of server power, and services like Netflix deliver so much content, it won't be an issue for them. And besides, over time the encoder will improve in efficiency, meaning you could see AV1 become a standard for consumer use too.

You might be asking "when will I actually see this in use?" The answer: pretty soon. Since the final, validated specification of the format was only released in June 2018, there's still work to be done. Yet, Google already supports AV1 in Chrome's newest versions, Mozilla promised Firefox support (beyond the Nightly version) in late 2018, and Netflix and YouTube already have test videos available, with at least Netflix intending to roll out full support imminently. So keep your eyes open. Though there's still some work to be done, there's a good chance that massive improvements are on their way.

Further Reading

- See Facebook's testing at `code.fb.➥com/video-engineering/av1-➥beats-x264-and-libvpx-vp9-➥in-practical-use-case/`
- Bitmovin, a large video services company, also tested the format; its results and dataset are here: `bitmovin.com/av1➥-multi-codec-dash-dataset/`
- Check AOMedia's site for more info, like the bitstream spec, at `aomedia.org`

by Edster from Dublin Ireland

Please note - information in this article is for educational use only blah blah blah, please don't do anything illegal, immoral, or even impossible. Don't stalk anyone.

The name of my article is "YITM" or "You're In The Middle." This is similar to "Man In The Middle," where someone else intercepts your network packets going back and forth between you and the server you are accessing to fetch a website or pick up your emails or data, but this time you are the person intercepting your own data.

The first obvious question would be: Why do you want to intercept your own data as you already know what you are sending or receiving? The answer is simple: you do not really know what you are sending. The data is not coming from you directly, but instead it is the data that the apps on your phone are sending on your behalf (and often without your knowledge).

The setup for this is fairly easy. You will need software to capture the packets as they fly past. I use Charles Proxy, but as it is a paid app, you can also do a quick search for "free MITM tools" and you will find other options if you want to play for free. You now change the settings on your phone's Wi-Fi connection to proxy via this bit of software. For me, it means tapping on the Wi-Fi settings on the phone and setting the proxy to manual, setting the server address to the IP address of my laptop, and the port to 8888. Now any data sent in or out of the phone's Wi-Fi connection will show up on the screen. Depending on the setup, you may wish to add a root certificate to allow you to catch the secure HTTPS (TLS) traffic. This is normally very simple and can be done in seconds by following the proxies' instructions. For example, with Charles, you send your phone to a local web address and click yes a few times to install the cert that downloads. Job done.

If this is your first time monitoring a phone, you'll be surprised at how much data flows back and forth. You may want to shut down all the apps except the one you are watching to keep the data a bit cleaner. Run your apps one at a time and see how much information they give away about you, or about the service that you are accessing.

To get some examples of the sort of information that "leaks" out, I installed two types of apps that would (or rather should) have security built in: dating apps and banking apps. Most of the apps were not too bad. Most of them didn't send too much data that I didn't have myself. Half of the bank apps used pinned certs which means I could not even intercept traffic, as it blocked me as soon as it saw this new self-signed MITM cert.

The first app that stood out as unsafe was the dating app "Happn." Clicking on a picture on the app allows you to see more

information on your future ex-wife (or ex-husband). This we already know. It even gives an approximate GPS for where you passed this person last. Some people allow this much of an information leak as the price for getting a hot date. What they do not realize is that when you watch the data fly past on your new tool, you are presented with all the data you see on the screen, and also with the Facebook ID the person signed up with. Copy that number to the end of the Facebook URL and press enter. You now have that person's full name, location, pictures, friend list, job locations.... Oh my - stalker's paradise.

The good (or bad) news is I have already told Happn about this and they have closed it down. I held off on publishing this article for almost a year for them to make the change. But that change is still not enough. The Facebook ID is still being sent - they send it as a base64 encoded string in exactly the same way. As well as base64, they have added a very small amount of encryption to it. This took me three minutes to work out.

YITM has another use. As well as learning what your favorite apps are sending back and forth, you can also mess with the data and see what it does. The software will normally allow you to specify text in the incoming or outgoing packets and change values in it.

Click on a profile and look at the data that comes with it.

Let's change:

`"is_invited":false` to `"is_invited":true`

`"is_accepted":false` to `"is_accepted":true`

`"has_charmed_me":false` to `"has_charmed_me":true`

A look through some of the other traffic will bring up other things to change. For example:

`"latitude":(.*),` to `"latitude":98.7654,`

The power of YITM is sometimes limited by the code at the other end. You'll find that altering the incoming balance on your account may look nice when it displays, but you will not be able to use the fake coins as the server knows your real balance.

Go through your apps and see what they send. You will be surprised. Play with some values and see what you can make them do. Note: you may want to sign out of your real accounts and sign into some new fictitious accounts, so if they ban you for messing with the data stream, you do not lose access to your own data. Please do not steal or stalk with this newfound skill. If you do find a big data leak, tell the company so they can close it. They may even give you a bug bounty.

by CyberGenesis

So... social engineering. Yes? No? Maybe? Although hackers are largely anonymous and seem to have very large problems with authority (as well they should), most seem to at least be on the same side. I won't go into government snitches here. I just can't understand or even remotely fathom why one hacker would turn one of their own into the government to be prosecuted. But that's another article in and of itself. Back on topic!

Hacking, back in the day, used to mean someone who could throw a program

together out of nothing in no time flat. How? Hacking means terrorism, "punk kids" (I'm 43 now), and criminal acts. But hackers are *needed*. They're our front line fighters. There's another group, however, that gains their information through more stealthy means, then hands it to the hackers so they can do their thing. It's this "shadow group" that people should *really* be afraid of. That's right. I'm talking about social engineers. I am a part of this ever-growing population.

Social engineering, as with hacking, is an art form and one that only a few people are called to, and even fewer truly get good at. Imagine meeting someone for the first time and within 30 minutes, they're giving you their life history.

Case in point. I'm incarcerated at FCI Beaumont, a low-security facility. I was taking their CBL course here and I got very bored, very quickly. A friend, knowing I'm a social engineer, challenged me. "I bet you can't get any personal information out of our instructor." I asked him how long I had and he said 14 days. (Like taking candy from a baby!)

Anyway, I noticed the instructor had a touch-screen watch that was flashing a warning that it couldn't connect to his cell phone because it was out of range. This was my "in." I asked what type of watch he had and who he used as a provider. He readily gave up that he had AT&T. Within a mere 48 hours, he was telling me he was married, how many kids he had, where everyone worked, what types of cars they all had, and what cities they all lived in. Bonus round - I even got that his wife was undergoing treatment for cancer.

Now, if I was unethical in any way, I could have passed this information on. But this time I let it go. I just couldn't pass up the challenge. My friend couldn't believe I'd gotten all that info from a paid prison instructor from the local university.

Knowing how people think and respond in given conversations gives the social engineer "control" over people. Here are three rules to remember when social engineering people for your cause:

1. *Be friendly!* A smile makes people *want* to trust you.

2. People *want* to talk about their families. It's a source of great pride for them. And as they talk, they're inadvertently giving you their username and password combinations. A proud parent will most often have their child's name as their password.

3. People with high octane jobs are more likely to have nice families and large bank accounts. If someone works at McDonald's, it's time to move on. If they say they're a bioengineer such as this instructor's 20-something daughter, it's worth your time and effort.

Being a social engineer also means being able to think quickly and being a chameleon. If your surroundings require you to be a paramedic to get someone to trust you, time for you to brush up on your anatomy and physiology. You're talking to a CTO and you want some info from them? Brush up on the latest technology. You have to literally become what it is you want. You've never done what you need to become? That's fine! Know enough to make yourself believable. People generally are not going to ask a lot of questions, though they will ask one or two to establish a baseline.

Now after saying all this, I have two more things to say. Then it's off to dreamland for me.

Personally, I've social engineered my way into a key card for a Silicon Valley company by convincing the secretary I was a new hire (I did my homework so I'd know names of current employees). I've SE'd my way into two marriages that financially benefited me, and I've also gotten into a secure county emergency management office using credentials that took me ten minutes to create.

In my opinion, social engineering is the wave of the future, but *please,* know one thing:

As stated in a previous issue of *2600,* if you call yourself a hacker or a social engineer, you're joining an elite war and consenting to being labeled a terrorist by your country's government. If you want to be an agent of change, then I invite you to join this war against our persons.

Thanks for reading!

They're trashing our rights! Hack the planet!

A Brief Tunneling Tutorial

by s0ke

Recently I came across an issue where I wanted to be able to SSH into a box behind a pesky corporate firewall. Not having access to said firewall. I decided to take matters into my own hands and set up a reverse SSH tunnel from that box to a box out on the Interweb that I can access.

Installation

The device that will be accessed behind the corporate firewall is a Raspberry Pi B+ installed with the vanilla version of Raspbian. Out of the box, this is already set up for DHCP. The following commands are all run on the Pi.

First, I will install autossh, which is a program that will automatically detect SSH connection drops and reconnect them - essentially keeping my tunnel alive and up.

```
apt-get install autossh
```

I then generate an ssh key for my Pi to be able to SSH into "myremotebox".

```
ssh-keygen
```

I copy the key from my Pi to "myremotebox".

```
ssh-copy-id user@myremotebox
```

Bash/RC

Here is a simple bash script that creates the tunnel using autossh.

```
$ cat tun.sh
#!/bin/bash
sleep 30
/usr/bin/autossh -M 9090 -R 9091:localhost:22 user@myremotebox
```

-M = Monitoring port to use.

-R 9091:localhost:22 = Reverse tunnel. Forward all traffic on port 9091 to "myremotebox" on port 22.

I then add the following line to my /etc/rc.local file. I want this to run as my Pi user. I also add a sleep timer to ensure that networking is available before this script attempts to execute.

```
/bin/su - pi bash -c '/home/pi/tun.sh'
```

Tunnel UP

Now that everything is in place. I covertly place my Pi inside the corporate office and leave for the day. I then access my public Linux machine later that night and connect to the reverse tunnel.

```
s0ke@pine64:~$ ssh -p 9091 pi@localhost
pi@localhost's password:
Linux raspberrypi 4.14.50+ #1122 Tue Jun 19 12:21:21 BST 2018 armv6l
The programs included with the Debian GNU/Linux system are free
➥ software; the exact distribution terms for each program are
➥ described in the individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Sep 26 18:21:26 2018 from ::1
```

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I just finished a busy weekend with a lot of terrible driving. Snow came early this year to the Pacific Northwest. This time of year, when Mother Nature unloads, access can be cut off except through the Columbia Gorge when Snoqualmie and Stevens Passes are snowed in. Naturally, on the day I needed to travel, both passes were... *impassable*. I had to drive the long way around, starting at six in the morning. South to Oregon, east through windy Hood River, and finally north again into Washington State to one of the most remote pieces of tribal land in the country. It was the weekend, I was working, and I needed more coffee. But what I did today was important enough to volunteer to do it. That's right: today, I'm not getting paid!

East of the mountains, the terrain is high desert. It's the Old West here, with sagebrush, tumbleweeds, and bitter winter cold. The distances are vast and the population is sparse. This is the kind of place that my employer never wanted any part of. Once GTE country, it was briefly acquired by an East Coast ILEC. In a series of transactions, the territory was then sold cheaply, multiple times in rapid succession, like an ugly sweater that nobody wanted. From a telecommunications perspective, it's the bottom of the barrel, serviced by a bottom feeding carrier that specializes in rural telecommunications. And by "specializes," I mean "provides the bare minimum service to continue receiving federal subsidies." Practically nothing has been upgraded or maintained since GTE serviced the area, and GTE was notorious for poor service. Broadband, for the most part, isn't available outside of town. And what the local provider calls "broadband" is 4Mbps ADSL. When you call, you're talking to someone overseas who can't do anything but read you a script and tries to sell you things until you hang up in frustration.

On tribal land, the picture is even more bleak. Residential broadband? Forget it! There are entire communities with no access to broadband at all, apart from schools and libraries. The Universal Service Fund has an "e-rate" which provides a federal subsidy for these institutions to obtain broadband connectivity. It's real broadband, it's fast, and it's usually not supplied by the area ILEC. The problem is, it's only available at schools and libraries. Public safety agencies don't have access, City Hall doesn't have access, and homes don't have access. Kids who need Internet access to do their homework and compete in a modern digital economy often must travel vast distances - sometimes 20 miles or more - to gain access to the Internet when they're away from school.

"Why don't they use wireless Internet?" you might think. Good question. After all, the FCC reserved 4G spectrum in the 2.5GHz range for school districts. Unfortunately, most school districts, not realizing the value of what they had, turned around and leased the spectrum to a major national wireless carrier. Now leased, the national carrier doesn't allow schools to use the spectrum, even if no local service is provided. And naturally, mobile phone carriers don't actually provide service out here. The PCS and 4G spectrum licenses under which mobile phone carriers operate 3G and LTE data services do require license holders to provide service, but they're only required to provide service in the most populated areas. There is no geographic coverage requirement (unlike the old cellular licenses, which operated on a "use it or lose it" principle).

Fortunately, the tribe we're working with retained their 4G spectrum, so I get to build a cell tower! We'll be building them a 4G LTE network, which will provide fixed wireless Internet access to a total of 30 homes on the reservation. Using ordinary wireless routers, the connections can be shared with neighbors, so we expect that in practice over 50 homes will be covered. I'll be meeting another telecommunications engineer, the local fire chief, some folks from the tribal IT department, a carpenter, and a whole high school IT networking class.

This is a community that is highly motivated to bridge the digital divide, and they're excited to step up.

If I were working with a typical wireless carrier in a typical area, there would be endless fussing about the equipment to be used, where we'd be deploying it, and the geography it would cover. There would be endless site surveys and permit applications, and the build-out would take a few months from beginning to end. My friends at MuralNet were first contacted by this community three weeks ago. They agreed to help, contacted me through a friend of a friend, and today, we're on the way to do the build. First, MuralNet ordered all of the parts and had them delivered to me. This definitely isn't the carrier-grade stuff I deploy at the Central Office: it's made by companies like Jetway Computer, BaiCells, and KP Performance Antennas. The entirety of what we're using costs about $10,000 because MuralNet got a Black Friday special on some of the equipment. Some items were purchased on eBay, some through a Chinese website called Alibaba.com, and a lot of it from Amazon. Most of the three-week interval was spent waiting for sketchy-looking boxes to show up from China. The only pieces of equipment that arrived from a respectable, traditional telecom vendor were the lightning and surge protectors, which came from Graybar. Once the base station, SIM cards, and customer premises equipment arrived, I pre-provisioned the SIM cards and base stations to save time on site.

Permits weren't required: a highly motivated community has a way of making red tape disappear. Site surveys weren't required either, because there was really only one choice of site. We're building the tower on the roof of the middle/high school, because the school is situated on top of a hill overlooking the settlement and it has the fastest Internet connection in town. The speed clocks in at a blazing 100 Mbps. This is just fine, because the base station can't go faster than 110 Mbps anyway. A broom closet will house the Internet gateway computer; we're kicking out the broom. We were initially planning to put the gear into the existing IT network room, but decided against it because it's also used as a classroom and students often disconnect things accidentally. Instead, the high school networking class ran Cat5 cable from their existing core network switch (which isn't accessible to students without direct supervision) to the broom closet. There is a 120 volt, 15 amp circuit in the closet, but that's all that we really need. It will power a network switch, the base station (which pulls less power than a 100 watt light bulb), and a low-powered (Intel Atom) PC.

There are some tweaks we could do to the antenna positioning once it was up, but once we picked a spot, we knew we'd be committed. Fortunately, we had a ton of help! One group of high school kids scattered throughout the reservation with FRS radios and, by talking with them, we were able to find the spot on the roof with the strongest signal. With a little trial and error, we put up the antenna. The IT crew in the broom closet already had the PC racked, stacked, powered, surge protected, and networked. The school's maintenance technician drilled a hole in the roof and pulled power from the circuit in the broom closet below. We ran the rest of the cables, and in 20 minutes flat, we were on the air! Most of the next few hours were spent deploying customer premises equipment in the settlement. This was dead simple because everything had been pre-provisioned. People just needed to find the spot in their house where they had the strongest signal. All 30 CPE connections were online and working within the next three hours. And while the speeds weren't blazingly fast, they were a whole lot faster than ILEC customers up the road in town could get.

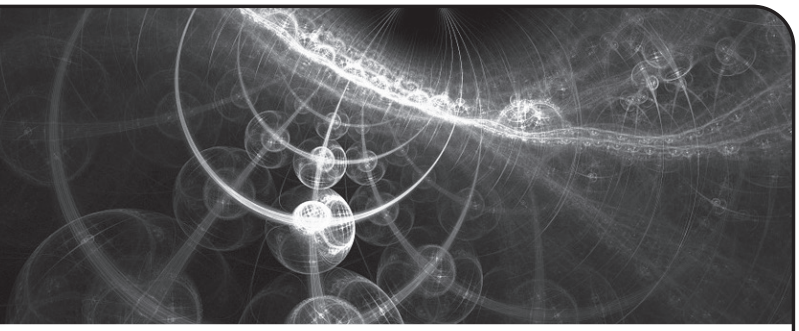
Three weeks from inception to deployment. Half a day on site to bring broadband connectivity to a community that has never had it. That's what happens when volunteers instead of phone companies build a network. But don't tell my boss, because I worked really hard today, and here in the Central Office, it's time to take a nap.

Have a wonderful winter, and I'll see you again in the spring!

References

- https://www.usac.org/sl/about/➥getting-started/default.aspx - Universal Service Schools and Libraries Fund
- https://muralnet.org/ - MuralNet, a nonprofit organization bringing connectivity to rural communities
- https://docs.google.com/spread➥sheets/d/10CfrZvAMSmMilNH4eI4N➥MzqOcyksP6IQhKus8eszLBQ/edit#➥gid=950100882 - Everything you need to build your own wireless ISP

Quantum Computers and Privacy



by Thor Mirchandani

As Dave D' Rave points out in the article "Quantum Computers and Bitcoin" in issue 34:4, practical quantum computers are just around the corner. While quantum computers may not pose an immediate threat to the hashing algorithms such as SHA256 commonly used by Bitcoin and other cryptocurrencies, the threat to Internet security and privacy as we know it today is another kettle of fish.

There seems to be a consensus among experts that most strong hashing algorithms and strong symmetric key ciphers are resilient to quantum attacks if sufficient key lengths are used, thus Bitcoin's immunity in the short term (several decades). On the other hand, most public key ciphers in widespread use today are vulnerable to quantum attacks. This class of algorithms includes those currently used in Internet privacy and trust protocols including SSL/TLS, HTTPS, digital certificates, digital signatures, and PGP.

Put differently, given a sufficiently large quantum computer, all the Internet data we assumed was private is completely transparent and the trust chains we have relied on are easily broken. Are you scared yet? Keep reading.

Post-Quantum Public Key Ciphers

All cryptography algorithms worth their salt depend on a proof of equivalence to a hard mathematical problem. Unfortunately, many computationally hard problems, including the algorithms currently in use on the Internet, look "soft" to a quantum computer.

But fortunately, not all hard mathematical problems are trivial in the eyes of a quantum computer. It appears that the solution to our post-quantum privacy concerns would involve a switch to ciphers that reduce to "quantum hard" math problems. Luckily, there are several open source projects that address this issue, and one of the more well known is Open Quantum Safe (OQS).

Getting Started with OQS

Enough of the dry stuff - let's jump right in and get wet! In other words, let's write some OQS code. The example we're going to use is a bare bones quantum safe Internet chat application. Our application consists of a client and a server. The client initiates a quantum safe key exchange with the server using a quantum safe public key cipher called Frodo, which offers a quantum security of 2^130 bits in our setup. In the exchange, the client and server agree on a unique symmetric key that they will use for the duration of the session. All subsequent messages will be encrypted and decrypted using this key and the well known symmetric key cipher AES.

First we have to download the OQS library, liboqs, from github either by cloning or downloading/extracting the zip file. The URL is:

```
https://github.com/open-quantum-safe/liboqs
```

The library has several dependencies that we need to install as well. I used Ubuntu 16.04 LTS and on that OS I would issue the following command:

```
sudo apt install autoconf  automake cmake libtool
```

On MacOS you would use brew instead, and the download includes a Visual Studio setup to cater to Windows users.

Once the dependencies are installed it's time to build the liboqs library. On Ubuntu 16.04 LTS:

```
autoreconf -i ; ./configure ;  make clean ; make
```

When the commands complete, you should have a library called liboqs.a that must be linked to the final executable. You should also have a header file called oqs.h in the include folder.

Building a Chat Application with OQS

The main purpose of this application is to show how we can use a quantum safe public key algorithm to safely perform a key exchange across a network connection. In other words, the goal is not to write a full-fledged chat application, and, as you will see, the capabilities of the application are quite limited.

By the same token, the code is kept extremely simple, and thus there are many shortcuts. In fact, there are some non-quantum related vulnerabilities that I didn't bother to address. For example, it is vulnerable to side channel attacks, there are potential buffer overflows, and so on. It doesn't matter for demonstration purposes, but would be disastrous in a production system. In other words, it's a toy, so don't use this for real work! You have been warned.

In the following, please refer to the code which follows this article.

The main() function of the program sets up the OQS infrastructure. It then checks the command line to see if it should operate in client mode ("Alice") or server mode ("Bob"), -C and -S respectively. The server listens to a TCP/IP socket on port 36000, and the client communicates on the same port.

The first step is the interesting one: Together the client and server perform a quantum safe key exchange using Frodo. This results in both client and server having a 256 bit (32 bytes) shared key.

This shared key is used by the client to encrypt messages using plain old AES. The client then sends the encrypted message across the TCP/IP socket to the server. The server decrypts and displays the message, adds some text to it, encrypts the message, and sends it back to the client. The client then decrypts the response and displays it. And that's it.

To run the application, open a terminal window and start the program in server mode. Then open another terminal and start the program in client mode. Type some text in the client terminal and you should see the encrypted and plain text in the server terminal. Then the encrypted and plain text response should appear in the client window momentarily. Below is a sample session:

```
$ ./phqchat -S
starting server...

Creating socket
Listening
Accepted incoming connection
Reading first message
Starting key exchange
Bob message          (11288 bytes):  9C211D538E335F5FF276156071598FF
➥4D399BFD6...
4229C83CDBC03595EF844D49474634D28F39ED3C
Bob session key      (  32 bytes):  A26EE735B15F28FB47ECF6F096E661BC
➥ 418601BA8FE2
F3EDF62579045F42646B
Key exchange complete


Encrypted message from client:
ffffffa8ffffff89ffffffd170ffffffeffffffa86c68ffffffddffffffac174bffff
➥ffc1ffffff
927069ffffffff6ffffffda4c341d4f43ffffff965affffffd57dffffff946cffffff85
➥63 b30ffff
ffc3ffffffd8ffffffff1ffffffb2ffffffa2ffffffacffffffff8165b75ffffffdf 4ff
➥ffffa0ffff
ffbeffffffc4
Decrypted message: Hello Bob. Typing something for you.

$ ./phqchat -C
```

```
starting client...
Creating a socket
Starting key exchange
Alice initial message (11280 bytes):  72E12292ECCD6911B3A93D6A6C7B7051
➥B8E3CFB6
...09B337FA6487B088B5127A0CF44EF023A484D973
Alice session key    (  32 bytes):  A26EE735B15F28FB47ECF6F096E661BC
➥418601BA8FE2
F3EDF62579045F42646B
Key exchange complete

Hello Bob. Typing something for you.

Encrypted response from server:
ffffffd951763c 7fffffffc7bffffff8cffffff9a 9fffffffdffffffcb30fffffff5
➥6266ffffff
fc20ffffff8dffffffb23affffff9349ffffff9d76 c3e2fffffffcbffffffe3ffffff
➥eaffffffff6
72 c25556746ffffff80ffffff98ffffffd4ffffffbd4dffffffa6535bffffffb765ff
➥ffff97ffff
ffbeffffffd427ffffffed6ffffffffc9ffffff89ffffff9bffffffeeffffffe011ffff
➥fff8555b13
Decrypted response: Dear Alice,
You typed Hello Bob. Typing something for you.
```

The Road Ahead

As I mentioned, the program we built is a cheap parlor trick. The real value of quantum safe public key encryption technology will be realized when it's incorporated in mainstream applications and tools for quantum secure communications, encryption, digital signatures, and certificates. That has not happened yet, but there are efforts underway. For example, the OQS team has created a version of OpenSSL that uses quantum safe ciphers. It's also available on github. The URL is:

`https://github.com/open-quantum-safe/openssl`

In addition to Frodo, OQS contains several other quantum safe ciphers and tools that you can use to implement communications apps, digital signatures, encryption apps, and anything else you can dream up. Happy hacking!

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
#include <unistd.h>
#include <arpa/inet.h>
#include "oqs.h"


#define LETS_USE_FRODO
#ifdef  LETS_USE_FRODO
/* Use Frodo (Learning With Errors) for the key exchange */
static int algorithm=OQS_KEX_alg_lwe_frodo;
/* Length of the seed */
static const size_t seedLen=16;
/* The seed (16 bytes) */
static const uint8_t *seed="qwertyuiopasdfgh";
/* Use the "recommended" parameter for >= 128 bits of security */
static const char *namedParms="recommended";
#endif

/* Host IP adress */
static const char *host= "127.0.0.1";
/* Port number */
```

```
static const int port=36000;
/* Some data buffers */
static char buffer[16384]={0};
static char plainText[16384]={0};
static char cipherText[16384]={0};
/* Prototypes */
int bob(OQS_KEX *kex);
int alice(OQS_KEX *kex);
int calculatePaddedLength(int len);

int main(int argc, char** argv){
    int rc=0;
    /* Initialize random numbers */
    OQS_RAND *rand = OQS_RAND_new(OQS_RAND_alg_urandom_chacha20);

    /* Initialize key exchange */
    OQS_KEX *kex = NULL;
    kex = OQS_KEX_new(rand, algorithm, seed, seedLen, namedParms);
    if(NULL==kex){
        return -1;
    }

    /* Check command line parms */
    if(argc<2){
       printf("Command line args:\n-C for client mode\n-S for
➥ server mode\n");
    }
    else if(0==strcmp(argv[1],"-C")){
       printf("starting client...\n");
       rc=alice(kex);
    }
    else if(0==strcmp(argv[1],"-S")){
       printf("starting server...\n\n");
        rc=bob(kex);
    }
    else{
       printf("Command line args:\n-C for client mode\n-S for
➥ server mode\n");
    }

    /* Clean up */
    OQS_RAND_free(rand);
    OQS_KEX_free(kex);
    return rc;
}

/* This is for AES. A block has to be exactly 128 bits (16 bytes) */
int calculatePaddedLength(int len){
    if(0==len%16){
        return len;
    }
    int n=len/16;
    return 16*(n+1);
}

/* Set up and run chat program in client mode */
/* Client is Alice by convention */
int alice(OQS_KEX *kex){
    void *alicePrivate = NULL;   /* Alice's private key */
    uint8_t *aliceMsg = NULL; /* Alice's message */
    size_t aliceMsgLen = 0;  /* Alice's message length */
    uint8_t *aliceKey = NULL; /* Alice's final key */
    size_t aliceKeyLen = 0;  /* Alice's final key length */
```

```
    int rc=0;

    /* Open a socket */
    printf("Creating a socket\n");
    struct sockaddr_in address;
    int sock = 0, numChars;
    struct sockaddr_in serv_addr;
    if(0>(sock = socket(AF_INET, SOCK_STREAM, 0))){
        printf("Socket creation error \n");
        rc=-1;
        goto client_clean;
    }
    memset(&serv_addr, '0', sizeof(serv_addr));
    serv_addr.sin_family = AF_INET;
    serv_addr.sin_port = htons(port);

    if(0>=inet_pton(AF_INET,host, &serv_addr.sin_addr)){
        printf("Invalid address\n");
        rc=-1;
        goto client_clean;
    }

    if(connect(sock,(struct sockaddr *)&serv_addr,sizeof(serv_addr))
➥  < 0){
        printf("Connect failed\n");
        rc=-1;
        goto client_clean;
    }

    /* BEGIN KEY EXCHANGE */
    /* Alice sends the Diffie Hellman initial message */
    printf("Starting key exchange\n");
    rc=OQS_KEX_alice_0(kex, &alicePrivate, &aliceMsg, &aliceMsgLen);
    if(OQS_SUCCESS!=rc) {
        fprintf(stderr,"ERROR: OQS_KEX_alice_0 failed!\n");
        goto client_clean;
    }
    OQS_print_part_hex_string("Alice initial message", aliceMsg,
➥ aliceMsgLen, 20);
    send(sock,aliceMsg,aliceMsgLen,0);

    /* Get response back from server */
    numChars = read( sock,buffer,sizeof buffer);

    /* process the response */
    uint8_t *bobMsg = NULL; // Bob's message
    size_t bobMsgLen = 0;  // Bob's message length
    bobMsg=buffer;
    bobMsgLen=numChars;

    rc = OQS_KEX_alice_1(kex, alicePrivate, bobMsg, bobMsgLen,
➥ &aliceKey,&aliceKeyLen);
    if(OQS_SUCCESS!=rc){
        printf("ERROR: OQS_KEX_alice_1 failed!\n");
        goto client_clean;
    }
    OQS_print_hex_string("Alice session key", aliceKey,
➥ aliceKeyLen);
    printf("Key exchange complete\n\n");
    /* END KEY EXCHANGE */

    /* Now start the chat */
    while(1){
```

```
        /* Get input from keyboard */
        memset(buffer,'\0',sizeof buffer);
        fgets(buffer,sizeof buffer,stdin);
        numChars=strlen(buffer);
        int len=calculatePaddedLength(numChars);

        /* Encrypt using session key */
        memset(cipherText,'\0',sizeof cipherText);
        OQS_AES128_ECB_enc(buffer,len,aliceKey,cipherText);

        /* Send encrypted message */
        send(sock,cipherText,len,0);

        /* Get response*/
        memset(buffer,'\0',sizeof buffer);
        numChars=read(sock,buffer,sizeof buffer);
        len=calculatePaddedLength(numChars);
        printf("\nEncrypted response from server:\n");
        for(int i=0;i<len;i++){
            printf("%2x",buffer[i]);
        }

        /* Decrypt using session key */
        memset(plainText,'\0',sizeof plainText);
        OQS_AES128_ECB_dec(buffer,len,aliceKey,plainText);
        printf("\nDecrypted response: %s\n",plainText);
    }


client_clean:
    OQS_MEM_secure_free(aliceMsg, aliceMsgLen);
    OQS_MEM_secure_free(aliceKey, aliceKeyLen);
    OQS_KEX_alice_priv_free(kex, alicePrivate);
    OQS_MEM_secure_free(bobMsg, bobMsgLen);

    return rc;
}

/* Set up and run chat program in server mode*/
/* Server is Bob by convention */
int bob(OQS_KEX *kex){
    uint8_t *bobMsg = NULL; // Bob's message
    size_t bobMsgLen = 0;  // Bob's message length
    uint8_t *bobKey = NULL; // Bob's final key
    size_t bobKeyLen = 0;  // Bob's final key length
    uint8_t *aliceMsg = NULL; // Alice's message
    size_t aliceMsgLen = 0;  // Alice's message length
    int rc=0;

    /* Set up a listen socket */
    int server_fd, new_socket, numChar;
    struct sockaddr_in address;
    int opt = 1;
    int addrlen = sizeof(address);

    /* Creating socket file descriptor */
    printf("Creating socket\n");
    if(0==(server_fd = socket(AF_INET, SOCK_STREAM, 0))){
        printf("socket failed\n");
        exit(EXIT_FAILURE);
    }

    /* Bind listening socket to the port */
```

```
    if(setsockopt(server_fd, SOL_SOCKET, SO_REUSEADDR |
➥ SO_REUSEPORT,&opt, sizeof(opt))){
        printf("setsockopt failed");
        exit(EXIT_FAILURE);
    }
    address.sin_family = AF_INET;
    address.sin_addr.s_addr = INADDR_ANY;
    address.sin_port=htons(port);
    if (0>bind(server_fd, (struct sockaddr *)&address,sizeof(
➥address))){
        printf("bind failed");
        exit(EXIT_FAILURE);
    }

    /* Wait for a connection */
    printf("Listening\n");
    if (listen(server_fd, 3) < 0){
        printf("listen");
        exit(EXIT_FAILURE);
    }

    if(0>(new_socket=accept(server_fd, (struct sockaddr *)&address,
➥ (socklen_t*)&addrlen))){
        perror("accept");
        exit(EXIT_FAILURE);
    }
    printf("Accepted incoming connection\n");

    /* BEGIN KEY EXCHANGE */
    /* Read the first incoming message */
    printf("Reading first message\n");
    memset(buffer,'\0',sizeof buffer);
    numChar=read(new_socket,buffer,sizeof buffer);

    /* Process first incoming message, which is part of key
➥ exchange */
    printf("Starting key exchange\n");
    aliceMsg=buffer;
    aliceMsgLen=numChar;
    rc=OQS_KEX_bob(kex, aliceMsg, aliceMsgLen, &bobMsg, &bobMsgLen,
➥ &bobKey, &bobKeyLen);
    if(OQS_SUCCESS!=rc) {
       fprintf(stderr,"ERROR: OQS_KEX_bob failed!\n");
        goto server_clean;
    }

    OQS_print_part_hex_string("Bob message", bobMsg, bobMsgLen, 20);
    OQS_print_hex_string("Bob session key", bobKey, bobKeyLen);

    /* Send the message to client */
    send(new_socket,bobMsg,bobMsgLen,0);
    printf("Key exchange complete\n\n");
    /* END KEY EXCHANGE*/

    while(1){
        /* Wait for next message */
        memset(buffer,'\0',sizeof buffer);
        numChar=read(new_socket,buffer,sizeof buffer);
        int len=calculatePaddedLength(numChar);
        printf("\nEncrypted message from client:\n");
        for(int i=0;i<len;i++){
            printf("%2x",buffer[i]);
        }
```

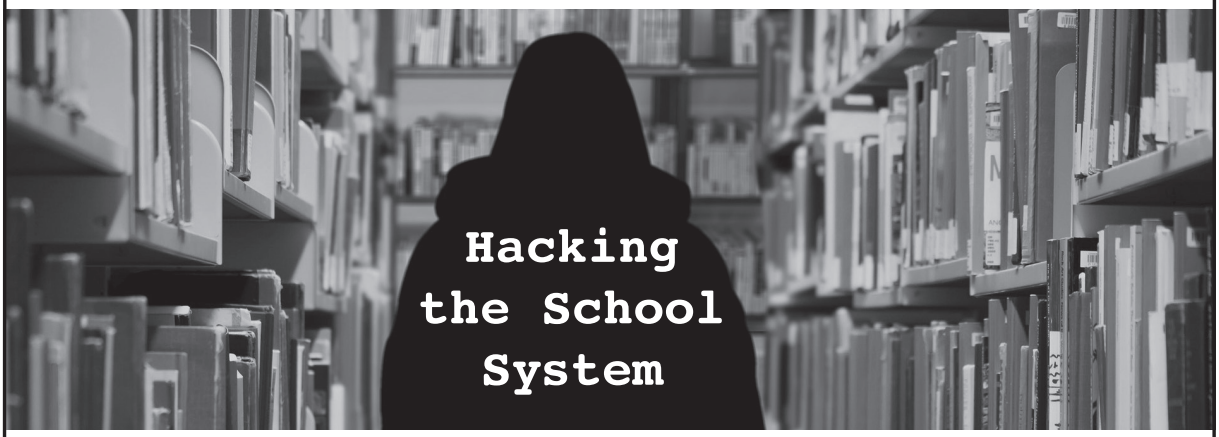
```
        /* Decrypt using session key */
        memset(plainText,'\0',sizeof plainText);
        OQS_AES128_ECB_dec(buffer,len,bobKey,plainText);
        printf("\nDecrypted message: %s\n",plainText);

        /* Compose a response */
        memset(buffer,'\0',sizeof buffer);
        sprintf(buffer,"Dear Alice,\nYou typed %s\n",plainText);
        numChar=strlen(buffer);
        len=calculatePaddedLength(numChar);

        /* Encrypt it using session key */
        memset(cipherText,'\0',sizeof cipherText);
        OQS_AES128_ECB_enc(buffer,len,bobKey,cipherText);

        /* Send to client */
        send(new_socket,cipherText,len,0);
    }
server_clean:
    OQS_MEM_secure_free(bobMsg, bobMsgLen);
    OQS_MEM_secure_free(bobKey, bobKeyLen);
    OQS_MEM_secure_free(aliceMsg, aliceMsgLen);

    return rc;
}
```



Hacking the School System

by Behawolf

When I was a kid, I used to believe teachers were always right. Like a computer following a programme, I assumed the person giving the instructions knew what they were doing. I thought just so long as I worked hard, and followed all the rules, I would be OK. Alas, this has proved to be far from true. So here is what I wish I had known.

Before we can hack any system, we need to understand it. The school system was introduced in response to the industrial revolution, by governments. This was not done out of the goodness of their little hearts, but as a way to train children for the industrial workforce. As in the factory system, fear was the main means of control. The main purpose was to instill obedience into the child. Thus, learning requires passivity from the student, and getting used to doing repetitive and menial tasks for minimal pay, just as it is today. These qualities might be necessary for the school system, but will be a complete hindrance to you for the rest of your life in whatever you decide to do. Unless of course you want to be stuck in a dead end job.

Capitalism is a tough environment, with everyone trying to sell you something, regardless of whether you want it or not, regardless of whether you need it or not. But we've all got to pay the rent. So, there is no shame in wanting to make a better life for yourself, especially if you are living in an environment that is physically or mentally harmful to you. I'm with you bro.

So, assuming you can't persuade your parents of the benefits of home education, how can we hack the school system and make it work for you? Since I am writing for kids like you all over the world, I am only able to give you general advice.

If you can't get off the school premises, then try and find a safe place within the building. You may want to consult some texts on urban exploration for this. Think creatively - maybe there are some air ducts you can squeeze into. Don't forget a torch for reading, some spare batteries, and something comfortable to lie on. Be careful not to get lost or stuck in there if you decide to go exploring. Or what about a locked door you can pick, or get the key to? Maybe you can "borrow" the key and get a copy made or, if you're lucky, maybe it's a generic key you can buy from a key shop. Wherever you go, make sure you are not followed. Don't get careless. If no one will mind you being there, just spend all your free time in the school library. The important thing is that you are safe from teachers and bullies.

If you want access to information and computers for an affordable price, go to your local library. If they haven't got the book you want, then they should be able to order it in from another library, possibly for a small fee. If you want to highlight in the book for future reference, it might be worth buying it. Note, computer books tend to date very quickly - although books about programming languages and UNIX-based commands, less so. If you want to figure out how people's emotions work, read literary fiction.

Don't do homework unless you really want to. The only time you need to do work at home is if you have course work that will count towards your final exam. I leave it up to you, dear reader, to decide whether you want to worry about any end-of-year exams. Ultimately, the only thing that counts is if you get any qualification for the exam you are doing. Employers like qualifications, so try to get some from school if you can.

If people start hassling you for not doing enough work, demand payment, and don't do any work until you get some money. Pay negotiation is a key survival skill for adult life. If they do pay up, you can then use some of this money to help fund your further education, be that another course after you leave school, or books that you want to read now.

School sport is merely an excuse for the bigger boys to hurt you through physical violence. So, unless you are one of the bigger boys or girls, skive off it. Have you ever noticed how the sports teacher gives everyone the orders to run about like headless chickens, while they stand there doing sweet FA? Eating healthily, with a little exercise each day, will be much better for you than school sport. A brisk walk for ten minutes should do it. One mistake I didn't make was to take up smoking. Smoking is the work of The Man. They get you addicted so you have to keep spending money to buy a product that will slowly kill you. Stick it to The Man. Don't smoke.

Be wary of any religion they try to instill/brainwash you with. In my experience, this is an attempt to keep you in fear. It makes it easier for those in power to manipulate you. They do this by making you feel guilty for having basic human emotions. It is essential to rebel against the idea that one should stoically take whatever life throws at you, as God will look after you. It is not virtuous to become a victim, no matter how many religious stories they tell you, implying God will bail out the meek. So you don't have to be nice to nasty people. Standing up for yourself does not make you a bad person.

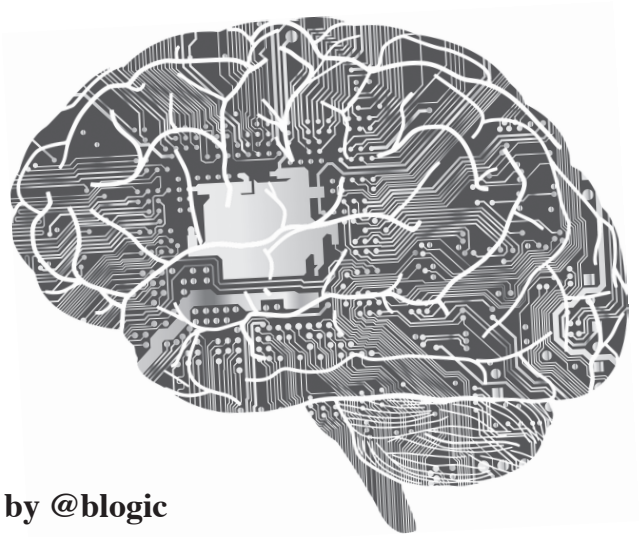
If all of this sounds like the bitter rantings of a Generation Xer, then perhaps it is. But this is what I have learned.

Now you have more free time and you have the space to work things out for yourself, at your own pace. I would recommend you go over anything you have not understood in class. Then you can study what you are interested in, be that the sea, or C++, Python, or philosophy, Linux, or Tantric sex.

I hope this proves useful to you.

Best of luck!

A READING OF THE AI HYPE METER



by @blogic

The hoopla of artificial intelligence (AI) among the industry continues. Buzzwords like machine learning (ML), prediction, and AI continue to infiltrate the cyber security consciousness with a bit of fabrication. There was a 112.5 percent increase from last year in the number of briefing summaries and training descriptions from the big summer hacking conferences containing the following key phrases: data science, machine learning and artificial intelligence. At Defcon, there were three mentions of these keywords in 2017 and four mentions in 2018. Blackhat had a steeper jump in hype with a count of five in 2017 to 13 in 2018. This is palpable enough that I hope readers like you will want to learn more about it. Even though vendors and your colleague at the water cooler may think AI will be the panacea or the Terminator of the hacker, let's first start off with a realistic understanding of ML for cyber security before we reach conclusions that AI will be taking our jobs.

In its truest form, AI learns on its own and improves on its capabilities to make better decisions like humans. Today we have pseudo-AI and their names are Siri and Alexa, yet neither have been able to defend against a zero day or develop a patch for my Mac firmware that prevents against undiscovered vulnerabilities. ML is being used to drive cars and tweet nonsense like Microsoft's "Tay." Under the hood, it has the ability and agility to learn without being programmed with rules and logic.

Let's take, for example, the daily activity of security engineers. They create static/pattern matching rules for intrusion detection systems (IDS) to identify attack signatures and patterns from network flows. If true AI were to create new IDS rules (without a security engineer's assistance), it would use historical signatures and attack logic to make brand new signatures against unseen attacks on the fly. Even though there are valiant attempts to use ML for understanding netflow and learning new attacks, building new signatures to block attacks on the fly with algorithms is not feasible yet.

Can ML and Cyber Security Coexist?

As much as we want Siri or Alexa to build IDS signatures for us, there are already worthwhile cyber security use cases in the field today. With ML we can use methods like supervised and unsupervised models to identify malicious activity. For a supervised machine learning algorithm, we use labels like confirmed "threat" to identify a direct hit from a verified threat actor or a malware detection match from an Internet download. Unsupervised machine learning algorithms don't have labels, but the data can be leveraged by user and entity behavior analytics tools to cluster users' suspicious activity or differentiate network flows from an attack versus a misconfigured internal system.

In both unsupervised and supervised machine learning, there needs to be a vast amount of curation on the data set to feed the algorithms that then derive output. Data quality is crucial to the success or failure of ML to accurately pinpoint malicious activity from the vast amount of noise analysts see today. This data validation accounts for the majority of the effort implemented

in a machine learning model.

Below is a basic Python structure of an ML prediction model:

```
#prediction code
X = dataframe.filter(['feature1', 'feature2','feature3','feature4'
➥ ,'feature5')]
y = dataframe.filter(['dependent_variable'])

import sklearn and train,test and split packages
from sklearn.cross_validation import train_test_split
X_train, X_test, y_train, y_test = train_test_split(
➥ X, y, test_size=0.2)

# logistic regression is the prediction algorithm of choice
from sklearn.linear_model import LogistricRegression
from sklearn import metrics
logreg = LogisticRegression()
logreg.fit(X_train, y_train)

#Determine the accuracy of model
From sklearn.metrics import accuracy_score
Logreg.fit(X_train, y_train)
Predictions = logreg.predict(X_test)
accuracy = accuracy_score(y_test, predictions)

#scoring the model
print('Accuracy score: ' )
print(accuracy)

#cross validation matrix for accuracy
confusion_matrix = confusion_matrix(y_test, predictions)
print(confusion_matrix)
fig, ax - plot_confusion_matrix(conf_mat=confusion_matrix)
plt.show()
print ('#TRUES POSITIVE | FALSE POSITIVE')
print('FALSE NEGATIVE | #TRUE NEGATIVE')
```

Conclusion

In order for supervised and unsupervised models to accurately identify attacks, they will first need a domain expert to infer this context within the data and tune the algorithm to get better results. Without a combination of domain expertise and proper implementation of a prediction model, algorithms can be extremely biased or even dangerous. For example, many systems have machine accounts configured by humans that run scripts. If that machine's account password expires and a human doesn't change it, it may fail to run a script 139 times in an hour. This activity may appear as an outlier among other machine activity, but it's not a brute force attack.

Machine learning is not a silver bullet that will solve cyberattacks. Let's be wary of vendors stating that their products are foolproof or "100 percent predictive and prevent[s] cyberattacks from being successful." The human element of creativity and ingenuity is existential to both the hacker and the defender. The human way of solving problems will always reign over the future of ML decisions which will lead into AI.

George Box, one of the greatest statisticians of our time said, "All models are wrong, but some are useful." In fact, some machine learning prediction models can be useful to the offensive attacker and defender blue teams alike. Because of the endless announcements of breaches and leaks of private and personal information we are now accustomed to, our blue teams need help sifting the signal from the noise. Although the margin for error in these investigations is extremely thin, there is still a large margin of upside to derive malicious signals with the use of ML. Along this journey for ML, we still must understand the caveats, be careful with implementation, and understand that our output may be wrong or biased. More importantly, let's empower our security analysts to overcome the monotonous work that leads to career burnout.

The Hacker Perspective

by BJ Snyder

I'm a hacker and you're not! Nah nah nah na! Or am I? I think that everyone is using the term so loosely that the meaning is lost. I'm a hacker. You're a hacker. My grandmother was a hacker. Actually she was a junk collector and metal scrapper. But I think when you call yourself a name, it doesn't have the credibility as if someone else had called you it.

A friend of mine said he would call me Spock because I like math and science and I am more about the ideas than actually the business side of earning money. Well, to be called Spock is an honor. But the fact remains that there is already a Spock and I can't fill his shoes. On my website, I took to calling myself "Trurl." I don't know if you have read Stanislaw Lem's *The Cyberiad,* but Trurl also has some big shoes to fill. I think a title or nickname should come from your peers, critics, or friends. Friends call me BJ or Beege. I think that is a fitting nickname based on my name. But there is no reason why BJ shouldn't become a hacker. The fact is he should worry about the things a hacker does and leave the title to philosophers.

I don't want to put forth the opinion that hackers are bad or that everyone cannot be one. I just think the actual things that make hackers hackers are the ideals. I know this is "The Hacker Perspective," but I believe you are talking to a non-hacker. Again, I know those of us reading *2600* know the true meaning of a hacker: one who is not a destructive criminal, but one who learns for the sake of learning and tries to be creative, even when corporations try to dominate the world. I am not trying to insult those who consider themselves to be hackers. In a sense, you probably are a hacker. I am happy with this definition. I just want to challenge anyone who considers themselves to be a hacker to act as one and not worry about the terminology.

Let's consider an example. You are a broke, overworked undergraduate in college who happens to play the lottery when the jackpot is multi-millions. You win. But what did you lose? There are benefits to being a "starving artist." The multi-millions have just ruined you. Now you have "friends" or those who claim to be friends and relatives you have never seen asking for money. That supermodel who wouldn't talk to you before has suddenly fallen in love with you. It is difficult to find true love, but somehow you just did. The fact is that being a millionaire has just affected how you live and how the future of your life will go. Is it better? I don't know. But maybe you were a better, more motivated, creative person when you were that starving hacker. Heck, maybe this is the reason most hackers don't care about money. They know the dangers of what it does, how it can affect their lives, and that it isn't their ultimate goal.

Let's consider another example of being classified as a hacker. Did you ever see the Spider-Man comic where Peter Parker is out of his suit and can't fight the Green Goblin? Maybe the suit does make the man - just as the term hacker can make people perceive you as a criminal. I'm not saying it should, but you have to admit it does happen a lot. It is like when a criminal can't commit a crime without a mask. Of course they don't want to be identified, but if the victim could see them they would be ashamed of their actions. Being defined as a hacker could work to make you into a criminal, or it could make you believe you're something you're not. If you let others make the call as to whether you're a hacker or not, I believe you have the potential to make the term what it should be. You define the word hacker; it does not define you. If you want hacker to mean someone who creates or builds, I think you have just broken the mold of criminal. We should be hackers by example and not by false percep-

tions. So we all might be hackers after all. But when everyone is a hacker, we get compared to the criminal element of hackers. But that categorizing is only done by those who are ignorant of the hackers that we are.

So don't think it isn't important what type of hacker you are. It is like the police force saving a woman from a burning car and then the next day five cops beat up some teenager. Do you remember that cops are good and there to protect us? No. You see that cops are corrupt. This will cause the whole honorable meaning of what it is to be a police officer to be forever tarnished by a fraction of those who belong to the force. So you think that crashing a computer or placing a Trojan on someone's system will go unnoticed? Do you want to tarnish what it is to be a hacker?

That is enough of not self-proclaiming yourself to be a hacker. Chances are if you are reading this message you are a hacker. But let's not call ourselves hackers; let's lead by example and show the world what hackers do.

I think the greatest factor in how we will be judged as hackers is by what we create. The Nobel Peace Prize was created out of Alfred Nobel's guilt for inventing dynamite. A hacker's dynamite may be malware. Not all creations are good. I have seen a PBS documentary on microbiologists who were making viruses. Why on earth would someone do such a thing? They claim that it helps them to understand viruses better, but it is the deadliest of weapons. So when designing something, we should be aware of the results. It may be an impressive achievement to create something, but how will it be used?

I love cryptography. I have spent hours reading, researching, and trying to discover new methods. This could be considered hacking, but I don't want to call myself a hacker. The fact remains that I have to break 256-bit RSA before anyone cares about any of my work. While there is a big following of math and cryptography on the Internet, most people I show my work to don't care. It just doesn't interest them. If you care about being called a hacker, you may be disappointed when the vast majority doesn't care. But the beauty of being a hacker is that you don't care that people don't care. But we do care when they perceive us a criminals. What would I do if my equations broke RSA? I would be known as the guy who broke a 40-year-old algorithm. I don't believe I could actually do that. But if I did break RSA, I would be known as the guy who crippled security - a title I would not want. But if a civilian could break or, at the very least, show a pattern in RSA, I imagine the NSA already knows about it. Maybe it is the hacker part of me that doesn't like ciphers that can't be broken. I feel a need to find why.

As part of "The Hacker Perspective," we are supposed to share our hacking views and past experiences. Perhaps me not wanting to be called a hacker stems from my lack of credentials. That is at least what Sigmund Freud would say. My id wants to take control of the Internet, but I have delusions of being able to find the product of two prime numbers. But here, we know that achievements and credibility are not the only things that make a hacker.

Maybe the psyche is the key to the hacker. I want to be a mathematician, inventor, and engineer, but I am intimidated into thinking I have to have the achievements of Newton. I had a coach say: "Never let anyone intimidate you." This is because once you get it in your head that you can't do something, you will not succeed. If you think you aren't a hacker, I guess you aren't one because you decided that you are not.

Just as I cannot categorize the hacker, neither can anyone completely categorize you. We are more than just labels and multiple choice questions. Personally, I hate psychology because most of it is fluff. I mean, why analyze people instead of accepting them for who they are? I know it is important to study ways that people learn, but so much of it is looking for man's answers to spiritual questions. Spiritual beliefs are personal. Believe what you want insofar as what you believe the definition of a hacker to be, but you must admit the psychologist categories of people benefit only psychologists' opinions on how the world works. Just as we don't understand most of the world, who is qualified to call you a hacker? Who better to understand you than you? It doesn't matter if you refer to yourself as a hacker or not. Just by doing what you do, the proper definition will find you. The word hacker isn't just a title. It is a way of life.

THE CIRCLE OF HOPE

VIDEOS

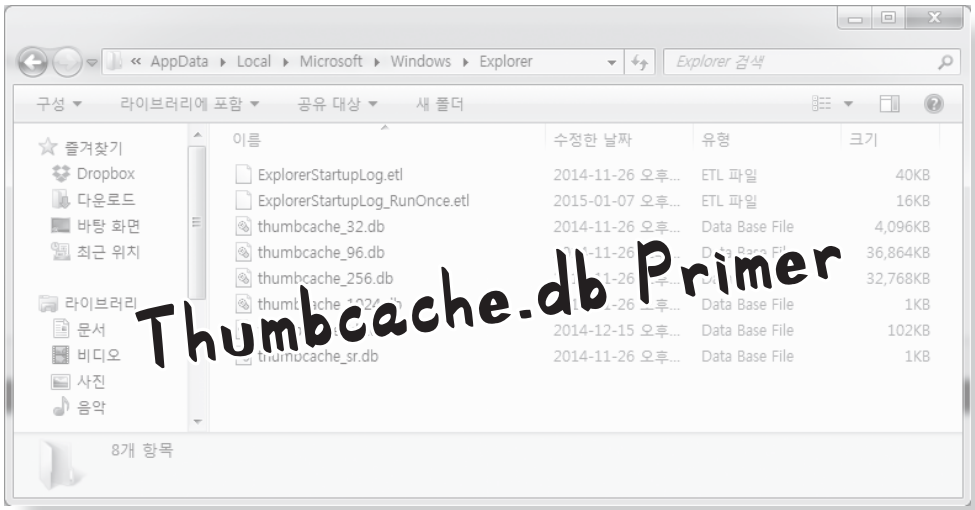
**There's no way you could have seen it all,
whether you were there or not. We can help.**

As is our tradition, we have an archive of all of the talks that were given at this year's HOPE conference. There are far too many to list here, but suffice to say, we have more content than ever before - all in high quality HD recordings. The efforts of the folks over at the Internet Society and our amazing A/V team make all of this archiving possible.

We're making these available in three ways:

- Full sets of all talks in MP4 format, no DRM, easy to copy, for $89 on more than one thumb drive (we're at that awkward stage somewhere between 128GB and 256GB).
- On DVD, where a full set of over 100 DVDs will cost $249 or $2.99 per DVD (you can see a full listing of talks at xii.hope.net or on our store site below).
- For download directly from **store.2600.com** at 59 cents a talk - you get the same MP4s that would come on the thumb drives, but you can choose the ones you want and not have to deal with any hardware.

Looking for HOPE shirts? Sorry, we sold out at the conference for the first time ever! But we have plenty of other cool things like our 2019 Hacker Calendar, *2600* baseball caps, hoodies, etc., etc.



by Michael L. Kelley Jr.

Thumbs.db is a Microsoft Windows thumbnail cache "database" file. This file holds information pertaining to thumbnails of images saved on a computer. The most common file types that make up these thumbnails are from .JPG, .PNG, and .BMP files. This file can also include thumbnails from formats other than images, such as DOCX, PDF, HTML, AVI, and others. In forensics, this is a pertinent file to pay attention to. The main reason being that when images are deleted from a computer, thumbs.db will retain the thumbnail data for the image file unless it is cleared out too. Some might be unaware of this, allowing forensic investigators to trace back an image that was previously deleted. Thumbnails have been brought up numerous times in court cases. For the purposes of this article, I will be working with the Windows 10 operating system and a few bits of Python 3 code just for fun.

General

Thumbs.db has been around in Windows since Windows 95. By default, thumbs.db is a hidden system file and is automatically created by the operating system when image files are present in a folder. Thumbnails are created to help speed up image processing and to provide a quick preview for images in Windows Explorer. If an image is deleted, the information will be retained in the thumbs.db file. From a forensics standpoint, thumbs.db is significant and can be used to prove if an image was indeed on a given computer system at one time. In Windows XP and earlier, the thumbs.db file would get created whenever there was an instance of an image thumbnail. The thumbs.db file would be stored in the same folder where those images occurred. In my opinion, this makes the thumbs.db thumbnails easier to work with and find. Starting with Windows Vista and later, thumbs.db was switched with thumbcache_xxx.db files, where the xxx corresponds to maximum pixel size. The format of these files are:

```
thumbcache_16.db
thumbcache_32.db
thumbcache_96.db
thumbcache_1024.db
```

And so on and so forth, according to the resolution size on your given machine.

In Windows 10, thumbs.db is a handled a little differently. Instead of making a .db file in every folder that has an instance of an image, Windows keeps the thumb cache files in a central location. Thumbnails are only generated for images saved in a user's directory. You must enable hidden files to see these files show up. These files are found under a given user's profile in the location at:

```
C:\Users\%username%\AppData\
➥Local\Microsoft\Windows\
➥Explorer
```

Thumbnails also have a distinct ID that corresponds to each thumbnail. This is called the ThumbnailcacheID and a list of these ID values can be found in the file thumbcache_idx in the above folder.

Setup

For this article, the following software will be used/looked at. Please install in order to follow along:

- Microsoft Windows 10
- Python 3.6.4 - `www.python.org`

- Thumbcache Viewer - thumbcache ➥viewer.github.io
- Thumbnail Database Cleaner - www.it ➥samples.com/thumbnail-➥database-cleaner.html

Enabling Hidden Files and Folders in Windows 10

- Open a File Explorer window
- View > Options > Change folder and search options
- View tab > Advanced settings > Show hidden files, folders, and drives > OK

Research

To begin, copy a few image files to a new folder on your desktop named "Photos". Open them up a few times. Now we will use Python to make sure the thumbcache.db files are present on your machine. This code was run in Python 3.6 and assumes you run the program from the specified folder. Also make sure you change the file path in the code to reflect your specific username:

```
import os
# assign variable for file list
files = os.listdir(r"C:\Users
➥\%username%\AppData\Local\
➥Microsoft\Windows\Explorer")
# print the contents of the
➥ directory
print(files)
```

You should see the various thumbcache.db files showing up in that directory. Now, we will want to grab a copy of one of the thumbcache.db files and save it to another location for later use. We will use some quick Python code to accomplish this as well. Make sure you run the Python file from the same directory that the thumbcache files are located. If you want to skip the Python code you can just use the old fashioned right-click Copy > Paste. The code to copy the file is:

```
import shutil
# copy a file and then make a
➥ new copy
# shutil.copyfile(src, dst)
# copied file name must be
➥ different
shutil.copyfile('thumbcache.db',
➥ 'thumbscopy.db')
```

Now, open the Thumbcache Viewer program you installed earlier. We will use this to check what is going on with the Thumbcache.db files located in the Explorer folder. Once Thumbcache Viewer is opened, navigate to one of the thumbcache.db files and open it up.

What do you notice? The contents of the image you just deleted are still visible in the thumbcache.db file. If this were an investigation, you would have just been found out! This is the magic of the thumbs.db and thumbcache.db files and how they can be used for evidence. If someone could get access to these files, they could see the thumbnails for images that may have been deleted from their original folders/location a long time ago.

One important note is that the thumbnails found in the thumbcache.db files do not retain the same file name as the original image that they point to. Instead, they are named using a Unicode string, the ThumbnailCacheID. This ID is useful to have to be able to tie together the thumbcache entry to the original source image because thumbcache.db files do not store the path to the source images in the way that thumbs.db files do. To research this aspect further, check out the Thumbcache Parser software by Guidance Software.

Thumbnail Database Cleaner can be used to clear out the thumbcache.db files. Once cleared, remember that the files will begin to repopulate for any future images on your system. You can also have Windows disable thumbnail caching by going to Folder Options and enabling the setting "Always show icons, never thumbnails." This will ensure that the thumbnail_xxx.db cache files do not get generated. Another program that is able to clear out thumbnail cache files is CCleaner, which can also clear out various other temporary and junk files.

Additional Software

- FTK Imager
- Vinetto
- Nirsoft's ESEDatabaseView

Further Research

- Using a program such as FTK Imager with these thumbnail files
- Using a hex editor with these thumbnail files to examine differences
- Comparing the hash from a thumbcache

file to that of a Windows generated file of the original content

- Examining thumbcache files from an encrypted system. What do you notice?
- Obtaining some thumbcache.db files from another system and seeing what you can find
- Researching important court cases that used thumbnails for evidence

Further Reading

https://bit.ly/2GPP8ST
http://bit.ly/2GzQa2P
http://bit.ly/2HCXGsQ

Conclusion

Thumbs.db and thumbcache.db are featured in Windows operating systems to speed up image processing and loading times, but the impact they have in computer forensics can be significant. Knowing that these files exist is important because they take up space, can be used to track down a lost image, and can be used as evidence to show that an image was connected to a specific computer system in some way. Play around with these files and see what you can come up with. *Shout out to my fellow forensics alumni: Michael Sapienza, Verna Mineard, and Danielle Yandura. Also, special thanks to my computer forensics mentor, Dr. Raymond Hsieh. Take care.*

Sorting It all Out: The Long Lost Bastard Children of the United States Postal Service

by Pop Rob
poprob.com

Years ago, I worked as a data conversion operator for the United States Postal Service Remote Encoding Center. That may sound important if you are unfamiliar with the job, but when it comes down to it, we were simply doing data entry. At its height, my facility employed around one thousand people who all worked assorted hours, day and night, typing in zip codes and addresses deemed unreadable by the sorting machines at the postal processing plants. I worked there for about five years, and something always nagged at me as I sat there night after night at my static-colored desk, keying millions of random addresses from mail pieces: "Where do these images go next?" and "Are there images of *every* mail piece sent saved somewhere?"

Let me back up here for a bit of history - in 1994, the USPS established the Remote Encoding Centers (or RECs) as a temporary solution to help with processing mail with unreadable addresses. When mail is processed at sorting facilities, everything is run through sorting machines that scan the face of the package or envelope with optical character readers. If the scanner is unable to read the address on the mail piece, it transmits an electronic image to a REC, where the image would then be displayed on a terminal for one of the data conversion operators to key in what they see displayed for the mail piece. Sometimes the system would ask for the specific information needed - postage type, street address, zip code, etc. Then, the information is transmitted back to the processing plant where a barcode strip (usually seen on the bottom of envelopes) would be applied to the mail piece to get it to the right destination. This is similar to what happens if you have ever moved and had your mail forwarded to another location - the sorting machines check to see if there is a Change of Address (or COA) in the system, and a yellow sticker with the updated information is printed and plastered over the previous address. By 1997, the USPS had 55 RECs open across the nation with thousands of people employed for this task. However, the plan was never to keep

these centers open forever. A combination of decreasing letter volume and improving scanning technology would quickly bring better readers at the plants that would reduce the need for the encoding centers. Mine was one of many that shut down in a consolidation effort back in 2007. Today, only one lone REC remains in Salt Lake City, UT - which employs more than 1,200 workers who process around four million images a day.

In our post-9/11 world, why wouldn't our government agencies take advantage of the resource of having a record of physical correspondence sent from one person to another? The NSA has collected phone records since the dinosaurs. The entire Internet is nothing more than an elaborate market research experiment. Surely there is a vast database somewhere holding the history of what has traveled through the mail stream. A simple Google search confirmed my theory: In 2013, a *New York Times* interview with then Postmaster General Patrick R. Donahoe confirmed that the USPS uses imaging to photograph each envelope and package that passes through. After all, they have to be scanned to be sorted to the right location. He also verified publicly that it is practice to offer that information to law enforcement agencies if requested as part of criminal cases, but that the images were destroyed after 30 days, as it would not be cost effective or possible for someone to store images of billions of pieces of mail. Well, sure. The USPS may not have that capability - but surely interested parties have plenty of server space lying around, right?

Assisting with surveillance is a common practice for the USPS, as agencies can also make requests under the program called Mail Covers for postal employees (i.e:, your local carrier and clerks) to record names, return addresses, and other information from letters and packages before delivering to the recipient in question. However, as it is still a federal offense to open someone else's mail and would require a warrant to do so, only the outside information can be recorded. As you may know, the USPS even has their own law enforcement arm known as the United States Postal Inspection Service (USPIS). While the USPIS's main objective is to protect the integrity of the mail system to prevent it from fraud or abuse, and to protect the well-being of USPS employees, they are essentially sworn federal officers who carry firearms, make arrests, and also work alongside other agencies as needed. What does that have to do with images of the mail? Not much, but it sounds *bitchin'*.

There are certainly practical and legitimate reasons for keeping historical records of the mail, both on the internal USPS side as well as the law enforcement side. However, the obvious drawbacks to visual images are that if someone is going to send something harmful or suspicious, it is doubtful they are going to put their name and return address on the outside of the package. While the process of scanning the images of the mail was originated as a result of the technology used to make the sorting work, it would only make sense to utilize those same images available for alternate purposes. The concern is how can this turn into unwanted surveillance for an unsuspecting person? What if someone is sending illicit materials through the mail and is being monitored and you just so happen to by a harmless *Golden Girls* Season One DVD sent from them off eBay? Are you being monitored now? While none of this really makes much difference to the common everyday citizen who is not overly obsessed with privacy rights, this simply points to yet another facet of our life that is under the ever-enlarging microscope. Everything is on the record.

I would be curious to hear from the USPS today to see if they are still destroying those images after 30 days, as was reported back in 2013. My guess is no - hard drives are a dime a dozen.

Addendum

After the writing of this article, there are now reports of a new USPS service called Informed Delivery, where the scanned images attained by the Postal Service can be sent to customers to notify them of the mail being delivered to their address. This has come up in the news, as people are abusing the service to sign up for addresses that are not their own in order to know what is being sent - for potential theft of packages left unattended. This indicates a further expansion of the use of scanned images by the Postal Service, now as a customer service for recipients to access and monitor as well. Guess they found some more drive space for those images.

Configuration Negligence: Who is Responsible?

by lg0p89

A hotel is much like any other business. The network is present along with the cabling, switches, server, etc. Another like area is Wi-Fi. In a business, there would be a guest and an internal Wi-Fi network to connect with. The distinction is clear in that the guest Wi-Fi is for the convenience of the visitors and the internal is for the staff to conduct business. The internal Wi-Fi has access to the sensitive portion of the business where authorized persons should be.

As a rule of thumb, more cybersecurity would be applied to the internal Wi-Fi and network. After all, the business would not want unauthorized persons nosing about in their private and confidential area, files, and systems.

What Happened

A security researcher from China visited Singapore and stayed at the Fragrance Hotel in late August 2018. The researcher was attending the Hack in the Box conference and participated in the capture the flag (CTF) competition. The researcher happens to work at Tencent, which should sound familiar to those involved in red-teaming vehicles. Being a security researcher, he naturally was curious and began to investigate, using his tech finesse to test the hotel's Wi-Fi. As the researcher stayed at the hotel, he detected the hotel's Wi-Fi system. The hotel's Wi-Fi used the Ant Labs' IG3100 gateway for authentication. This device happens to have backdoor accounts for telnet and FTP. These services have not been an industry standard for literally many, many years. These services are rather insecure and easy prey for attackers. On another point, the services had backdoor accounts open, which also is not prudent. On yet another point, the default login credentials also happened to be publicly published. These also had not been changed.

Thus, entering the system was very easy with this data. While in the system, the researcher noted a server was present still running MySQL 4.1.2. The password happened to be stored in the /etc directory. The researcher had access to the admin account and had complete control. The researcher, specifically, was able to monitor the devices on the system, the number of clients logged in, and other data with the system. The researcher posted this on a blog, which began his issues in earnest.

Breaking the Law

The laws are naturally different for each country, as well as certain laws within each state. In Singapore, the researcher could have been put in prison for years and received a massive fine. In this case, compromising the system clearly was against the law, unless authorized. He did not have permission to do so. The researcher posting the compromised information added insult to the injury. The researcher ended up being fined SGD $5,000 (USD $3,500).

In a Different Frame

Indeed, the researcher compromising the system, even without a malicious intent, was not the optimal route. The researcher should not have been meandering about in this gray area. Yes, he should have received some form of punishment as negative reinforcement for his acts.

On the other side, the hotel, however, should accept a good portion of the blame and responsibility. The hotel did not act even remotely in a reasonably prudent manner. The password treatment and using telnet/FTP were shameful at best.

This is analogous to a tort law (attractive nuisance) in the United States. If you happen to own a pool, for example, in the U.S. under common law, you should not just have this in the open without any form of barrier (i.e., a fence). If you do not have a barrier in place and a child walks into the pool and drowns, you may be sued, depending on the jurisdiction, under the attractive nuisance doctrine. Of course, the researcher is not a child and has the ability to reason as an adult would.

The issue is more with the manner in which the hotel did not appropriately handle its business. There were several missteps taken by the hotel, which may have been in place for years. These services should have been configured correctly in line with the industry standards at the time, which had been in place for years, and updated as needed. Having this poorly configured system in place and in full operation is a complete dereliction of duty in so many ways (e.g. telnet, FTP, passwords easily found on the server, not changing the default passwords, etc.). There is a certain level of competence that is expected, but at times is not applied. This negligence surely assisted with the issue, creating the attractive nuisance. This is a bit of a stretch for legal reasoning, yet still should be explored.

GENERALITIES

Commentary on Issues

Dear *2600*:

I'm a relatively new subscriber and just wanted to thank you for the commitment you expressed in the "Injustice for All" article of the most recent issue.

I didn't attend HOPE, nor am I that familiar with *2600* or its history. However, I'm a Republican who also voted for Trump and a programmer.

"Disagreeing on issues, strategy, and history are all healthy things that need to be encouraged" - this stuck out to me. For the past two years, it has felt like compromise and conversation have been thrown out the window. I've completely avoided talking politics with anyone for fear of being branded something absurd, rather than agreeing to disagree on policy.

I don't know much about the hacker culture or ethos. If it's one that espouses the sort of tolerance and genuine pursuit of truth expressed by *2600,* then it's no doubt one of the sanest left.

Cheers.

N. S. Montanaro

There's a big difference between disagreements in policy and developments that are truly harmful or hateful. We will fight the latter with every fiber of our collective being and we will engage in the former as much as possible. Dialogue is crucial, but so is standing up for your ideals and not yielding on what's truly important. It's up to all of us to decide whether all of that is still possible under a single roof.

Dear *2600*:

The new *2600* issue just arrived. I took it out of the envelope and *smelled* it. That's the smell of the printed word. Of civilization. And today it's become an anomaly.

Think about that.

John Goodmont

We'll never be insulted again when someone tells us we stink.

Dear *2600*:

Hey, I saw that my article got printed. That's super cool. It's a great issue to be in. All the articles (including mine) are very lively and informative, and I totally love this issue's traditional opening reader address about diversity and such. I've already gotten my first email from the article.

Article Writer

We hope all of this feedback and diversity leads to more articles, as well as more comments about them.

Dear *2600*:

In response to "How to Hack Your Way to a Guilt-Free, Political Ideology" (34:3), first, I'm not sure how serious this is, but after Donald Trump's election, and Nazi furries duking it out with Socialist juggalos, I'm not taking any more chances. The article reads like "A Modest Proposal" by Jonathan Swift, if not quite as well thought out, chock full of catch phrases and buzzwords. The most hilarious is the initial statement of trying to be deeper than "talking points," and then writing an essay which is nothing but a few popular buzzwords.

The first, which is somewhat depressing, is "consumer-driven ideology market." Here we reach peak liberalism and maximum hipster, where everything is for sale, nothing means anything, and you finally are your khakis.

Your next mistake is taking a cheap shot at the "handout-dependent cockamamie cuckoo liberal left." Which is funny, because you then espouse what is a standard Marxist talking point of one world government, along with your very base college radical utopiast vision enforced by this one world totalitarian government. Essentially everything wrong with "the left." Next up, you then drop environmentalism and fascism - again, two more popular talking points.

The next glaring problem is a two-tier system of haves and have-nots. Who decides who gets to be an "engineer" or who is allowed to possess technology? Consider this: before the hacker scene exploded and more or less took over, entry in engineering fields was somewhat selected. In a bureaucratic hierarchical system, the only real skill is self promotion. You'll see companies like Microsoft of the 1990s, monotonous unproductive behemoths with sub-par products that stayed afloat more from their bureaucratic prowess than their technical ability. It wasn't until GNU, Linux, and the Free Software scene came that the software world was shaken and innovation restarted. So yes, some grad school student's for-fun project eventually upsets all industry giants with a team full of enthusiasts who would have never been let into your magical spaceship. With this, a giant cultural shakeup happened as well, and it changed the perception of "what does a programmer look like?" or "what does a system engineer look like?" The old joke of the 1990s Internet was the bumbling MSCE, or odd collection of certificates who used that to speak as an authority on computers. Truth is most everyone else knew far more.

The hacker scene was a hangout for the engineers, most not looking to do work for a company or daytime society, in effect perpetual have-nots. Phone phreaks especially. You've already left most of the readership out. When you have someone deciding who gets to be an engineer, chances are in short order. Actual talent gets left behind for politically expedient choices. I'm shocked I even have to remind you about the power dynamics of the hacker/phreaker scene of the 1980s and 1990s. In *2600* of all magazines. Did no one make you read "The Hacker Manifesto?" Even today, we see the same mistakes being made where looks and bureaucratic ritual take precedence over proven abilities. Even today in the hacker scene, we see more self-promoting "startup" types trying to cash in on venture capital with little proven ability. They resemble little of the hacker of old.

Speaking of fascism, here is the giant fatal flaw in the premise of all Third Position ideologies: Dunning-Kruger. This is the illusion of untalented low-skilled people thinking they are far more skilled than they are. As in any hierarchical system, the general rule is that "self promotion is the only real skill." This ends poorly,

as the self-promoting types, especially common in today's society, will reign and actual engineering and science will again be repressed. Simply put, while a "meritocracy" sounds nice, methods of determining "merit" where power structures exist wind up being dubious. This becomes a thin justification for personal power grabs and conquest.

If your idea sounds like the plot to a dystopian science fiction thriller, it is. Cyberpunk was meant as a warning, not as a framework for future development.

Your concept of a foolproof ideology is to string together all the buzzwords and catchphrases you've seen repeated in Internet conversation as a single semi-coherent ideology. This reads just like "A Modest Proposal." I'd like to think this is a joke or parody, but in these days, parody and satire of yesteryear have become dead serious reality. As far as "leftist" ideology, please try actually reading some first or, even better, try reading any *serious* political essay instead of random buzzwords you've seen others use on the Internet or last generation's 19th century inspired satire. It might give you a better world view.

GI Jack

Dear *2600*:

In the Spring 2005 *2600*, there was a piece on the MTA subway system, specifically the MetroCard. To the point: The article stated the project was far from over. There was also a link: 2600.com/mta. The URL isn't working. I was hoping there was some sort of follow-up or updated link? Thanks.

Daniel

While we try not to let anything fall into obscurity, there's only so much we can do and this was a project a particular writer was following up on. They apparently stopped working on it. If it's any consolation, the MetroCard system is being phased out over the next few years. We'll undoubtedly have an article on the new contactless card system they're now starting to introduce. Let's hope we're able to keep adding updates on that for more than a decade into the future.

Dear *2600*:

What building is on the Autumn 2001 *2600 Magazine?* I bought that issue but I threw it out, so I thought I would email someone at *2600 Magazine* to ask.

Stephen

You came to the right place (although we're not sure why your throwing out this issue somehow makes you more curious as to what was on the cover). Full explanations of all of our covers appear in our Hacker Digest compilations. This one is explained as follows: "The old New York Telephone (now Verizon) building in Manhattan was given a black color and blown up in size, giving it the appearance of a huge monolith. The writing down the side of the building was a very loose Japanese translation of a famous phrase making the rounds: 'All Your Base Are Belong To Us,' which itself came from a bad translation of the Zero Wing video game."

Meeting Fun

Dear *2600*:

I have started a *2600* meeting in Tallahassee, Florida. I have a handful of regular attendees and am getting more coming in.

Kevin

Sounds like you're doing everything right. Please keep us informed as your meetings continue. Good luck!

Dear *2600*:

Not sure how this keeps happening, but every so often things get confused. (Okay, last time with Plano, it was a pure lack of recon and everyone's insistence of lumping Plano into Dallas, but I digress.)

Just noticed that the Dallas *2600* is again listed at another location. The actual Dallas *2600* meeting is still at The Wild Turkey. It has a regular and active group on the patio by the front door - same spot for the last 15 or more years.

I know you all just post what you are told and greatly appreciate your work. Just wish others would exercise a little due diligence before starting a new meeting.

isac

The reason this has happened a couple of times is because people are reporting your meetings as being moved to another location and nobody has been posting updates to say otherwise. This is why it's so important to keep sending us updates and/or maintain a web page or Twitter presence so we know you're still out there. We've reinstated the info as it was before.

Dear *2600*:

From what I can tell, the meeting at State College, Pennsylvania is dead. No one showed for the past two. I'd like to start it back up again. For the Spring issue, can we change the location to the Big Bowl Noodle House? Thanks!

Josh

We'll do even better and change this for the Winter issue, provided you don't have to get a big bowl of noodles to attend the meeting. Since we haven't heard from others at this meeting, we'll make this modification with the understanding that it will be delisted entirely if we don't get any updates. Good luck.

Dear *2600*:

After being more than a year looking for a comfortable venue for having meetings, we finally can confirm that in Paraná, Entre Ríos, Argentina, there's a *2600* meeting.

We've been having regular meetings since August of 2017, but the bar where we started meetings closed its doors. Meetings have been taking place in our current venue since April 2018, and we have at least one new member per meeting. Our meetings used to be only three or four people, but for the last four meetings, we were up to nine (and it's not summer!).

Chin0x00

Great to hear. Congrats on the new meeting and let us know how it goes. (It's listed as of this issue.)

Dear *2600*:

Thank you for listing the Portugal *2600* meeting! It was great to see it there and I believe it will help to get traction around here and meet fellow hackers.

All the best!

billk3ls0

It's always more of a challenge for overseas meetings as difficulty in obtaining the magazine leads to less people being aware they even exist. In places where the magazine can be easily found, we've seen great success with meeting attendance. Unfortunately, there don't appear to be any good distributors for us overseas. We've been looking and they either wind up costing us money or they never bother to get back to us. This didn't used to be such a problem.

Dear *2600*:

I've decided to hold a *2600* meeting even if I am the only person in my town to attend.

John

Well, that's the spirit, but please don't let that be a foregone conclusion. Even if you are the only attendee for one or a few meetings, there's no reason it has to stay that way. Get the word out, find other groups that may have members who would be into one of our gatherings, and communicate with people, both locally and long distance, so you have as much support as you can stand. Above all, don't be discouraged - this is a positive thing you're doing.

Dear *2600*:

I keep missing the meeting in Melbourne, Florida because something else always comes up. I promise I'll try my hardest to go to the next one! Keep it at 5:30 pm since I don't get off work until 5 and that gives me enough time to get there!

Joshua

We'll do our best.

Dear *2600*:

Is Fort Collins, Colorado still an active meeting? What is the Twitter name?

Allen

Last we checked, it was. And last we heard, their Twitter handle was @noco2600.

Dear *2600*:

We had 12 people at the Davenport, Iowa meeting. We turned some robots loose in the lobby and let the wider Internet control them.

Ben

This is probably not the sort of thing you could pull off in the lobby of a food court without some sort of consequence, so this is an advantage to having your meetings in a hackerspace, something we normally discourage. One day, unleashing robots in public will hopefully be a lot more normal.

Dear *2600*:

I'm hoping it's possible to update the meeting listing page. Under Chico, California, we've moved the meetings to 7 pm at the Idea Fab Lab. Starbucks doesn't have enough room for more than four people at a time.

Thanks in advance!

Brian

How on earth did you ever hope to have meetings at a place with room for only four people? There are bathrooms bigger than that! We have made the change and not a moment too soon.

Dear *2600*:

A new coffeehouse has opened up two doors down from the bar where we currently meet in Titusville, Florida for the monthly First Friday meetings. In the spirit of making the meeting site more accessible to the youth that might read *2600* and be too young to visit a bar, I'm making the move to the Crescent Coffee Company on the first Friday of each month. Please update the website as soon as you can. I'll tape a copy of a *2600* cover on the window for the next couple of months to catch the people still going to the Playalinda Brewing Company down the street, but updating the website makes the move official while waiting for it to make it into the magazine.

Cheshire Catalyst

Consider it done. (And having a cover prominently displayed near a meeting is a great idea.)

News of the World

Dear *2600*:

The approval by a federal judge to allow AT&T to go forward with the planned purchase of the Time Warner corporation (and future telecommunication company mergers) is bad for consumers. Telecommunication mergers drastically raise costs to consumers for various services such as telephone, Internet, and cable. Many consumers in recent years have been cutting the last service mentioned (cable) for the very reason that costs have risen to a point of being considered ridiculous. The other reason that telecommunication mergers are bad for consumers is that they greatly reduce innovations which might have otherwise taken place. Telecommunication company mergers which create monopolies, like any other industry, only create less choice, higher prices for consumers, and in the end, only help shareholders, the board of directors, and the overall bottom line.

Bill

There is nothing new here - the alarms have been sounding over this for decades. What's different lately is the sheer magnitude of these mergers and takeovers. There is very little room for any entity that isn't already a giant. For those who believe that the market can be trusted to regulate itself, this is the end result. And it's pretty obvious that it isn't healthy for consumers or innovators.

Dear *2600*:

The new NIST password standards are great in theory, but now it's a matter of cracking the standard instead of cracking passwords. "correct horse battery staple" is a great password because of its sheer length. The problem is standardizing four words. What had been a password 25 characters long can be reduced to essentially four characters: "correct", "horse", "battery", and "staple". Sure, there's 171,000 words listed in the Oxford, but huge swaths of those words simply are not appropriate for an easy-to-remember password. Users will not look up how to spell words to make a password.

Go find a wordlist of the top 20,000 English words by usage. Odds are all four words of the password will be in that list. Hashcat combinator the wordlist against itself to create a new wordlist with every possible combination between the two. Use that new wordlist as both left- and right- sides in a dictionary attack. My machine is not optimized for cracking, but any password made from words in the top 20,000 list will fall in roughly 2.5 years. If we shorten the wordlist by eliminating all the 1- to 4- character words, that time drops to a little over 300 days. Even something like "evolution scattered insufficient geographically" makes for a 45-character password - what we would normally think of as insanely long but secure - but that would fall to the same wordlist in just over 300 days.

If you have some high-value hashes, set up a few cryptominers to crack the same hash, each with just a portion of the wordlist, maybe rent a few on AWS, and these super-safe long passwords will fall in no time at all. The problem is we can reduce these passwords to four elements and not have to brute force the whole thing. This little bit of security also relies on people choosing four random words. Humans don't do random very well. Please use multiple symbol sets. Add in a capital letter somewhere, or a number somewhere, or a ! somewhere - even if it's just one ! in the middle of a word. That ! means we can no longer reduce the pass-

word to four elements and instead have to brute force the whole damn thing, which just ain't happening with the computers out there now.

ghostinthemachine

This is fascinating and scary at the same time. We'd love to hear more creative ideas on how to make more secure passwords. And how to crack them.

Scams

Dear *2600*:

Are you interested in knowing about a rampant scam being conducted against sellers on an iconic online auction site?

Ph@nt0m1776

Is this a part of it? We become suspicious when people ask such obvious questions. We've been discussing "rampant scams" since 1984 and there's little reason to believe we would have lost interest since then. So please either pull us into the conspiracy or tell us the whole story.

Dear *2600*:

Hi there, I'm selling cloned credit cards with PIN code; ready for carding and using at ATM the cards are mostly VISA and MasterCard they work worldwide. Cards are discreetly mailed worldwide using priority mail. We are the only trusted spammers. We accept: Bitcoin, Ethereum, Bank Deposit and Litecoin. One card with $2000 guaranteed and up to $3000 - price $20. [...] One card with $6000 guaranteed and up to $7000 - price $40. All our goods are 100% Verified. I will give a great deal on orders of more than one card.

Peresuodei

Wow. "The only trusted spammers." That just says so much about the kind of people you are. What is it about us that made you think even for an instant that this kind of blatant theft was something we'd be interested in? Clearly, you know nothing of the hacker world and simply assume that hackers are criminals like you. Sure, you'll find people in our community who will be tempted, just as you will in any community. You prey on greed, fear, poverty, and human weakness. And you give digital currency a bad name. Our only comfort is that this kind of idiocy never lasts long, at least on an individual level. There's certainly no shortage of new idiots who jump on the bandwagon. We trust our readers will exercise common sense and avoid these types of people like the plague. In fact, give the plague a second chance before believing anything they say.

Dear *2600*:

Is it illegal to ask for cards? I'm broke and my shoes are kinda getting worn. So I asked a few people if they can score cards. I never got any but now I'm worried about going to prison and ruining my life and going to life in prison due to the three strikes rule for just asking for them.

Josh

We ask for things all the time that never come. And it would probably be more trouble than it's worth if they did. So don't stay up nights worrying about stuff you never did. Instead, consider yourself lucky that it didn't pan out. Because otherwise you'd be keeping company with the type of person above, either in or out of jail and going nowhere fast either way. And don't kid yourself - the temptation will come again. Everyone experiences it at some point. Hard as it may be, you have to avoid outright crime like this, even though it may seem like a sure thing that you'll never get caught for. That luck usually runs out fairly quickly, and it's actually worse if it doesn't since you then become someone who lives a dishonest life, something that will seep into every relationship you have. So whenever you get the chance, as it appears you have here, turn around and move in a different direction. While you may think the path is predictable and not worth the trouble, you'd be amazed at how often unexpected developments occur. And those are the real opportunities for change.

Dear *2600*:

Hi from greece I want to buy skimmer can you tell me please someone site to trust it thanx

ektorastheodoratos

So 1990s. Don't you know all the cool criminals are now using shimmers?

Inquiries

Dear *2600*:

Hey I saw a post about submitting an article about hacking. What kind of hacking are you interested in? Is iCloud hacking sufficient for a story?

Hello Friend

You can pretty much put any noun in front of the word "hacking" and it would likely be something we were interested in. So please write the article! You'd be amazed at how many inquiries we get about writing articles that never result in actual articles. It's our leading cause of depression, in fact.

Dear *2600*:

Just wondering what is up with the QR code on the main page of the site. It says that the QR code campaign has been disabled for some reason.

Clinton

You're referring to the QR page that greeted visitors to our website for a couple of months and which also appeared in the Autumn 2018 cover. The code took people to a voter registration site so they could register to vote or see their status. We fell into a little trap with a company that claimed to provide free QR codes and then somehow thought it was fair to ask for a monthly fee. We disagreed and it's now fixed.

Dear *2600*:

Did you receive my previous email?

Garrett

Yes, and it was even lamer than this one. At least your writing style is improving.

Dear *2600*:

I am 57 years old and I would love to learn how to program.

My background: I started in computers in 1987 with the IBM XT/AT as a word processor. In 1994, I got certified in Novell. In 1998, I was certified in Solaris as an admin and then engineer, and also as a Cisco CCNA. Then I lost my job when the World Trade Centers were attacked. I was a block away on Broadway heading to Sun Microsystems on the 25th floor of Two World Trade Center when the building collapsed and I was caught, smothered in the cloud of dust and debris. A year later, I got my real estate license and worked until 2009 when I was diagnosed with multiple sclerosis.

Since then, I have died, have been in a coma, had a seizure, had a few hematomas that required emergency blood transfusions before I bled to death internally, have had multiple blood clots, and now I am being tested for adenoma cancer.

I would like to know what computer/OS I should buy to learn how to program. Back in my day, C was the language to know to program, so I need to know what language or languages are the need-to-know languages to learn how to program a good back end website. (I knew how to build front end HTML websites back then.)

I actually talked with Dennis Ritchie at Bell Labs. As you know, he and Ken Thompson created Unix, then Dennis created C and ported Unix into C. So if you can help me in any way, I would appreciate it. I actually had a comment printed in one of your editions back in the late 1990s. So that's why I am asking for your help now. Can you teach an old dog new tricks?

Oh, I almost forgot. There was this website I used to go to that listed all the passwords for any application, any version, that you needed. I believe it ended in *.kz, but I'm sure there are many more. So if you can refer me to a safe site to get passwords for MS Word, McAfee, ZoneAlarm, etc., I would appreciate that as well.

I am finally going to build the website I started in the 1990s. It was going to be an Amazon-type website before Amazon, but better. I built the entire thing, but it was all click on this to get to the next area because I didn't know how to program the back end of a drop-down menu.

I am sorry for the long letter, but I figured I should give you the entire background of why I need to learn this before I die. It's the hardest thing to do on my bucket list.

Henry

First off, our sympathy for the rough road you've been down. You deserve a lot of credit for continuing to get back up and move forward when others might have given up. What you're displaying is a true hacker spirit.

We can only recommend paths to explore - there are no surefire answers or guarantees. But we can say that the entire process of learning (and by extension teaching others) is extremely rewarding in itself. As long as you're an active part of that environment, you're most certainly not wasting your time.

Languages like PHP, Ruby, and Python are great to know when programming the back end of a site. Each has their own advantages and disadvantages. We suggest looking into each of them and deciding which one to pursue. Stick with your choice and see where it takes you. Patience is a real virtue here.

The odds of putting together something like Amazon are slim to none, so don't be surprised if that doesn't pan out. Focus on refining skills and you will find yourself in demand on projects you've never heard of before.

The .kz file you remember was a KuaiZip file. You can certainly find passwords for software, but that carries its own set of risks like malware, viruses, and even prosecution if you're really not careful. It's understandable with the high entry price to many pieces of software, but it should really only be a last resort. There are often other options, like substantial student discounts or free versions without bells and whistles that you can get along without.

We hope to hear some progress reports.

Dear *2600*:

I'm just wondering what the average file size for the MP4 videos from The Circle of HOPE is. Would you please let me know what I should expect with the USB stick. The storage solution I am using only lets me keep around two gigs in my space (per file). So, thanks for your time and help in finding this info out.

M

It's hard to imagine in these days what kind of an environment you're in where file sizes are limited like this. Most of the MP4 files found on our two Circle of HOPE USB drives are under two gigs, but there are a few exceptions, with one even exceeding six gigs. While we recommend copying files from the USB drives to somewhere more permanent, they should be perfectly fine residing there until you find a better place to keep them.

Dear *2600*:

I help run a funeral home and we're experiencing a sharp increase in people requesting coffins wired with Wi-Fi (about ten or so this calendar year). Is this possible and, if so, what equipment should we use?

John

Just when we thought we heard it all.... So, if it's the person planning to be buried who's making the request for Wi-Fi, you probably don't have to worry much about them complaining if it doesn't meet their standards. Of course, if you're six feet underground and inside a box, you really can't expect much in the way of reception in the first place. A wired connection would make a whole lot more sense, which at this stage is still pretty solidly zero. If, in fact, these requests are being made on behalf of people planning to stay above ground, you could be dealing with something a bit more nefarious, such as a desire on their part to keep checking to make sure the coffin isn't vacated, which only opens up a whole lot of other questions.

If this is indeed a thing, there must be some readers out there who are making these requests. To them we ask: what in the world are you thinking?

Dear *2600*:

I was wondering who answers the letters printed in the magazine. Is it Emmanuel or a staffer?

Maya

It really depends on who's around or in a mood on a particular day. Answering letters is one of our true joys and it's really what keeps us moving forward. That's why we always want to see more. Comment on our covers, our articles, or even other letters. Tell us a story. Insult us. Ask questions. This is the one true hacker forum that will become a permanent record of our unique community. Amazingly, letters from our back issues, whether on paper or through our electronic Hacker Digest series, still manage to fascinate readers, even years or decades later. Our address is letters@2600.com.

Concerns

Dear *2600*:

I received an email saying that my email address was hacked, including my password, and they said they have my social media account info and they have been tracking me for months and are watching me through my webcam. Is this a fake email or should I be worried?

Pritam

These emails have been circulating for some time now. The short answer is not to worry about them. But there are some elements that are cause for concern. Here are some questions:

Why are you worried about your webcam? Assume it's always on and cover it with something so you're not constantly being spied upon. It's unlikely, but certainly possible.

Was one of your passwords displayed in this email? This is only a concern if you're still using that password or (worse) if you use the same password for everything. Then you may indeed have problems, but those problems predate this email. Never use the same password in more than one place if you care about those accounts. All it takes is one compromise from one company and you could be victimized due to their poor security. The Yahoo disaster alone exposed literally billions of passwords to the world. So people naturally freaked out when they received an email with their password on that system proudly displayed.

Are you keeping a huge amount of private info stored on your social media accounts that you don't want the rest of the world to know about? Well, guess what? The rest of the world is going to get access at some point, whether it's through a technique like the one above, a compromise of your social media provider, or a change in terms that you somehow missed. None of that includes your own possible mistakes. So don't give out any info that you don't absolutely have to give out. And you're not obligated to give out only truthful information. Go have fun with that.

So yes, don't worry about the email, but don't set yourself up to become the victim of something like this in the future. It's easy to take your security seriously. Nobody else will.

Dear *2600*:

I have not been able to find any *Off The Hook* programs on the 2600.com website for download in quite a few weeks?

Parrott

If you're asking us, then yes, you weren't able to find any programs in the period you inquired about. That was because we were preempted for three weeks in a row. We probably should have said something in retrospect, as quite a number of people expressed concern for our whereabouts.

Dear *2600*:

I'm trying to get information on something. I posted this around and haven't gotten any help. Can you refer this question to someone there?

I did a traceroute, and several of the nodes my traffic goes through are registered to the DISA, the Defense Information Systems Agency.

DISA? The DoD? What the f*uck is going on? Damn....

I haven't done anything wrong that I know of. Anyone have an idea?

The IP is 7.0.80.71.

Robert

We'd need to know more about this before reaching any definitive conclusions. It's entirely possible this is a non-routable IP being used behind a firewall of a provider. Some years ago, Rogers Communications in Canada was found to be doing this in place of 10.x.x.x IPs. If it was among the first hops, then it's likely a similar scenario. If this IP appears in the middle of a traceroute, though, that would be a lot more interesting and suspicious. Perhaps our readers have more experiences to share.

References and Developments

Dear *2600*:

Just wanted to let everyone know about a podcast from *Left Right & Center* out of KCRW. It's *All the President's Lawyers* and covers the legal mess that the presidency is experiencing. Ken White (@popehat on Twitter) is the lawyer answering questions, and I find it as stimulating as his other podcast (*Make No Law* which covers First Amendment issues). A big thanks to Marc Ronell's article on Reality Winner in the Autumn 2018 issue for causing me to think of this while reading my issue.

E85

We're happy to pass along this and other references/inspirations, including the one below:

Dear *2600*:

Something I'm super excited about announcing. Recently at Derbycon, we had the first Mental Health and Wellness Village to support hackers that are struggling or have friends or family who are. We learned about a whole barrage of brain hacking techniques and provided a nice quiet space to get away from the noise and crowds. Since then, it has kind of snowballed into what will soon be a 501c3 called Mental Health Hackers, Inc. We'll be looking for volunteers, charitable donations, speakers, teachers, etc. for future villages at other conferences. If you are interested in any other information, feel free to DM @hackershealth on Twitter.

Amanda

Endangered Privacy

Dear *2600*:

Did you know that Google Docs will read your private files and lock you out if it triggers the automatic ToS? If you receive too many of these violations, your entire account can be disabled, even if the files were never shared.

Brando

What surprises us is that people actually believed their files were secure and private on a cloud service like this. While many will say that it's a good thing if people uploading child pornography or terrorist material are found out in this manner, the fact that may not be so apparent is that this kind of surveillance becomes normalized with these actions. While today the authorities may be going after the people you think they should be going after, tomorrow it could be people who uploaded plans for a demonstration or who are members of a particular political organization, or literally anything else. In some parts of the world, this type of surveillance is the norm and introducing technology that makes it even easier is about the worst thing we can do.

Dear *2600*:

Everyone knows that it's not a matter of *if* your private information will be breached. It's a matter of *when*. I don't have much of an expectation of privacy these days. A search in the Amazon application on my iPhone means that I'll start seeing Facebook ads for that item. Google maintains a timeline of my visits to various locations. Video cameras are everywhere.

JM

Let's not be so fatalistic. You actually do have control over your privacy; it just often requires putting in a bit of effort. Be aware of who you are giving your private info to and ask yourself if it's necessary every time, despite what you may be told. There is no reason

on earth that Facebook, Twitter, Google or anyone has to have your actual info. It's not a crime to lie to them and it'll help protect you a great deal if you do. Use a fake name. Don't give out your actual birthday to anyone you don't personally know. Keep your address to yourself. And don't associate accounts with each other. It may make things a whole lot more convenient to play by their rules, but you can adjust and benefit from not having your entire life traded from one site to another. Use ad blockers so you're not a captive audience. Don't be logged onto Google when searching on their site. There are a million other things you can do, but if you start with these, you're ahead of nearly everyone else insofar as protecting your privacy.

And yes, video cameras are everywhere.

Dear *2600*:

Google Chrome's new semi-mandatory SSL is annoying. I am a web developer for a band and all the site does is give you dates, press kits, and other information that doesn't have to be secured. Now, when a normie visits the site and it says "not secure," they think they're visiting an infected site. Now I have to install SSL on a site that doesn't even take payment info or login sessions at all.

Josh H.

We hear what you're saying, but thanks to the "Let's Encrypt" project from the Electronic Frontier Foundation and the Internet Security Research Group, it's now possible to have this working quickly and easily without costing you anything. (More info is at letsencrypt.org.) Previously, it was a bit of an ordeal and a huge ripoff. It's definitely important to protect browsing data even when it's not about payments or personal info. We do agree that Google has this nasty habit of imposing their security values on you when they determine it's important and completely ignoring your concerns when the situation is reversed.

Dear *2600*:

Google is now labeling some business websites as "possibly hacked," and the only way you can remove this message from your site is to, of course, register for a Google service. I'm guessing best case scenario this message is accurate and is simply broadcasting what websites are vulnerable?

Jesse

The actual message is "This site may be hacked" and it's enough to get everyone to not want to visit your site. The only way to remove it is to sign up for Google Search Console, which allows you to address the issues that make the dreaded message appear. The service is useful, but forcing people into it in this manner just doesn't seem right.

Confusion

Dear *2600*:

Could you remind me the name of your magazine? I think I know which submission you accepted. Also, can you tell me where I can find an issue? Or can you mail me one when my article is printed?

Unidentified

Every now and then, someone sends us an article and is extremely surprised when we accept it. We can understand losing track of what article they sent in the first place. But the email we send comes from the magazine, so it's hard to figure out how they would need help with our name. (Incidentally, authors will get copies of the magazine if they choose a subscription for their article.)

Dear *2600*:

You accepted my submission a little while ago. I was told it would likely be in the Autumn issue. It's not in there. Where is it? Is it still even going to be in an issue? I am very confused and would like clarification on this. I would really appreciate if someone could get back to me on this and help me understand what's going on. Thanks for all your help.

Unidentified Still

First off, we very rarely make that sort of commitment. Second, unless you can see the future, there's no way you could have known if it was in the Autumn issue or not as you wrote this while the Summer issue was still out.

Dear *2600*:

Never mind. I see the issue I just got was the Summer issue, not the Autumn one. I thought the last one was the Summer one. My bad.

Unidentified Yet Again

It's OK, but please be content that your article will be appearing like we said it would. In fact, it may have already appeared since we don't even know who you are.

Injustices Galore

Dear *2600*:

What is it with Facebook refusing to accept notification that their site is showing video of a man sexually assaulting women? I get a video of a man on an up escalator who is reaching across to the down escalator and stroking people's arms in a sexually suggestive way. It is presented as a joke, but it is behavior that would have you arrested and charged in many parts of the world. So I naturally tried to report the video, but Facebook makes that impossible to do. You can hide the video but that does not cause it to be reported. You can block the sender which gives a report option, but you can only report an assault on yourself or a friend. This isn't an accident. It is a deliberate policy on the part of Facebook to reduce the number of reports they are required to deal with by making it impossible to make a report. Yes, I get it, some people think sexual assault is a laughing matter. Mr. Donald Trump, for example. Yes, being anti-sexual assault makes me a "snowflake." Well, here is my hack for dealing with Facebook's reaction. I drew up a very carefully worded explanation of the situation and sent it to my friend Jerrold Nadler, who will shortly be chairing a House committee that will be calling Mr. Zuckerberg to answer a large number of questions about the way his business operates. It isn't the most serious question, of course, but it is one that every journalist knows they can explain to their audience.

Phill

Dear *2600*:

In 2015, I was wrongfully convicted of a crime I did not commit. The law firm of Locke Lord was hacked by a Chinese hacking group called "Comment Group," associated with PLA in China. I have been trying to expose the cover-up but they're trying to silence me. Is there an attorney or organization that can help? I need to bring all the facts I have into the light. There is already a lawsuit against Assistant U.S. Attorney Paul Yanowitch (see Laoutaris v Yanowitch). Your input would be appreciated.

Anastasio Laoutaris

It does sound like an interesting case. We have a number of lawyers who advertise in the 2600 Marketplace who might take an interest. We have many more who read the magazine. You can also place a free ad and give out your specific details. Between all that, we should be able to help make some progress.

Dear *2600*:

My husband is an activist being prosecuted by the same U.S. attorney's office that Aaron Swartz was. My husband was actively standing up for a girl being abused by a Harvard-affiliated hospital. Prosecutors claim he is Anonymous. More to the story here. Would love to talk if you're interested.

FreeMartyG

The level of our interest unfortunately doesn't always correlate to how much we can actually do. We certainly encourage you to make sure your story is told - and the best way to do that is to actually tell people the facts. Avoid long conspiracy theories and rants that will make people look for excuses to get away. If the story is engaging, it will spark interest in the people who hear even the most basic details. There are lots and lots of stories out there, so it's vital that the one you're telling is something people want to hear more about.

Dear *2600*:

I wanted to point something out that deals with the U.S. Army, Cyber Command, Beyonce, and the Vigenère cipher.

On the web page www.recruitahacker.net/puzzle, the U.S. Army (per the TV advertisement showing the above URL) asks the reader to decrypt a message. According to various people on the Internet, the decrypted text translated to "Beyonce has a big ass". An alternative key was found that translated to "Arcyber has a big gun".

One can only wonder: Is this the official opinion of the U.S. Army? Given they are paying for both television advertisements and a website, well, you make the choice.

Maybe someone in the Army thinks guys will like the decrypted text, but can't there be *female* cyber warriors, too? Can't there be female cryptoanalysts? Maybe the Army only wants people who feel it is OK to say what the above text says?

I know President Trump has issues with women (according to the videotape shown during the campaign). Should the U.S. Army be saying this about any woman, especially a public figure?

The page says to prove what it takes to be a cyber warrior. Solving this puzzle wouldn't make me feel like a warrior given what was found. Sorry!

Bertram

We quite agree. Though it's always interesting to play with cyphers of various sorts, it's sad to see ignorance and sexism finding its way through such things. We must fight it whether encrypted or in cleartext. (As of press time, this page has become unreachable.)

More Circle of HOPE Feedback

(Note: Here are some more letters that were sent as feedback for The Circle of HOPE and, as is now traditional, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600:*

I was fortunate enough to attend The Circle of HOPE, so first of all, thank you for an amazing event. Having grown up in Scotland, somewhat isolated from like-minded folks, it was a very interesting experience to see the culture that exists in the U.S.A. (It was many years before I could afford a modem, which was long after my computer was a C64 with a lowly Datasette, so I operated somewhat in isolation.) I regret not taking part in the workshops, which would have been great for interacting directly with the hacking culture.

I was disturbed by the reports of intimidation that were going on. Visiting the U.S.A. from the U.K. has always been strange, as any foreign country should be due to different cultural practices, norms, etc. I have always found the American people I've interacted with to be generally very friendly and kind. However, with the current Trump regime, there has been a change in tone. The Fox news broadcasts in the hotel were disturbing, having the tone of a dictatorship's mouthpiece - "Trump declares...." Kudos to the person who put googly eyes on one of the lift's screens.

The tone of the conference was very good - welcome all, set some ground rules, and expect that people are generally good to one another. It is shameful that that was abused, and I hope with the discussions that follow that measures can be put in place - you have the right people to speak with. I was sorely disappointed with Steve Rambam's announcement that he wasn't going to be attending HOPE in the future. My impression is that he is a good man with an allegiance to the office of the president I find baffling while it is occupied by an utterly corrupt and probably treasonous boor.

I would love to attend HOPE in 2020. If the U.S.A. isn't split asunder by then, I sincerely hope instead there will be some reconciliation in mainstream politics. Tone is very important, and it is set by those at the top.

Wishing you all the best.

The Circle of HOPE Writer #13

P.S. The demoscene session was great!

Dear *2600:*

This year's HOPE was my first one, and in fact the first time I've attended any sort of hacker conference. I was very happy to attend, and it was very significant for me. Given the storm surrounding the event, I wanted to share my experience.

I found out about the "alt-right trolls" both by seeing/hearing them and by reading the Twitter threads. I expected that these people would come and knew that dealing with them was gonna be hard. I understand and agree that a lot of this was blown out of proportion and I am grateful that you guys addressed it, both in the closing ceremony (however small it was) and on the *Off The Hook* radio show. What *did* worry me, however, and made me consider not coming back on Sunday, was Steve Rambam's talk. I was very interested in the talk's subject, and sadly did not perform proper research on who he was. I found both his opening and closing statements extremely unprofessional and, in the case of the last one, uncalled for and even distressing. I understand that he is not coming back to the conference and that's that. But, as a first timer at the conference, the words of a speaker with such a long segment combined with the presence of alt-right trolls and all the finger-pointing at the staff made me think twice about whether I wanted to be there at all. As I told one friend at the conference,

not only was what he said irrelevant and uncalled for, but also I did not attend a conference to hear someone tell me which presidential candidate is good or bad, or to tell me their political agenda. *Yes,* it is true that there is no way to be apolitical, and I couldn't agree more, but there is a difference between having your own opinions and forcing your opinions on other people. He even got booed for it! And, of course, then told people to shut up. This is what made me the most uncomfortable, beyond the MAGA hats and all that. It was notorious, from what I saw myself at the talk, that the MAGA people and other assorted associated trolls were rooting for him.

Nevertheless, this conference was a wake-up call for me. I don't remember how or why I got started in cybersecurity/hacking, and I had forgotten all about it until I came to the conference. When I was a kid (around 12ish), I wiped my laptop, installed Linux, and started using Tor. I honestly don't remember why I did all that, but it all came back to me that weekend: all I used to think and why I thought it, what things I would do to protect myself and avoid being tracked (even if I was not being tracked), etc.

I come from what is commonly known as a "third world country." I am not used to having a voice, to be face-to-face with leading figures and projects, to be involved and have a say in what and how things go. Being in the same room as all these people, ideologies, and projects is something I would have never have even dreamed of. Hell, I remember reading about *2600* and thinking "wow, that is so cool, too bad I will probably never be able to read their stuff' and here I am, attending a conference organized by them. As years have gone by and I've had to deal with "adult problems," I had left this all behind and again, I didn't remember any of this until that weekend. Saying this was a trip down memory lane is an understatement.

So thank you. Thank you for doing this conference, for creating an environment where everyone can see eye to eye, however experienced or inexperienced they might be, for allowing everyone to have a voice. I know you said on *Off The Hook* to share our experiences because of all the drama that went around. But honestly, for me that is but a small stain on what this conference meant for me personally. I know now where I am and where I want to go, after remembering all I used to do and seeing so much in front of me.

I am glad to have attended, and I hope to return someday.

The Circle of HOPE Writer #14

Thanks for the kind and inspirational words. And while it may be disturbing to be confronted with a different political view, the question you have to ask yourself is if it's stifling other forms of expression or actually inspiring them. What we're getting from most of the feedback so far is that our community is open to being challenged and quite ready to defend the positions we believe in. When that exchange of ideas isn't there, whether through intimidation or because we choose to not permit it, we've lost something that we really need to hold onto.

Dear *2600:*

I'm not sure who chose to omit the HOPE code of conduct (and instructions for reporting violations) from the printed program guide, but maybe that had something to do with only one phone call to the hotline published on the website and the small number of webform submissions during the conference.

Thoughts?

The Circle of HOPE Writer #15

This is just flat out not true and an example of how mistruths are spread. The code of conduct was printed quite prominently in our program along with the means of communicating any violations. Signs were also posted, but we don't believe enough of them were, nor was there adequate oversight as to whether any had disappeared. Most importantly, we didn't have a clear method of reporting problems on the spot in each of our spaces, which resulted in incidents being reported to people who had no idea how to handle them, leading to all sorts of miscommunication. That is where we need to focus our attention in the future.

Dear *2600:*

I had a great time at HOPE this year. The expanded space really helped with the crowd! I do wonder if you could get the stairs unlocked from the lobby or mezzanine so we can reduce traffic on the elevator? I think enough people would be willing and able to take the stairs to significantly reduce the congestion.

One of the reasons I attend HOPE is to hear from those with different experiences and have my world view challenged. There seems to be a vocal group of authoritarians who want HOPE to be an ideologically safe space, free from those they disagree with. I'm all for HOPE being free from harassment and hate. I think you did a reasonable job drawing the line between harassment and unpopular viewpoints.

I experienced a small number of attendees who were disrupting Rambam's talk and booing those asking on-topic questions at "Online Monitoring of the Alt-Right" and other talks. It seems there was a notable increase in disrespectful behavior this year, and I'm saddened that activists on both sides are taking advantage of the situation to make the conference uncomfortable for others.

I'd really like to hear how others think it went. Hopefully you will publish some of the feedback in the next issue of *2600*. Thanks for putting this together, can't wait until 2020!

The Circle of HOPE Writer #16

We appreciate the support and intend to continue to have an event open to dialogue from all different quarters, obviously excluding overtly fascist and hate-filled sources. But having our views challenged on a variety of topics is what hacking is all about. We're not going to give that up.

Dear *2600:*

First of all, thanks for another great conf. You do a fabulous job!

This has been my third HOPE and I've had the same thought about cue lights since the first one. Cue lights come on in view of the speaker and let them know they are running out of time. By making them also visible to the audience, they also set the audience's expectations, involve them, and help to bring a talk to an orderly end.

I saw that you were using nice big easy-to-read clocks to help the speakers and I thought that was a great idea. A clock, though, needs some concentration to read, whereas some cue lights are instant and obvious. I was thinking that we could modify the existing clocks by adding three green and one red large LEDs to the top. I was thinking they could go something like this:

xx:45:00 First Green LED comes on

xx:47:00 Second Green LED comes on as well

xx:49:00 Third Green LED comes on as well

xx:50:00 All three Green LEDs go off and Red LED comes on

xx:51:00 Red LED goes off

I'm thinking we could hook into the seven-segment LED displays and decode them using some old-fashioned 74xx chips. This would free up a volunteer, as hopefully you'll be able to ditch the low-tech holding up a card which does seem a little incongruous at a hi-tech conf.

We could, of course, get much more sophisticated. Use a Pi or Arduino, allow them to be remotely set, sync time using NTP and so on. This might make them a CTF target!

My inclination is to try a lowest possible tech solution to begin with and perhaps have a second project to make a more sophisticated one.

Interested to hear what you think.

The Circle of HOPE Writer #17

We think this is great and will be in touch before the next conference to hopefully plan more specifics. This is exactly the kind of project we like to see. This year we definitely had a big improvement with speakers not running over, as well as our nifty on-screen displays that showed where talks were and how much time remained. Tiny steps, but significant ones.

Dear *2600:*

If you videotaped Steven Rambam's last talk at the HOPE conference (and I was very sorry to learn that it will be his last), I'd be very much interested in buying the DVD. Could you please let me know how and where to purchase it? Thanks a lot.

The Circle of HOPE Writer #18

All of that info should be prominently displayed on our websites (although sometimes we actually forget to publicize our own projects). We've got all of the talks available on two flash drives or individual DVDs that have some great menus and intro music. You can also download them from store.2600.com in full HD format.

Dear *2600:*

I was there and I was witness to the MAGA hat incident. I don't think the events of fascists infiltrating groups (of any kind) is new. But just because some fascists infiltrated a group does not mean that the group is at fault or complicit in fascism. It means that the fascists are one step ahead. I think anyone with a grain of moral fiber understands this. Yes, it is frustrating that fascists gained an upper hand. But we are a creative group of hackers that can and will do something about this. We can solve this problem and many others.

I refuse to use the word provocateurs for these people. Even if they are professionals and paid to do this while not directly being fascists, they are complicit in fascism. So, to me, they are fascists.

By the way, I knew of the one incident but was unaware of the others. I enjoyed the conference very much. All I can say is keep HOPE going - there is a lot of support for it and many of us will help protect HOPE from fascists.

The Circle of HOPE Writer #19

Thanks for the support and perspective. It's healthy to think of this challenge as one of many that hackers have met and conquered. We can route around this.

Dear *2600:*

Just wanted to write in to share my experience with this year's HOPE, it also being not only my first HOPE conference, but first hacker conference in general.

I'd like to thank all of you at *2600* for making this year's HOPE happen. I came down from Toronto and not only had a great time, but made quite a few new friends from around the globe. I dropped by Thursday to help set up and, even in that short time, I met people from as far away as Melbourne and was engaged in conversations only possible through your efforts in gathering like-minded minds under the same roof. So thank you all!

I'll touch on the MAGA subject since I did experience it firsthand, but overall I had a great time at HOPE this year. From registration to moving around, I don't have any other conference experience to compare it to, but it was pretty smooth going and since you mentioned it during *Off The Hook*, I'll say there was plenty of room!

Although I found many of the talks interesting, by far the conversations that you find yourself involved in - either through the talks or issues and projects outside of HOPE - are such a mesmerizing experience. Having listened to *Off The Hook* for many years, and past ones from as far back as 1989, it was quite the experience to randomly find myself on the elevator with BernieS and TProphet. Amazing individuals!

As for the MAGA issues that have been greatly covered and talked about, I did experience it firsthand. I was attending the talk on "The Hacker Mystique" and, when questions were allowed, an individual with the MAGA hat came forth. As the presenter couldn't see through the lights, she asked the person if he was indeed wearing a MAGA hat, which seemed to upset her. This individual then proceeded to demand proof regarding the Captain Crunch issue, to which she explained where he could find his proof. At this point, he wanted to ask another question but was cut off, although he proceeded to shout something anyways, not audible to me, and was shut down by the speaker. She did handle it well. The troubling point came when he sat back down. He was visibly very upset, his leg bouncing and twitching; you could clearly tell this guy was angry. His body language and reaction to being cut off made me a little uncomfortable, but only because he was sitting directly across from me. It looked like this guy was going to go off like a cannon.

That was the only experience I had with this MAGA situation, and it in no way altered the great experience I had at HOPE. My take on this issue is that while I don't think it's reasonable for there to be a complete ban of people who wish to wear these hats, it's when they forcibly speak out with their hatred and wish to push their views onto others that they should be removed.

Mitch Altman on *Off The Hook* made a great point: while the MAGA hat to some means (possibly) positive thinking, to many it shares the views of your president, and moreover is viewed as a hate symbol to many others. And I'm guessing that's why it offends so many. I'm not bothered personally if someone wishes to wear that attire, but I am bothered when the same individual wishes to push his hatred-filled views at a convention which emphasizes equality, and is suppose to be a peaceful medium for the sharing of information with a technology focus.

I wore a Pirate Bay shirt, and I witnessed many others wearing shirts sharing their support for one idea or organization, but it's my personal view that political attire should not be worn to a conference, as undoubtedly they might/will offend many, and MAGA is a symbol of hate.

With that said, I just wanted to mention it was a great conference, and I genuinely hope (no pun) that it continues. Don't let the bad few stop the great gathering of minds. Such a great time and experience. I'm guessing the only thing you'd all like to do now is kick back with the remaining bottles of Club Mate!

The Circle of HOPE Writer #20

We're not going to tell people not to wear political attire if that's what they choose to do. Hate speech is another matter entirely. We don't think MAGA hats alone meet that standard, at least not yet. As you rightfully observe, it's the behavior that's the true issue, something that hasn't been a real problem until now. So that's one of the areas that we need to focus upon.

Dear *2600:*

Just sending some general feedback. "First time caller, long time listener." This was my first HOPE. I booked it specifically because it fell on my birthday weekend, and how else should you spend the big day but with some like-minded awesome people? It was great. I really had a good time, met a lot of nice people and, best of all, passed my Technician Class license.

As far as the event, I felt that the talks were great and timely, as well as informative. It is hard to pack so much into three days, but you did a great job of making an agenda that was jam-packed with interesting and relevant info. I understand there used to be elevators for just HOPE and they were down, so sure, that was a bummer, but the hotel did a decent job keeping things moving. The second floor seemed to close early Friday and maybe I didn't check the schedule close enough, but that's just my opinion.

I know there was "the incident heard round the world" but I was not in that talk, so I won't comment or speculate. I trust that HOPE's CoC team and security handled it the way it was supposed to be handled. Overall, I felt very safe at the event, and noticed a security presence without them being pushy. The whole RTFM on the floor was funny also. Not sure why some people felt that was "non-inclusive," but as IT and InfoSec people, we often deal with those who don't read even the basic info and expect every detail handed to them. As a first time attendee, I felt the registration and security staff downstairs were very helpful. Any HOPE volunteer I ran into or asked a question of was very kind and helpful. I appreciate the video feed downstairs too, so I didn't have to fight crowds and could find time to eat. TOOOL and the vendors were very nice and awesome to talk to.

I'm very proud of HOPE for having a connection with Queercon. I wasn't aware of how large they were as a group, and I had a great time meeting and connecting with them. They too were very welcoming.

I have to say for a group of hackers on planet earth, "we" really do get a bad rep in the world as this closed off society of basement dwellers. Everyone I talked to was super nice and willing to chat.

A really great event put on by exceptional people. I look forward to the next HOPE! Also planning on attending my first *2600* meeting next week, and trying to get involved in ISOC in my local community.

Thanks for what you put into HOPE!

The Circle of HOPE Writer #21

Yes, we had a few people who were offended at the RTFM notice on the floor in front of the information desk and so we had it removed. Not a big deal. While elevators are always a challenge, for the most part they seemed to be working well for the conference, especially considering we had added an additional floor this year. The second floor was actually open around the clock - it's possible a lot of people had migrated to the first floor for Friday night's concert when you were there. Registration, however, closed during the overnight periods.

Dear *2600:*

Thank you so much for putting on an amazing HOPE conference! I just wanted to write and say thank you for everything. I am a longtime fan and supporter, and I was also the person (or one of them, at least) that had the medical emergency at HOPE - during Jason Scott's talk, because I get anxiety from medical talk about veins and heart surgery, etc. I ended up getting lightheaded and passing out, collapsing unconscious onto the (carpeted, thank goodness) floor. Your security and medical staff were very helpful and I really appreciate the assistance. Luckily, I was fine after a bit of cooling off and water, and I ended up heading home with my cousin.

Unfortunately, because I had to leave early, I did not get to buy the HOPE talk DVDs that I wanted! I hope you can please make them available online or post the audio/video soon.

I know there was some discussion on *Off The Hook* about the MAGA hat controversy/disruption at HOPE, but I would just like to say thank you to the staff for all of their help and assistance with my situation. I appreciate it.

The Circle of HOPE Writer #22

We're glad you're OK. Our security/medical volunteers are probably the least recognized in our team. So many crises took place behind the scenes that never disrupted the rest of the conference due to their efforts, not to mention the fact that they were always there to help people who were dealing with emergencies. We all owe them big time.

Dear *2600:*

This year was my first time attending a HOPE conference, and it was a pleasant experience. To my surprise, when listening to your July 25, 2018 *Off The Hook* podcast, I learned of alt-right agitators that trolled the conference. I was there for all three days and did not see them, nor did I hear anybody else talk about them.

When I went to Twitter, I saw that a few in attendance discussed the matter at length and, in doing so, gave the agitators exactly what they wanted: attention. To make matters worse, this was the subject

of an entire podcast immediately following the conference, giving them further propaganda they could take back to their base to show what they can do with just a few actors, consuming the dialogue on Twitter and in the podcast, giving the misimpression that they disrupted the conference when they were contained and largely unnoticed. It is unfortunate that a "letter of no confidence" was published regarding the incident, as this too can be used by the alt-right for propaganda.

As *2600* continues to espouse its values of free speech, tolerance, respect, and encourages those "to step beyond prejudices, societal norms, and other perspectives that lead to disrespect for people and groups" (and the occasional anti-Trump comment), it becomes a convenient target for the alt-right because its values are the antithesis of theirs.

I think it's important to consider that one of those agitators was at the Charlottesville rally, which indicates that this person, and the few that came with them, are willing to go to great lengths to target *2600*. These actors were able to provoke the appearance of causing major disruptions at the conference and can now use the latest podcast and Twitter screenshots as highlights and recruiting material.

Again, great conference, look forward to returning in 2020.

The Circle of HOPE Writer #23

You are dead on in saying that we're all giving provocateurs exactly what they want when we provide them with undue attention or wind up turning on each other. Once that happened, we had no choice but to address it, even if that had the effect of making it even more of an issue. All the more reason to address the initial situations with caution and unity.

Dear *2600:*

There are three things I want to say just in case the rest of this gets too long to read:

Thank you for putting on this event.

Thank you for having it at such a convenient venue.

Thank you for being so welcoming, especially to first time attendees.

This was my first HOPE conference. I wanted to attend the previous one, but couldn't pull a plan together before tickets had sold out. Really, I don't know why I didn't come many years sooner. Maybe it was a fear of not belonging.

After missing the boat two years ago, I decided to attend some *2600* meetings, which helped me a lot, and in some ways that I didn't expect.

The last time I had set foot in New York City, prior to showing up for my first *2600* meeting in June of last year, was sometime in 1993. I didn't get to know the city as well as I would have liked to back then. In 1993 I was still underage, so lingering or exploring were not my choices to make. Going to the meetings proved a great way to get to know the area around Hotel Pennsylvania and discover what resources would and would not be available to me.

Since my teen years, for reasons unknown, I developed several different food allergies. A few of them have grown severe enough to force me to carry an epinephrine pen. Having advance knowledge of the turf, and what food I could and could not buy was invaluable in maximizing my time spent enjoying the conference.

An unexpected bonus came by way of making friends, who quickly helped me realize that my worry about "fitting in" was unwarranted. It's wonderful how we don't all have to be the same breed of hacker to sit around the same table.

That being said....

Thank you for including chemistry, biohacking, and broader scientific topics. "Torrent More Pharmaceutical Drugs" was the perfect talk to kick off my HOPE experience.

A good part of my early Friday afternoon was spent shopping for food, but I made sure to return in time for the social engineering panel. Thank you for the supplemental screens; they made bad seats into good seats.

Of all the rooms, I liked Booth the best, in part for its intimacy (and its phone booth), but mainly because the lighting in there was particularly well done.

Sleeping later than I had intended led to my having a very different Saturday than some attendees did. I watched Barrett Brown on the wall downstairs. I missed out on much of Chelsea Manning, opting instead for the Wi-Fi safari workshop (which was quite fun). I brushed by one of the controversial hat wearers while on my way into Vaughan late Saturday afternoon.

I admit I went from shocked to angry very quickly. What I did not know at that moment was that someone had already let their anger get the best of them. It took conscious effort on my part to not say or do something. What kept me in line was a strong desire to not get thrown out, and to not make things any more unpleasant for the nice young security person walking him out.

Staff really went above and beyond in rising to meet certain challenges, in particular a medical incident on the mezzanine. After all that transpired, the great, the good, the not-so-good, the bad-but-it-could-have-been-a-hell-of-a-lot-worse, the weird, the wonderful, and the wonderfully weird, it seemed completely appropriate to start Sunday with an LED rainbow dildo and end it with a singing rat. I hope there will be another HOPE. I hope all of us can make it there.

Thank you for an educational, entertaining, and memorable weekend.

The Circle of HOPE Writer #24

And for anyone who might not get some of those references, we invite you to watch the videos and experience the entire conference. Thanks to everyone for engaging in the dialogue, living the experience, and helping us to improve.

Got Something to Say?
(of course you do)
letters@2600.com

EFFecting Digital Freedom

Unintended Consequences? Twenty Years under the DMCA

by Jason Kelley

One of the consequences of the rapid pace of tech's advancement over the last 20 years is that a layer of software is in nearly everything. What used to be relatively mechanical devices like tractors and coffee makers are now "smart," filled with thousands of lines of code. Which could be very cool for coders, researchers, and anyone who wants to interrogate the technology they use - like being in a more pleasant version of *The Matrix*, where knowing a little bit of programming practically turns you into a superhero.

But there's a big problem with this version of the story: much of the code that powers the devices around us is hidden behind "access controls" that make it off limits. It's been this way for 20 years now, thanks to Section 1201 of the Digital Millennium Copyright Act, an incredibly overbroad law that prohibits "circumventing" those digital locks when they control access to copyrighted works like movies, music, books, games, and software. As a result, a lot of useful and important activities are banned. If you're doing what mechanics have done for decades - taking apart your car to repair it - or if you're trying to update the software on a device that the manufacturer has stopped supporting, you're potentially wading into illegal territory. That could be true for your interaction with just about any device that's got software on it.

It's no surprise that the broadly written law - which was supposed to (for example) stop DVDs from being ripped and shared online or stop cable customers from descrambling channels they hadn't paid for - would also be used to protect phone makers who want to restrict users' carrier options, and to allow manufacturers like John Deere to stop farmers from getting independent repairs. In fact, it was so evident that the law would create a domino effect like this, impacting users of devices that hadn't even been thought of yet, that a supposed "safety valve" was built in. Every three years, Section 1201 permits the Librarian of Congress and the U.S. Copyright Office to create exemptions for important activities that would otherwise be banned by the DMCA - and that means that how it affects users like you changes fairly often.

This exemption process - known by the *Game of Thrones*-like title of "The Triennial Rulemaking" - has a lot of problems. To start, it turns a group of copyright lawyers into decision-makers who determine what every single user can do with their electronics. Even when exemptions are granted, they're often too narrow. In 2009, the Librarian first granted the petition exempting jailbreaking of smartphones, but other smart devices, like tablets, weren't included until 2014. So, despite their similarity, up until that point an iPhone was exempt but an iPad was not. It sounds like progress, but there was no valid reason it took so long for tablets to be included. At this year's rulemaking, we argued that the exemption should also apply to smart speakers and voice assistants - because of course it should. We received the exemption (yay!), but to understand more about why so many consider this an outrageous law, here's what the opponents - the manufacturers - argued: jailbreaking is likely to enable voice assistant devices to access pirated content, and in fact, more likely than laptops or smartphones because the devices are so "simple." The Copyright Office was unimpressed by this, but in three years we'll have to do it all over again to include whatever new "smart" devices have been popularized in the interim. Meanwhile, jailbreaking them may be off limits.

There's also no guarantee the exemptions won't expire. Despite the fact that arguments against jailbreaking your phone or remixing video snippets don't get any better, groups like EFF return every three years to defend our victories while also trying to expand the exemptions for new and nonexempt activities and devices. In 2006 and 2009, the Librarian of Congress granted an exemption for cell phone unlocking. But in 2012, the exemption was granted only for a limited window of a paltry few months - and by January 26, 2013, cell phone unlocking was once again a potential DMCA violation. Luckily, a massive public outcry convinced Congress to pass a special law effectively reversing the Librarian's decision, because practically everyone agrees that people using their phones with the carrier of their choice has nothing to do with copyright infringement.

Importantly, DMCA 1201 contains several distinct prohibitions: a ban on acts of circumvention, and a ban on the distribution of tools and technologies used for circumvention, which chills the free speech of researchers, among others. Activision, Apple, Microsoft, and HP have all threatened security researchers who wanted to share information about security flaws. Even *2600* was the subject of censorship: eight major motion picture companies brought successful DMCA claims against the magazine to stop it from publishing DeCSS, a software program that defeats the CSS encryption used on DVDs. While the law contains exceptions for encryption research and security testing, like the rulemaking exemptions, those exceptions are far too narrow and have never been successfully raised as a defense by anyone.

All of this amounts to a patchwork of changing regulations that severely hinder what should be legal, fair uses of devices. These regulations harm consumers by being used and abused to increase manufacturer control and to discourage competition; they limit accessibility by hindering applications like screen readers; they squash creativity and art which can help us critique media or create new works that build on older media; and they interfere with legitimate research.

Thanks to work by advocates, researchers, archivists, artists, and more, the latest round of exemptions, released in October, are the most expansive yet. Researchers have more freedom to investigate and correct flaws on a wider range of devices. People who repair devices, including vehicles and home appliances, have more protection from legal threats. Filmmakers, students, and ebook creators can use video clips more freely, and a small expansion for online video game preservation allows certain groups to reproduce and modify some video game server software. But the exemptions are still too narrow and too complex for most technology users.

On behalf of a security researcher and a digital entrepreneur, EFF has sued the federal government, arguing that Section 1201 and the rulemaking process are unconstitutional restraints on speech. Having finished this year's rulemaking - the Seventh Triennial - we look forward to continuing that case. Until then, EFF will continue to fight to make the world safer for those who want complete control over the devices they own.

Facts About Honesty/Integrity Tests and Interviews

by David Ricardo

It was with some interest that, among the letters of the Spring 2018 issue of *2600*, I read that a correspondent named "GazetteMed" was interested in an article regarding honesty tests written by "U.R. Source" as published in the Autumn 1993 issue. I have to use a pseudonym here, unfortunately, because revealing many of the matters discussed in this article may have consequences. Honesty tests and psychological tests in general derive much of their strength from their mystique - but there is no mystique. Anything devised by the mind of man can be beaten by the mind of man and it is only when you start messing with natural things, like the climate, that you get into real trouble. As long as there has been technology, there have been hackers, and all you need do is think back to that kid down the street who, in the 1930s, took a radio apart, reassembled it, and suddenly he or she was listening to the news from Paris. It is natural to want to know how things work and psychological tests are no exception to this rule.

Honesty tests (or "integrity tests" as they are now often called) still exist and are still used. In 1993, they were all pencil and paper tests, and scored with a perforated piece of card stock by counting the "correct" answers. Now the company administering the test buys software and they are all machine scored. Twenty-five years ago, the leader in the field was the Reid Report, now called the Reid Test, named for John Reid, a pioneer in the field of using a polygraph, another pseudo-science that has somehow gained respectability in certain quarters where, unfortunately, it can make a difference in your life. John E. Reid and Associates is doubtless among the leading commercial entities in this field and one of the services they now pitch is an "integrity interview," which is a highly structured process which (they say) will uncover every dark secret in your past. The interview is a very detailed and highly structured procedure that takes some time to completely administer and requires a trained interviewer. Despite its highly structured nature, the length of time it takes will vary depending on what salacious details you reveal - after all, if one little thing comes to light, there must be more and bigger things, and all it takes is digging. The interview is based on a simple technique: all tests of all kinds must be normed, that is, baseline scores must be established that derive from what the test constructors believe to be normalcy, hence psychological tests generally have a white, upper middle-class bias built into them because these are the people who construct the tests.

The polygraph works, when it works at all, because the person unlucky enough to be hooked up to one believes that there is some technological magic about it, and this places the test taker at a serious disadvantage. With the interview, it is different: many people do have a strange compulsion to confess their sins, real or imagined to other people. Maybe they feel this makes them seem more human, maybe they think that confession will cleanse their soul or maybe they just want to talk to someone and that is certainly a good way to strike up a conversation – a fact, I might add, that has led to many false confessions. There is no built-in evolutionary mechanism compelling us to confess to others. Instead it all goes back to your parents when they looked you in the eye and made it seem that they knew the truth even if you weren't telling the truth or even if you did not know what the truth was yourself. This is why the confessional works as well as it does: you are confessing to your "father" in exchange for cleansing you of the sin you are confessing and, theoretically, you are the winner in that transaction. I do not know this is true in the case of the confessional; with integrity tests, this is not the case, theoretically or otherwise.

The integrity interview works because the person administering it builds up rapport

with the person being interviewed, usually by indicating some similarity between them: "Your father was a dairy farmer? Well, what do you know, my uncle had a dairy farm..." and the interviewer will say this to you even though he has never been near a dairy farm in his life, and the people who made the integrity interview learned this trick from studying very good salespeople. In the world of honesty testing and interviewing, it is ethical for them to lie to you but not the other way around. Most people will open up to the interviewer because this person has been established as one of them. The easiest way to get the interviewer off balance is to know even a very little bit about the field, and ask the interviewer a question about this alleged past that only someone in the business would know. They are prepared with some stock answers in many common fields, but when it comes to a discussion of the specifics of dairy cow productivity, they will know nothing. Since they are trained to not get flustered, they will respond with a stock answer like "it was a long time ago, I was young, my uncle sold the farm and I really don't remember much about it, except that I was very happy there." This will satisfy 99 percent of the people likely to be interviewed. It will also tell you that this is an integrity interview, even if the interviewer does not (which he or she won't) and if you should ask, they will say that it's just a personality test or a general employment test. The interview starts out with simple questions that are intended to get you talking: do you like animals, what's your favorite food or color or kind of car - and this just reinforces the belief that it is just some silly personality test. Then the questions get progressively deeper: are you happy, do you like your boss, have you ever hurt an animal? Before the end of the interview, the questions are "Have you stolen anything from your current employer?" and because you have been talking so much and so easily, it is simple to say something in response to this, and if you believe that the interviewer has the ability to peer inside your mind and know whether you are being truthful, then you will tend to be truthful. If you have stolen something and you are truthful, you get no points for your candor, as the interview will immediately turn to determining what it was that you stole, how many times you did this, when you did it, and the cumulative value of these things you stole, which can even include time for which you were paid but during which you did nothing for your employer. If you are truthful and adamant about this, then the question is "Have you ever stolen anything from any of your employers?" The people who constructed the interview believe that the test taker will regard their current employer and their past employer as somehow different, but as far as the test/interview is concerned, if you stole from a past employer, you are almost certainly stealing from your current employer.

Here is the really strange thing about the interview, and the Reid Report, too: the instrument was designed and normed by people with that white, upper middle-class mentality and morality, and they do truly believe that everyone has stolen something from their employer. After all, it is the American way. In this case, it is a good idea to admit to stealing something small a long time ago: pencils, pens, or a stapler are good choices. Just be sure to keep it under ten dollars of value and in the distant past, when you were young and your moral sense was not yet fully developed, and there is actually some truth to this. You should indicate that you do not dwell on it (because if you did, you'd be thinking about stealing again) but when you do think about it, you are not pleased with yourself for having done this thing but, again, don't stress this. In the course of taking any integrity interview or test, *never* confess to *anything* else that is not a matter of public record. Now, let's say, just for the sake of argument that you truly have never stolen anything from anybody and that you are being completely honest about it. You will immediately fail the interview and/or the test because, according to them, everyone has stolen something and you must be "faking good" as they call it.

There are many states where pre-hiring honesty tests are illegal, though these generally refer to the pencil and paper or computer variety of test, rather than the

interview. The Reid Company is very secretive about these things, and the interview could have been developed to get around this limitation while offering its customers a pricier alternative. In other states, these tests can be used, but the results of such tests cannot be the "primary" determining factor in deciding to not hire someone. This is a matter of such legal complexity, particularly given federal employment laws, that the potential employer will simply find another reason for rejecting the applicant, and it is very difficult or impossible to prove anything in a way that is legally actionable in court. If you are applying for a job where you are handling money or merchandise that is easily sold for money - liquid Tide detergent or Gillette razor blades - you almost certainly will get some version of the test, assuming it is legal in your state, so cashiers and retail shelf stockers are frequently subject to employer integrity testing. If you are in a position of trust with minimal supervision, such as a security guard, a field service rep, or a home health aide, you will probably be subject to some form of integrity screening.

There are myriad psychological tests that will measure any aspect of the human mind. "GazetteMed" mentioned personality tests and there is no critical shortage of those. The most commonly used test is the MMPI, the Minnesota Multiphasic Personality Inventory, which consists of several hundred questions each in the form of a statement and you are asked whether you agree or disagree with it. This is commonly used in criminal justice, though it can be found in use elsewhere, such as job screening or for diagnostic purposes, and it is a test where there is no middle ground: you either agree or you don't. Whole books, and very thick books at that, have been written about this test, and many very thick books remain to be written about it. There are also projective tests, such as the TAT and the Rorschach, both of which are subject to the vagaries of interpretation, and the ever-popular intelligence tests, and I haven't even scratched the surface.

Here are some quick suggestions for beating these tests: in the MMPI, be aware of what the question is asking, and make a mental note of how you answered this. The people who constructed the MMPI think you are not capable of doing this, but if you do and you are consistent, then you can come across as anything you want from an absolute saint among people to another Stalin: it's your choice. Only in the most recent versions of the MMPI are there any measures intended to detect "faking good" and if you follow the advice regarding the integrity tests and interviews, you will make mincemeat of this feature. The Rorschach is another test about which whole books have been written and it and the TAT deserve an article of their own.

Without getting into the subtleties of validity and reliability and all the other characteristics (projective tests such as the TAT are not valid to the point of meaninglessness and the reliability of a projective test is largely dependent on the relationship between the test administrator and the test taker), and while the integrity tests and interviews may be valid in that they measure what they are supposed to measure, they most assuredly are not reliable. For example, the test-retest reliability when the same person takes the test a second time is highly variable. This writer does not know of any published information regarding the validity and reliability of integrity tests and I think that this is simply because the people using these tests are solely interested in results rather than whether they are actually good tests.

So, there you have it: about 2,000 words on this topic. Let me close this article on an ominous note: given the current political climate in the United States, it is highly possible that honesty tests will become legal in many jurisdictions where they currently are not. Yes, you can refuse to take the honesty test, but if you do, you are immediately removed from consideration for that job on the grounds that your application is incomplete. If you find yourself in that position, all you can do is be aware of what the test or interview is and know how to defeat it to get what you want from it.

BOOK REVIEW

Surveillance Valley: The Secret Military History of the Internet,

Yasha Levine, 2018, ISBN 978-1610398022

Review by paulml

Conventional wisdom says that, in the 1960s, a group of universities started what became the Internet with help from the Pentagon's Advanced Research Projects Agency. The reality is quite different.

William Godel, a military intelligence officer, thought that a better way to win in Vietnam was to use new technology to anticipate the movements of the North Vietnamese and understand their motives. Such new technology was quickly used on domestic war opposition. That is what led ARPA to help create the Internet, using computers to spy on Americans.

Today, all of the major tech firms, like Google, Facebook, and Amazon collect private information for profit, while letting agencies like the NSA scoop up their online activity for its own purposes. Silicon Valley and the military are generally one and the same: a sort of military/digital complex.

The Tor browser was supposed to be The Answer: a method of communication that the government can't read. But Tor got most of its original funding from the Broadcasting Board of Governors (the people behind Voice of America and Radio Free Europe), an offshoot of the CIA. For most of its existence, it has subsisted on large government contracts. Why is one part of the government, the Broadcasting Board of Governors (BBG), supporting Tor, and another part of the government, like the FBI, trying to shut it down? It keeps all the activists and other anti-government types in one place, where they can be easily watched. Tor's credibility is certainly helped by an endorsement from Edward Snowden.

This is an excellent book. For a few people, this book might be common knowledge. For the vast majority of people, this book is full of revelations about how ubiquitous surveillance has become in America. Nobody comes out clean in this book, which is highly recommended.

BOOK REVIEW

Ten Arguments for Deleting Your Social Media Accounts Right Now,

Jaron Lanier, Henry Holt & Co., 2018

Review by paulml

For most people, being on social media is as important as eating and breathing. This author gives a very different view.

There is a very strong comparison between a person who is addicted to social media and simply must check Facebook every ten minutes, and a trained dog. What is happening on social media these days is no longer just advertising; it has now entered the realm of behavior modification.

The present-day business model seems to be to find customers who are ready to modify their behavior.

In the past, advertisers could measure whether a product did better after an ad was run. But today, it is possible to measure if a specific individual changed their behavior (usually in a negative way), and their feed is continually tweaked to get that individual behavior to change.

The author talks a lot about a statistical machine in the cloud that he calls BUMMER. It stands for "Behaviors of Users Modified, and Made into an Empire for Rent." Among its components are: cramming content down people's throats, earning money from letting the worst people secretly screw with everyone else, and directing people's behaviors in the sneakiest way possible. Don't forget the rise of fake mobs. BUMMER can be found in the author's other objections to social media: social media is undermining truth, it doesn't want you to have economic dignity, it is making what you say meaningless, and social media hates your soul.

This book is short and excellent. The author is one of the pioneers of virtual reality, so he knows what he is talking about. This book is very much recommended, both for those who wonder if social media is really worth the time and for those who can't imagine life without it.

Modem and Me: The Loose Ends

by Emily Saunders

This is an update to the article "Nightmare on E Street (Modem and Me Against the World)" which appeared in the Winter 2017-2018 issue.

I called a private tech company and managed to snag a free in-home consult. The guy who came was friendly. We sat on my couch and I showed him a few of my screenshots and provided a summed-up overview of my issues. Unfortunately, he didn't seem to take me seriously. The gist of what he said was: *"What you're seeing is normal Internet traffic. Everything you've been told up until now has been inaccurate. Stop worrying about it*."

It would have been so easy to believe him if I had talked to him first. But even so, there were some things that just didn't add up, no matter how you looked at it. Yes (sigh), I had come to the realization that some of the site history that I hadn't recognized, like `art-0.nflximg.net`, was actually innocent stuff such as "Netflix images." Some of it was adware. But some of it, like `aia.entrust.net`, was genuinely malicious. So my stress levels improved somewhat, knowing both that a good chunk of it was just annoying but harmless crap, and also knowing that I wasn't just paranoid.

I still couldn't explain the email on my CenturyLink account being changed to a combination of my two email addresses. That wasn't the kind of mistake I would make. I was still unable to explain some of the unfamiliar site history, like the police officer forum or the Super User computer forum that the Geek Squad said appeared to be indicative of a hacker using my network to research more hacking strategies. I hadn't forgotten this stuff, but I was out of steam. Being a freaked out basket case takes energy. I was beginning to accept that, in the absence of taking computer science courses, there were some things that just might never make sense to me.

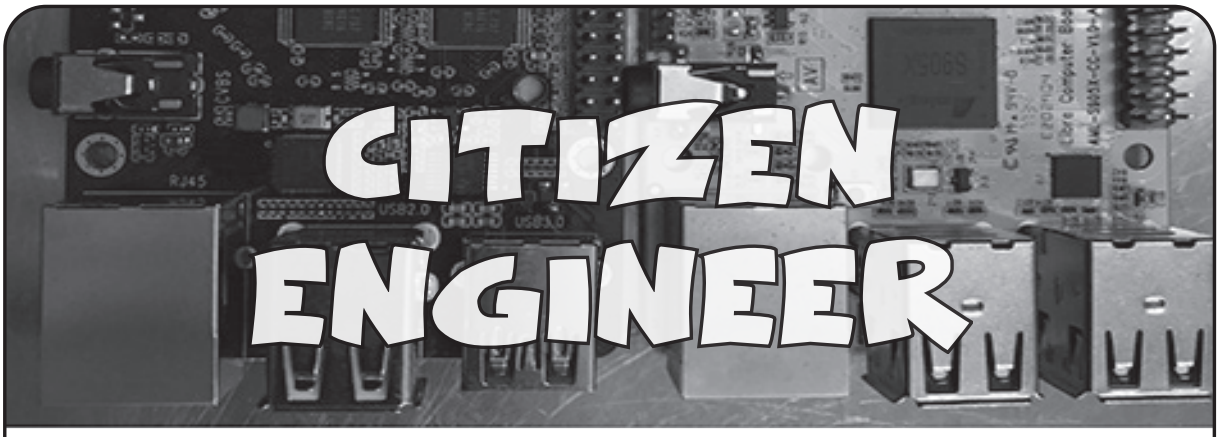
As I began to get used to Xfinity, I gradually thought about it less and less. One thing that helped was that the people in the apartment next to mine moved out. I had suspected it might be them messing with my Wi-Fi when I saw a brand name of another modem on my network and they were closer than anyone else. A little voice inside my head suggested that they moved because they couldn't get away with jacking my Wi-Fi anymore. Ha!

My Xfinity modem was a lease and, after thoroughly familiarizing myself with it, I decided it irritated the hell out of me and I should shell out for my own. The advantages of a decent modem far outweighed the only possible mitigating factor for me: modem tech support from the ISP. Owning my modem meant I had full control of it, whereas leasing came with the support, but then obviously Xfinity could tinker with it if they wanted to. So in my view, the advantage wasn't much more than getting to bitch at someone else when whatever modem issue you were having used up all your patience - as opposed to taking care of it yourself.

I went to Micro Center and ended up getting a Netgear Nighthawk AC1900 Wi-Fi cable modem router. On sale. I got it in October of 2016 and am still using it. It's a big improvement over the Xfinity lease. It's not perfect - nothing is - and I poke around in the modem settings every once in a while. I don't see much but the few things I do see, like right now the logs are full of stuff like DoS attack, Ping of Death, Teardrop or derivative, illegal fragments etc., but I just don't care. As long as they don't get through, I'm fine.

Probably what bugs me most is when a male buddy of mine was hanging out and tried to watch porn on his phone while using my Wi-Fi. This bugged me because not only does porn repulse me, but porn sites can be full of malicious crap that will f*** up your network. I block several things with my parental controls, including porn. Who knows, maybe that's a legitimate deterrent to hackers trying to steal your Wi-Fi.

I'm more confident in my technical knowledge now. I'm familiar enough with this stuff by now that anything left that I'm not familiar with I figure must not be too important. I know more than any of my friends do. It's endearing when they come to me for techie stuff because if I'm an expert, then the bar is set too low. I'm aware that I'm still a dunce compared to the likes of *Hacker Quarterly* readers. That's still plenty good enough for me.



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

Hardware Hacking with Linux SBCs Just Got Easier

Back in February 2018, Bartosz Golaszewski, speaking at FOSDEM (Free and Open Source Developers' European Meeting) at the ULB Solbosch campus in Brussels, announced a new GPIO interface for Linux user space . What's that? Before we get started, let's discuss SBCs (single board computers) and all the Linux-y hardware that's out there now.

According to `linuxgizmos.com`, there are more than 100 Linux boards that are under $200 and run Linux or Android. They have a comprehensive list at `http://linuxgizmos.com/january-2018-catalog-of-hacker-friendly-sbcs/` and a spreadsheet comparison at `https://docs.google.com/spreadsheets/d/e/2PACX-1vT_J1QkNQIFfMdcLisDUs4j-imyqwwsUpyn7RTKNYyz857TdT5PMlyeKTZ_lxemRIls-td9lAmupzo7/pubhtml`.

You've probably heard of Raspberry Pi, which is by far the most popular single-board computer (SBC) in the world according to the estimates we're able to gather. There are well over 15 million units in the wild. That's a lot of Linux and a lot of potential to do hardware hacking. The challenge is... each board interacts with hardware differently, and that brings us to libgpiod.

libgpiod is intended to be a fast kernel-level-supported method for writing/reading/monitoring GPIO pins on various Linux boards, replacing the two main methods that are currently used: sysfs file pokin' and devmem twiddling.

With sysfs style control, you end up with files such as `/sys/class/gpio/gpio16` (for pin #16) that you can write and read from to set direction and read values. It works OK, and is very easy to use with shell scripts, but is clunky from C or Python, and is slow and incomplete (for example, pullup/downs are not supported).

With devmem twiddling, you open up a file point directly to chip memory and start poking and prodding at the registers directly, somewhat similar to older computers' "peek" and "poke" commands, or the microcontroller style `PORTB |= 0x01`. Benefits? It is heckin' fast. Downsides are that its a horrible idea to poke into memory, and you end up having to make register maps for each processor and revision because the registers move around. You can see some example code for a DHT driver for Raspberry Pi here:
`https://github.com/adafruit/Adafruit_Python_DHT/blob/master/source/Raspberry_Pi/pi_mmio.c`

and then this different code for a BeagleBone (the register map is different):
`https://github.com/adafruit/Adafruit_Python_DHT/blob/master/source/Beaglebone_Black/bbb_mmio.c`

As you can tell, this quickly becomes hard to support and it's dangerous - you need to be running as root and it's incredibly easy to accidentally poke the wrong location.

With more Linux boards coming out with GPIO (there's probably a dozen more released since we wrote this), having a consistent, reliable, complete GPIO interface is pretty important to avoid icky unmaintainable code. So we're pretty psyched about libgpiod. From our experiments, it's much much faster than sysfs. It is not as fast as direct memory twiddling, but that's not too surprising - there are still kernel messages and error checking done. A Pi 3 got us 400Khz pin output toggles in a loop in C, 100KHz in Python examples, and that's pretty good for bitbanging. (For SPI or I2C, use the hardware peripherals - they can go multi-MHz and can be shared between processes!)

We really like the Python 3 bindings for libgpiod. They're very easy to use. Here's some example code for blinking an LED. This will work on any computer with GPIO pins and libgpiod. The only thing you might have to change is the PIN definition to match the pin you have an LED connected on!

```
import time
import gpiod
```

```
# the name of the GPIO peripheral, almost always gpiochip0
CHIP = "gpiochip0"
# this is the 'offset' for the chip, e.g. Raspi GPIO #18 is pin number 18
PIN = 18

# Open the chip
with gpiod.Chip(CHIP) as chip:
 # get control of the GPIO
 line = chip.get_line(PIN)
 # set the pin to be an output, the consumer string can be anything
 line.request(consumer="blinky.py", type=gpiod.LINE_REQ_DIR_OUT)
 # Toggle!
 while True:
 Line.set_value(1) # LED ON
 Time.sleep(0.1)   # wait 100ms
 Line.set_value(0) # LED OFF
 Time.sleep(0.1)   # wait 100ms
```

Likewise, here's a very simple example for reading a button press (digital input). This example does a little more, like keeping track of wire state. A pull-up resistor is required to maintain a non-floating state. Then connect a normal button or switch between the pin and ground.

```
import time
import gpiod

# the name of the GPIO peripheral, almost always gpiochip0
CHIP = "gpiochip0"
# this is the 'offset' for the chip, e.g. Raspi GPIO #18 is pin number 18
PIN = 18
# Connect a ~10K pullup resistor from this pin to 3.3V (or whatever your logic is)

# Open the chip
with gpiod.Chip(CHIP) as chip:
 # get control of the GPIO
 line = chip.get_line(PIN)
 # set the pin to be an input, the consumer string can be anything
 line.request(consumer="button.py", type=gpiod.LINE_REQ_DIR_IN)
 # we'll keep track of the last button state, so we print changes
 last_button_status = line.get_value()
 while True:
 # read the line
 line_status = line.get_value()
 # did the state change?
 if line_status != last_button_status:
  # print what happened!
  if line_status:
   print("button just released")
  else:
   print("button just pressed")
  last_button_status = line_status
 time.sleep(0.01) # De-bounce buttons by putting a light delay
```

To get you started with more advanced projects in C, we have a basic "collect GPIO pulses and store them in a circular buffer" program here:
https://github.com/adafruit/libgpiod_pulsein

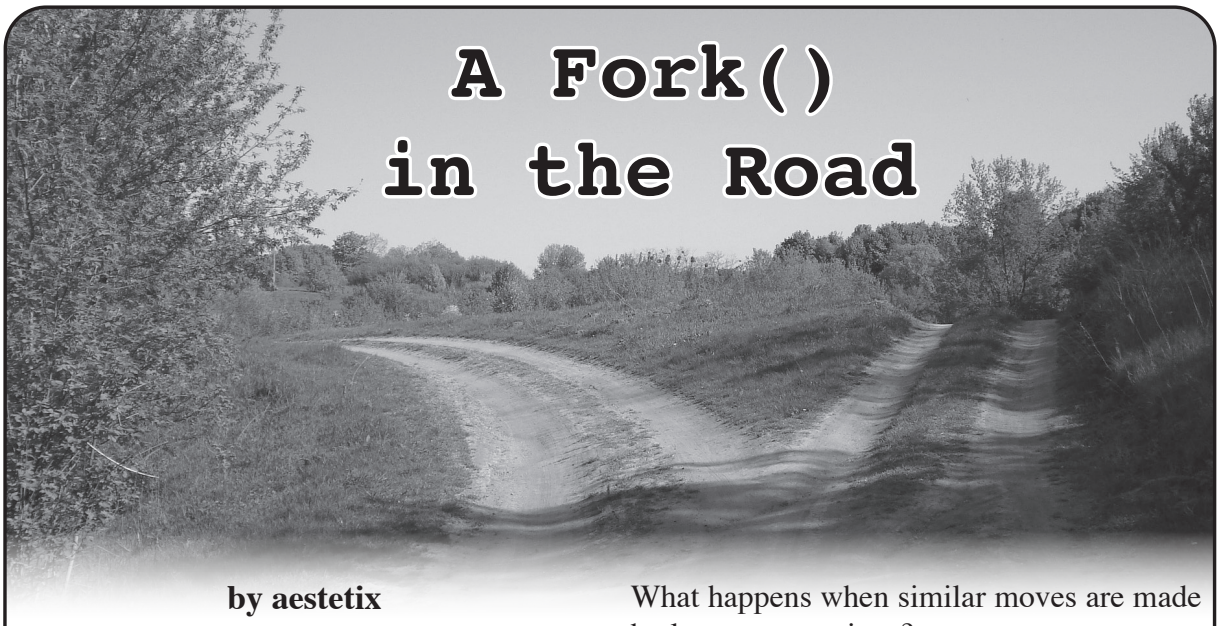
This is basically code that will replace some Python DHT drivers we released, and has the benefit of being forward compatible with any other Linux board that runs a 4.8+ kernel. We'll slowly be replacing the code we previously released to use libgpiod, so that we can have broad support for Raspberry Pi, Onion or Banana Boards, BeagleBone or Onion.io.

There's not a lot of libgpiod code out there, and libgpiod doesn't come stock on Linux distros yet, which may be why it's taking a little while to catch on. There are bindings for C and Python. Here's a script that can help you get started by compiling it for you:
https://github.com/adafruit/Raspberry-Pi-Installer-Scripts/blob/master/libgpiod.sh

If you have any controlling votes in a distro, please have libgpiod available through your package manager! The latest code is here, and as you can tell there's a lot of active development:
https://git.kernel.org/pub/scm/libs/libgpiod/libgpiod.git/

Good night and good luck.

A Fork() in the Road



by aestetix

"Someone must have slandered Josef K., for one morning, without having done anything truly wrong, he was arrested." This is the opening line of *The Trial* by Franz Kafka, a novel about a man who has been imprisoned. The authorities refuse to tell him the nature of his accusation, how long he will be in jail, and what - if any - due process he will receive.

Our relationship with technology over the years (and decades) has been one of tension at best. One can read the history of IBM and see how Big Blue established an almost monolithic enterprise, and then read Steven Levy's *Hackers* and see how the same kinds of technology were used by individuals to build creative inventions. On one hand, we can use technology to create massive surveillance instruments that give governments and corporations all kinds of unaccountable powers; on the other, the same technology can be used to give a voice to people who might never have had one before. This tension is a tango dance on the sharpened edge of a sword, and we're currently at a point where one slip in the wrong direction could be disastrous.

I see a lot of trends in current computing that I not only dislike, but which worry me. If my neighbor prefers to use a Mac and I prefer to use a PC, fine by me. But if my government decides to install surveillance cameras, not only does this threaten to override my personal preference, but it has the potential to impact others as well. And at least governments are (in theory) accountable to citizens. What happens when similar moves are made by large corporations?

I believe computers are tools that ought to be used to enable freedom. But what happens when the technology available to use starts making decisions for us? First it begins by demanding proof we have legally purchased the operating system (such as Windows product activation), then it begins to dictate what software we can have installed on our hardware (the App Store), and finally, it forbids us from even modifying our own hardware, pushing technology as fashion items that are impossible to repair. Add in a few extra features, like forcing people to go to the officially sanctioned company store to fix their increasingly opaque tech, and we've created a Cathedral that not even Eric S. Raymond could have dreamed up.

To make matters worse, we now see the moves by these same technology companies to further abstract control away from us in the form of "web applications." Now, instead of having software locally installed that might occasionally "phone home" to the corporate mothership, our entire computer effectively becomes a dumb terminal that is useless without both access to a fast Internet connection and proper credentials to access the service of our choice. And this extends into all kinds of domains: if services like Twitter and Facebook have forced their way into the public square, does this mean that to participate in important discussions, we now must have access to these services? What happens if one of them decides to kick us off, or to limit our account? And what if our

job depends on them? Right now, we have no recourse.

In some ways this is about control, in others it is about coerced profit. Take software that we would have once purchased and installed on our computer, which may now have moved to a "cloud" only subscription model. Maybe we can't even use it anymore unless we have an Internet connection. So now, not only does our data all exist in the cloud (aka, someone else's computer), but if we skip a month of payment for whatever reason, our access could be completely revoked. Whereas before, we made a one time payment and could confidently say we owned the software on our computer, now we're locked in a carrot-and-stick game that only lasts either as long as our ability to pay in perpetuity or until the company decides to shut down that service. And let's pray that there is no lobbying from said corporations to ensure that the laws remain in their favor.

So what can we do? We need to look at the various fronts upon which these trends thrive, and come up with ways to push back. While we care about our personal freedoms and liberties, these companies generally only care about the short term bottom line. Here are a few thoughts that might help guide us. First, the average person doesn't care about abstract ideas like "freedom" unless they see a direct cost to themselves, so maybe it's useful to construct a narrative explaining that, while there might be short term happiness, there will be long term misery. Second, consider the various cost-benefit analyses various companies employ, and see if there are alternative strategies that either help or make no change for the company while helping the individual, and come up with ways to propose them. If we can honestly tell a company our proposal will cost them nothing and even earn them more money, they will often start listening. Finally, keep a watch both at the local and higher levels of government for bills coming through, push back when necessary, and get involved when we can. Lawmakers are not technology experts, and they really appreciate help from their constituents. There are already some groups - like the "self hosting" and "right to repair" movements - working to make strides in these areas.

As these technology trends have continued to advance, all of us have been losing small bits of individual agency and freedom; the compound loss is significant. There is a clear struggle between the rights of the individual and that of the corporation: after all, surely Microsoft has the right to make sure people aren't pirating their software. But there is a limit. With each of these moves, the corporation gets a little more powerful, and the individual becomes less of a citizen and more of a user. We're now at a point where we need to step back, ensure that we as individuals become aware of what else we might lose, and decide what kind of future we want.

Making an Informed Business Decision Using Public Financial Records

by Brazilero2008

"They found him the same way we did. Financial records. They ran financials on everybody in that prison." - Castle[1]

The plotlines of TV detective shows often involve the navigation of secure databases by nimble-fingered law enforcement agents seeking to investigate the finances of a questionable business entity. In the real world, these rich sources of information do not necessarily require specialized training in data mining or digital forensics. Some of this information is readily available through public servers via an anonymous login (so you won't need an official badge). However, you should have a general idea of what you hope to discover before diving into online records. The following purely hypothetical scenario provides the context for running a quick, basic-level financial investigation across multiple databases in New York State. Of course, your particular situation will differ, so choose your sources of information accordingly.

The Offer

The coworker you met at an office party shares your interest in creating and marketing mixed-media art. This individual says he is the owner of a licensed, service-based business that helps artists sell their work at craft shows. If hired as your sales agent, he promises to increase your market visibility by placing your work in various scheduled shows across New York State. He asks that you contact him to discuss contractual details. Is there a reasonable level of risk exposure associated with accepting this offer?

Tax Liens

Start by visiting the Division of Corporations at the New York State Department of State (NYSDoS) to determine whether the target's business is a registered entity such as a professional or limited liability corporation.[2] Next, the Uniform Commercial Code (UCC) database of the NYSDoS lists debt obligations of registered businesses, including commercial loans and IRS tax liens. Check to see whether any liens are accompanied by a release indicating the debt has been satisfied. Outstanding liens could be a red flag.[3]

The New York State Department of Taxation and Finance reports liens to the local county clerk's office based on the address used when the most recent tax return was filed. If the business has relocated to a different county since the original filing date with the NYDoS, then you need to go to the clerk's office in that county. The new business address may appear on the UCC database if there are recent debt obligations. Incidentally, some municipalities have a paywall on their web page that requires a personal account before you can view or print documents; other municipalities may rely on a privately run, pay-to-access system.[4]

Court Records

There are many offices of the county clerk in New York State that only permit in-person access to public records. In these situations, continue your investigation by clicking on "WebCivil Supreme" located on the e-Courts webpage.[5] The State Supreme Court database lists civil actions against a business when creditors file a formal Summons and Complaint with the Court to attempt recovery of unpaid debts. If the target is listed as the defendant, click on the index number to bring up the case detail page. In a limited number of cases, legal counsel for each side will agree to e-file their respective documents. Click on the "Show e-Filed Documents" link on the bottom right of the page if available to find the "Decision and Order" stating the judge's ruling on the case or the settlement agreement to read the out of court resolution of the dispute.

Public Access of Electronic Court Records (PACER) offers access to case and docket information from bankruptcy, as well as other courts across the nation.[6] Set up a pay-to-access user account, then search for the target. If the business filed a Chapter 11 claim, you should find a file containing schedules listing: the creditors, the debtor's income streams and expenditures, in addition to the reviewing attorney's case summary and final decision concerning the debtor's application for bankruptcy.

Conclusion

Finish your search by visiting the user friendly site, "Find Lost Money," maintained by the Office of the State Comptroller.[7] You will see an extensive list of businesses as well as individuals who reportedly are owed $15 billion dollars from a variety of sources including unclaimed insurance policy disbursements, tax refunds, and utility company rebates. A business that frequently appears on this list may signal an inattentive managerial style. The information obtained from checking the databases cited can help assess some of the financial risks associated with a tempting business offer.

Sources

[1] *Castle*: "Knockout." May 16, 2012; S04, E23.

[2] appext20.dos.ny.gov/corp_public/corpsearch.entity_search_entry

[3] appext20.dos.ny.gov/pls/ucc_public/web_search.main_frame

[4] The Westchester County Clerk's Office, for instance, is an informative site featuring anonymous searching coupled with a paywall to view scanned documents: westchesterclerk.com/

[5] iapps.courts.state.ny.us/webcivil/ecourtsMain

[6] www.pacer.gov/

[7] www.ny.gov/services/find-lost-money

To the Unknown Hacker

By billk3ls0

I am sitting at a local *2600* meeting, wishing I had no time to write this article. But I am alone, at least for now and physically. So here goes something that feels like throwing a message inside a bottle and into the vast digital ocean.

I started hacking before there were computers at my house. I didn't know it was hacking, I just wanted to know how things worked and how to make them better. Sometimes I would break perfectly good stuff, sometimes I would manage to get things back to work or close.

Later in my early teens back in the 1980s, my father brought a Speccy home (Sinclair ZX Spectrum) and, although I did not have many games to play, I dove headfirst into what would become one of my greatest passions in life. I would spend hours playing games and finding out about cool stuff for a kid, like infinite lives. I tried coding BASIC but found out I needed to use assembly and machine code to dig deeper, get more performance, and save memory. I recall instructions even after years of not coding: 01 03 00 (ld bc, 768), ring a bell?! I liked messing around with code in ROM and coming up with improved code that would allow faster loading of all my programs. I guess I could write a full article just on that experience.

A few years later, I got my first PC. No longer did I have fine control over every aspect on that machine. Modems were becoming standard in this corner of the world and, for the first time, I was able to connect my computer with others. Even a 2400 baud modem was faster than the Speccy loading a game! Terminal mode games were big, and playing *Risk* online with turns taking days was a pleasure.

I continued to code, using QuickBASIC and Pascal for generic applications, like running a video club and keeping track of all the VHS tapes. I didn't know if I would code for a life; I just liked doing it. This helped me during my studies and kept me busy. I learned C, C++, and later some old school languages like COBOL, which are still much used in banking. I also learned other proprietary languages like ABAP to code for SAP and then, with more responsibility, I drifted away from coding and the computing community at large.

This is when Linux got in the picture sometime in 2005, with Fedora Core 5. I rekindled my passion for messing with computers. I started joining IRC chats to provide support every once in a while and using forums to report bugs. I am proud to say that, since then, close family and friends have been using Linux. I love bringing new life to old systems, and sometimes the results are pretty amazing - like using my refurbished Dell Latitude E6230, a 250USD machine that boots to a login screen in six seconds flat. May not seem like much, but it's faster than brand new computers at work. I am not against proprietary software; it's just that I like that you get to decide what is important or not to have.

The next serendipity came while browsing Amazon for some Kindle books and I came across *2600*. This was back in 2011 and it had been years since I had even read a computer magazine on a regular basis. Long gone were the days where I would wait for *Byte Magazine* articles on cool topics. I have been a subscriber of *2600* ever since, mostly as an observer. I love the fact that although computers and technology are a central topic, it puts the focus on hacking no matter what. In my particular case, it also comes in the form of lock picking and human relations, to name a few.

So why am I writing this article now? I guess I want and need other fellow hackers to know a bit more about me. See, I have never joined a *2600* meeting except the ones I started recently here in Portugal. *2600* meetings should be about getting people together, and openly and freely discussing all topics that revolve around hacking. Chatting on irc.2600.net is great fun, but does not replace face-to-face time.

Next time you plan on traveling, why not make Portugal your destination? And if you target first Friday, then I or anyone attending the meeting will most surely have the pleasure to share a beer or whatever fills your cup.

Happy hacking!

Hacking in a Slow Job Market

by Kamonra
kamonra@kamonra.com

Hacking in all its forms is a passion. It takes a thirst for knowledge, the capability to think outside the box, and the ability to persevere regardless of the roadblocks that you come across on your path. Many have made careers out of their passion for hacking - contracted security auditing, web developers, coders, programmers, software engineers, experts in telephony, etc. Many that had a chance to build their careers and succeed are also older - beyond their early-to-mid 20s, tipping towards 30, 40, or perhaps even 50. They're established - they got into the market early and found themselves in stable careers.

So what does the newest generation of hackers do with their passions in a mostly stagnant job market? Many find jobs in fields they aren't exuberant about - perhaps you work physical labor when you'd rather be compiling code, or waiting tables when you'd prefer to be taking systems apart and putting them back together. A lot of us are working jobs below our skill level - just to get by.

However, even if you're not in your dream job, you can make the best of a bad situation by finding work in an area you are at least not miserable in, one that can give you skills that will assist you (and your resume) as you move towards your dream career.

For example, let's say you have an exceptional talent for social engineering and you have the capability of leaving your soul at the coat rack when you clock into work (and trust me, these two skills aren't as common as you would expect). It may not be your career of choice, but you could certainly be employed (and probably excel) as a telemarketer, skip tracer, or first or third party collections. Most companies such as AT&T, Verizon, Comcast, Dish, DirecTV, Frontier, and Sprint offer these jobs in-house as well as through outsourced American call centers across the country. Often these jobs offer a full time position, a living wage, benefits, and a bit of reading time between calls. And since the companies are often competitive over warm bodies (er, I mean agents), they'll try very hard to keep morale up and pander to agents of quality. You also get access to corporate handbooks, which can help you further your education on the systems you may end up using as your career advances.

Or let's say you love to tinker with computers, machinery, or anything else you can take apart and put back together. You probably would enjoy working or shadowing at a small mom-and-pop computer store, motor shop, or lawnmower repair business. Open up the phone book, look up "repair," and flip through the stores. If they're not a chain, there's a good chance they'd be happy to show you around, let you shadow them, or even learn as an apprentice. When I was a teen, I had the opportunity to shadow at a motor shop with a plumber and an electrician, so I've had the luck to collect valuable skills regarding large and small machinery, electrical repair, and fixing the shower and toilet! If it's not a career choice, shadowing can still pay off (even if it's only due to not having to call a repairman to fix the motor in your washing machine).

If you're just a general knowledge collector - one of the few who reads nonfiction books for fun and finds joy in aimlessly surfing Wikipedia - you may find your happiness in a secondhand store or an auction house. Often, the proprietors of these stores and businesses have a passion for the items they sell - from art pieces, dishware, antique furniture and jewelry - each piece has a history and some fun facts to go along with them. I enjoyed a few years at an auction house and it gave me valuable information on the things that came through. (Case in point: don't ever purchase classic Fiestaware in the shade of burnt orange unless you're a collector. It's mildly radioactive.) It's also always helpful to have someone around who knows their way around a computer system - and that makes you doubly useful in these businesses.

You may not be making 80k a year as an independent consultant or own your own security auditing company... but in this downtrodden economy, not everyone will. The least we can do, however, is follow our passion and find a job that makes us happy and challenges us every day - even if our skills are being used in an unorthodox way.

Dev Manny, Information Technology Private Investigator "Hacking the Naked Princess"

Chapter 0x16

"Stop him! Anyone!"

Her scream was so shrill it hurt my ears. I used that pain as motivation to keep running.

The life of an Information Technology Private Investigator is one of action and adventure, heart-pounding action. Or that's what I once told a friendly drunk on the bus about two years ago. The reality of my job description was far less excitement and a lot more Googling.

The wash of adrenaline had kicked my fight-or-flight response into top gear. My pounding heart was a pressure in my chest that was moving up my throat as I ran. Focusing on gasping through each breath, my muscles shook in a scary mix of electrified and weak. My body was at redline.

The point is that since I was racing down the hallway inside RedAction headquarters, with multiple people screaming behind me, and me bouncing off walls trying to escape from an office building I'd just broken into.... Man, I was out of shape.

I chanced a look back and saw the mass of people chasing me, all led by Oober's impostor mom.

At least the plan had worked: P@nic's USB stick was now inside a LAN-connected PC. Her botnet was already attacking this place and had choke-slammed it offline. Hopefully the USB inject was all P@nic needed for her next steps.

All I needed to do was escape.

I turned away from the wave of angry office workers and my face slammed into a concrete pillar that was wearing a hat and utility belt.

I bounced and landed on my back. The concrete pillar leaned towards me - it was the security guard who'd originally seen me enter the building. He'd brought his turkey-sized fists with him, and one of them grabbed me by the shirt and lifted me to my feet. He spun me around and wrenched my arm so high behind my back that my fingers scraped against my neck. I screamed.

He wasn't satisfied because he then threw a Wozniak-sized arm around my neck, and he squeezed. My heart pounded harder as I struggled to breathe.

My vision doubled in front of me. Oober's fake mom stepped out from the wave of business-casual flotsam. My eyes were streaming tears and my head was counting down to an explosion. I tried to blink but couldn't.

Oober's fake mom leaned in, her friendly and vulnerable face suddenly glowering cruel and sharp.

"That's him," she snarled. She looked far up at the security guard behind me. "Take him out."

The guard grunted in acknowledgment and the Wozniak pressure increased. My throat - unable to choke - began to spasm against the pressure.

She leaned even closer, her eyes filling mine as my vision grew blurry.

"Goodbye, Mr. Manny."

My vision flickered and grew dark. I saw her pull back with an odd expression on her face. The vice around my neck had apparently squeezed enough and my vision went black. This wasn't the way I wanted to go. I'd rather have died during the First Attempted Singularity Upload, but my life - while shorter than expected - had at least been interesting.

I fell as the darkness enveloped me.

The screams began.

That was odd. I didn't believe in an after-life. Unless Lovecraft was right after all, I really shouldn't be hearing the wailing of the eternally doomed.

An angel of light flared at the center of my vision. Then another, off to the side. Handheld lights flicked on around the office as people turned on their smartphone flashlights. Black shadows danced on gray walls from a dozen weak LEDs.

From the floor, I saw the mountain of a security guard reaching toward me for a Round Two.

I began to laugh.

"What is this?" Oober's fake mom hissed. She looked down at me. Lit from beneath, her face looked gaunt and haunted. "Tell me right now what -"

"Your Internet's offline," I gasped. "And now the lights are out."

I had hoped P@nic had time to do whatever she was planning. Looks like she had, and she did.

"What," Oober's fake mom breathed above me as I struggled to sit up, emphasizing each word, "do you know about that?"

Since I was laughing in her face, she decided

to kick me in mine. Her black sensible pump wrenched my head to the side and I felt my teeth loosen. I stared at the shadows on the floor as dark liquid dripped from my mouth. I squinted up and grinned into her cell phone flashlight. I could taste the blood staining my teeth.

"She's coming for you," I said, and spat blood onto the floor. "When the lights are out, everyone get ready for P@nic."

Her eyes widened. She looked from me to the mountain range of security guard. She nodded at him.

I again felt the brutal embrace of the Wozniak as it lifted me and squeezed. I gurgled and struggled and my hands felt suddenly heavy and weak. The pressure didn't stop, and the starfield of cell phone flashlights around me flickered, dimmed, and disappeared.

***

The botnet was a world-spanning grid, millions of nodes within nodes, layered, interconnected points of energy blasting information back and forth.

The nodes' energy began to flash in rhythm, to become steadier and more constant. Across the world, nodes within nodes paused, re-oriented, coordinated. Packets exchanged, nanosecond timers synchronized, and the entire botnet - hundreds of thousands of zombie systems - turned to face their target. As one, they screamed at RedAction.

P@nic had taken control, and she'd turned her many tools into a single weapon. Her botnet could not be stopped or ignored.

RedAction was offline, worse than a drunk at the holidays... except for one small trickle of traffic. The USB drive that P@nic had me sneak into the building was a skeleton key, programmed to be ignored by the massive botnet. With that secret path through the botnet blockade, she was able to simultaneously take RedAction offline, and still access and compromise their internal systems.

She'd apparently started with the lighting controls. How long her access would last, I didn't know.

As my consciousness swirled around me, as I tried to determine what was reality or an oxygen-starved fantasy, I forced myself back to consciousness.

I opened my eyes and saw nothing different. The lights were still out. I had no flashlight myself - my cell phone was gone, along with my wallet. With increasing anger, I realized they'd even taken my Leatherman multitool.

I heard no sounds, none of the scramble and screams of people that should be running around in the dark.

There was an odd smell nearby, and it resolved itself into emotion - a pungent sense-memory from my childhood. It was laser-burned polycarbonate and aluminum, from a time when technology was so antiquated we had to physically engrave our data, like cavemen etching into stone.

Is that... a recordable CD?

I reached out blindly and felt around. Yes, there was a whole spool of old CDs. I ran my fingers over the smooth surface, brought them close to smell the faint but unmistakable odor of permanent marker. Important to some admin many years ago, now a bittersweet memory of my first Linux distro.

I sat up in this pitch-dark room. I smelled plastic. Shielded cabling. Spindle motors. Dead power supplies kicking out watts of age and dust.

Crawling and exploring, my blind eyes wide in the darkness, my hands fumbled over boxes, cases, cages, and towers. I gasped as my hands ran over what felt like a TI-99/4A. This place was a museum.... Or a graveyard.

I felt around the ancient tech, marveling at eight-inch floppy drives, some still containing disks with long-forgotten magnetic bytes. I ran eager fingers over old-school monitors, back when they were thirty pound boxes and not flat panels. I found old towers, from when PCs and servers weren't designed for planned obsolescence but for Armageddon. The heavy steel tanks would outlast us all.

RedAction had decided not to kill me yet. Perhaps they realized I was their only immediate connection to P@nic and could be used as a lever against her. Since they weren't with me now, I guessed that whoever was in charge decided it was more important to deal with P@nic's attack than me.

I wasn't supposed to be here. Not part of the plan. I felt the hot burn of embarrassment, of leaving P@nic in the lurch, of saying her name out loud to the wrong people, of getting caught and not being able to help. I felt shame - until I fully realized my situation and RedAction's big mistake.

I was early man being handed a burning torch. I was the Primitive Technology Guy with the R&D already done.

I was an IT private investigator in a room full of tools.

I didn't know how much time I had, but I would take this ancient technology and I would use it to improve my situation and escape from this room.

I got to work.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $200 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

January 18-20
ShmooCon XV
Washington Hilton Hotel
Washington DC
www.shmoocon.org

April 19-22
Easterhegg 2019
Technischen Universität
Vienna, Austria
eh19.easterhegg.eu

May 3-4
THOTCON 0xA
Chicago, Illinois
thotcon.org

May 16-17
Converge
Cobo Hall
Detroit, Michigan
convergeconference.org

May 17-19
Maker Faire Bay Area
San Mateo Event Center
San Mateo, California
www.makerfaire.com

May 17-19
NolaCon
Astor Crowne Plaza
New Orleans, Louisiana
nolacon.com

May 22-23
RVAsec
University Student Commons
Virginia Commonwealth University
Richmond, Virginia
rvasec.com

May 31 - June 2
CircleCityCon 6.0
The Westin
Indianapolis, Indiana
circlecitycon.com

August 8-11
DEF CON 27
Paris, Bally's, Planet Hollywood
Las Vegas, Nevada
www.defcon.org

September 20-22
DerbyCon 9.0
Marriott Louisville
Louisville, Kentucky
www.derbycon.com

September 21-22
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

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

For Sale

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 and Spotify.

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

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.

DEFEND YOUR WI-FI. Coaxifi delivers Wi-Fi over your home's coaxial cabling to eliminate dead zones. Reuse your existing router to send Wi-Fi farther. Check out our new spiral coiled Ethernet cables! 10% off with promo code "SUP2600". coaxifi.com

PORTABLE PENETRATOR. Find WPA WPA2 WPS Wifi Keys Software. Customize reports use for consulting. https://shop.secpoint.com/2600

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

$2 WILL BUY A FORMER ONE-WAY FUNCTION! https://www.amazon.com/Prime-Number-Factors-that-Solve-ebook/dp/B079XYZ596 Prime Number Factors that Solve N = p * q - Kindle edition by Bobby Joe Snyder. Download it once and read it on your Kindle device, PC, phones, or tablets. Use features like bookmarks, note taking, and highlighting while reading Prime Number Factors that Solve N = p * q.

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

HOW CAN WE ENJOY OUR PRIVACY when everything has a GPS tracking device attached to it? We want the Big Brothers to stop tracking us everywhere we go. We shall disarm all GPS systems from all of our toys. We must learn how to disconnect the GPS devices through our brothers and sisters in the hacker world, whether we are amateur or professional hackers. We must regain our privacy. Is there a way that we can disarm the GPS system without destroying or harming our merchandise (toys)? Seeking assistant on the GPS network. All are welcome to directly write to me: Mu'mit Muhammad, PO Box 945, Marienville, PA 16239.

JOIN THE HTTPS://CODEFOR.CASH community and earn money with freelance programming jobs. All hats welcome!

Announcements

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1030 products listed which include 220 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.

AUSTIN HACKERSPACE: A shared workshop with electronics lab, laser cutters, 3D printers, CNC machines, car bay, woodworking, and more! $60/mo for 24/7 access to all this and a great community as well. Open House and open meetups weekly. 9701 Dessau Rd, Austin, TX http://atxhs.org/

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

Services

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@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472.

PANIC STATION is a quarterly zine put out directly from prison that focuses on original writing, hacking, music, punk rock life, and prison shenanigans. *2600* readers can request a free issue by writing a letter to me. Submissions welcome, please only send letters (no stamps, etc.)! Vincent Veneziani, #249067G/1079583, 215 S. Burlington Rd. - SWSP, Bridgeton, NJ 08302.

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. 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 recover data nationwide from many sources, including computers, external media, tablets, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation

of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Our principals are co-authors of *Locked Down: Practical Information Security for Lawyers*, *2nd edition* (American Bar Association 2016), *Encryption Made Simple for Lawyers* (American Bar Association 2015), and hundreds of articles on digital forensics and an award-winning blog on electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

ASPIRING TO BE THE MOST ETHICAL TECH SHOP IN THE WORLD, Technoethical.com offers the largest catalog of hardware products certified by the Free Software Foundation (FSF) to Respect Your Freedom (RYF) [fsf.org/resources/hw/endorsement/technoethical]. As a user of Technoethical devices, you have the maximum control over your computing, being able to use, copy, modify, and distribute all the bits in the operating system and, when possible, even at lower levels, such as the boot firmware. The shop sells laptops and servers pre-installed with a fully free (as in freedom) BIOS replacement and GNU/Linux-libre distributions verified and endorsed by the FSF. All x86_64 devices serviced and sold have Intel's intentional backdoor, the Management Engine [u.fsf.org/2g0], completely removed. As the only shop that sells phones with Replicant [replicant.us] pre-installed, you can be the first hacker on your block to own an Android-based device with an operating system that can be compiled completely from source with no proprietary blobs. You can also buy from Technoethical a diverse array of WiFi adapters that work with drivers and firmware that are fully hackable and operate also in the Access Point mode. Moreover, Technoethical provides installation/liberation services for all computers that are also sold as products. You can ship your compatible computer to Technoethical, or ask the team to organize a workshop in your local hackerspace or free software event. With 4 years of experience on the market, Technoethical is operated by a geographically distributed team of hackers from North America, the European Union, Russia, and Australia that closely follow the software freedom principles of the GNU project. Use the coupon code 2600MAG to receive a 5% discount on all Technoethical products. Order today and join Richard Stallman among the many happy customers of Technoethical!

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

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. We have an increasing amount of digital download capability for the magazine and for HOPE videos. Best of all, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

INTELLIGENT HACKERS UNIX SHELL: Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted in Chicago with Filtered DoS Protection. Multiple Dual Core FreeBSD servers. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon Code: Save2600. http://www.reverse.net/

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

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

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!

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).

Personals

PENPALS: Seeking interesting tech/hacker friends to write. I'm 29 years old and from Cleveland, Ohio, but currently stuck in prison. Before the Feds kidnapped me, I worked network operations for an ISP/telco. Being out of tech for so long, I'm starting to feel antiquated; there's no Internet access here and hardly any resources to keep up. I have many other interests too, including general aviation, health/fitness, snowboarding, travel/foreign cultures, etc. I'd be happy to share the many crazy stories of what really happens in prison. Anyone international? Europeans? Deutschen? Do NOT use address labels or stickers; it will be rejected/returned. Looking forward to your letters: Dan Nieberding 61030-060, Federal Correctional Institution, PO Box 1000, Loretto, PA 15940, United States of America.

PENPALS WANTED: Fellow hackers! I'm incarcerated and need someone to keep me in touch and fresh on the hacking scene. The library here is horrific at best with absolutely no resources for my interests. With less than a year before my release, I am looking for someone to bounce ideas off of, ask questions, and talk about common interests with. I am from Dallas, TX and will be there when released. I have been looking into Bitcoin & mining. I also have fascinations with the dark web, methods, and carding. I LOVE GLITCHES!!! Please reach out to a fellow hacker before my release. I am determined to surround myself with like minds. Please don't send books! I can't get them unless they come directly from the publisher or bookstore (amazon.com and online stores are okay). Any & all financial direction and/or suggestions are greatly appreciated. If you know of ways for me to start an income once I'm released, please, please, PLEASE let me know! Just write me if any of this catches your attention or if you want to know more about me. R. Murphy #2148621, 6999 Retrieve Rd., Angleton, TX 77515.

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

Deadline for Spring issue: 2/21/19.

WRITERS NEEDED!

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

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

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

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

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

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.

2019 HACKER CALENDARS

The 2019 Hacker Calendar is out and in full operation!

Each month features a 12"x12" glossy photo of a public telephone from somewhere on the planet, and nearly every day marks something significant in the hacker world.

Get yours today! Visit store.2600.com

"I hope you understand, this is not how I meant for things to go, and I apologize for any harm done as a result of my neglect to consider how quickly the site would spread and its consequences thereafter... I definitely see how my intentions could be seen in the wrong light." - Mark Zuckerberg regarding his FaceMash project in 2003. We're sensing a trend.

Inspirational Music: Trigone, Focus, Donner Party, Pilote, Jesse Winchester, Willie Nelson, Anti-Nowhere League, Barbara Lea

Shout Outs: Logia Tattoo, Fran Ruina, Pickles & Violet, Alexandria Ocasio-Cortez, the InSight team, Strand

***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.
2000-2017 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, first table to the left of the front door.
Parana: One Love Bar, Cervantes 384. 8 pm
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499, Capital Federal. 7 pm

AUSTRALIA

Central Coast: Central Coast Leagues Club (ground floor, outdoor area). 6 pm
Melbourne: The Crafty Squire, 127 Russell St.
Sydney: Metropolitan Hotel, 1 Bridge St. 6 pm

BELGIUM

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

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm
Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.
Vancouver: International Village Mall food court.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Newfoundland

St. John's: Memorial University Center food court (in front of the Dairy Queen).

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm
Toronto: Free Times Cafe, College and Spadina.
Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

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

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECHIA

Prague: Legenda pub. 6 pm

DENMARK

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

FINLAND

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

FRANCE

Paris: Burger King, first floor, Place de la Republique. 6 pm

GREECE

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

IRELAND

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

ISRAEL

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

KAZAKHSTAN

Astana: CheckPoint Brasserie, Koshkarbayeva St 34. 8 pm

MEXICO

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

NETHERLANDS

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

NORWAY

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

PERU

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

PHILIPPINES

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

POLAND

Krakow: VRCafe, Dolnych Mlynow 10. 8 pm

PORTUGAL

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

RUSSIA

Moscow: RNDM, Podkopayevskiy Pereulok, 7. 7 pm
Murmansk: Teplo, Teatralny Bulvar, 6**.** 7 pm
Petrozavodsk: "Good Place" anti-cafe, pr. Pervomayskiy, 2. 7 pm
Saint Petersburg: Krasnodonskaya Ulitsa, 4. 7 pm

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

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

THAILAND

Bangkok: The Connection Seminar Center. 6:30 pm

UNITED KINGDOM

England

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

Scotland

Edinburgh: Beehive Inn on Grassmarket. 6 pm
Glasgow: Starbucks, 9 Exchange Pl. 6 pm

Wales

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

UNITED STATES

Alabama

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

Arizona

Phoenix: Lux Central, 4400 N Central Ave. 6 pm
Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

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

California

Anaheim (Fullerton): 23b Shop, 418 E Commonwealth Ave (behind Pizza Hut). 7 pm
Chico: Idea Fab Labs. 7 pm
Los Angeles: Union Station, inside main entrance (Alameda St side) near the Traxx Bar. 6 pm
Monterey: East Village Coffee Lounge. 5:30 pm
Petaluma: Starbucks, 125 Petaluma Blvd N. 6 pm
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Center near street level fountains. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Fort Collins: Dazbog Coffee, 2733 Council Tree Ave. 7 pm

Delaware

Newark: Barnes and Nobles cafe area**,** Christiana Mall**.**

Florida

Fort Lauderdale: Grind Coffee Project, 599 SW 2nd Ave. 7 pm
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm
Jacksonville: Kickbacks Gastropub, 910 King St. 6:30 pm
Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm
Sebring: Lakeshore Mall food court, next to payphones. 6 pm
Tampa: Cafe at Barnes & Noble, 213 N Dale Mabry Hwy
Titusville: Crescent Coffee Company**,** 311 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance.
Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

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

Indiana

Bloomington: Barnes & Noble cafe, 2813 E 3rd St.
Evansville: Barnes & Noble cafe at 624 S Green River Rd.
Indianapolis: The Tomlinson Tap Room in City Market.
West Lafayette: Jake's Roadhouse, 135 S Chauncey Ave.

Iowa

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

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm
Grand Rapids: Schmohz Brewing, 2600 Patterson Ave SE. 7 pm

Minnesota

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

Missouri

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

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

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

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St**.**

New York

Albany: Starbucks, 1244 Western Ave. 6 pm
New York: The Atrium at 875, 53rd St & 3rd Ave, lower level.
Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm
Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center)**.**
Raleigh: Morning Times, 10 E Hargett St. 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm
Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd.
Columbus: Front of the food court fountain in Easton Mall. 7 pm
Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.
Youngstown (Niles): 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 first floor.
Trujillo Alto: The Office Irish Pub. 7:30 pm

South Carolina

Myrtle Beach: SubProto, 3926 Wesley St, Suite 403**.**

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm
Nashville: Nashville Software School, 500 Interstate Blvd S #300. 6 pm

Texas

Addison: Dunn Brothers Coffee, 3725 Belt Line Rd.
Austin: Whole Foods 2nd floor pavilion, 525 N Lamar Blvd. 7 pm
Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm
Houston: Ninfa's Express seating area, Galleria IV. 6 pm
Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

Burlington: The Burlington Town Center Mall food court under the stairs.

Virginia

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm
Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm
Lexington: Collaboratory**,** 18 East Nelson St, #103. 6 pm
Reston: Refraction, 11911 Freedom Dr. 8th Fl. 7 pm
Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Washington

Seattle: Cafe Allegro, upstairs, 4214 University Way NE (alley entrance). 6 pm
Spokane: Starbucks, 4727 N Division St.
Tacoma: Tacoma Mall food court. 6 pm
Wenatchee: Badger Mountain Brewing, 1 Orondo Ave.

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

URUGUAY

Montevideo: MAM Mercado Agricola de Montevideo**,** Jose L. Terra 2220**,** Choperia Mastra. 7 pm

All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle!

Payphones with Cards

Italy. This little yellow phone was found at the Basilica of Saint Paul Outside the Walls (yes, that's the actual name) in Rome. There was no dial tone.

Photo by Matthew H M

Ukraine. It looks like this poor card phone has been through hell, but it somehow seems to have survived in the streets of Odessa.

Photo by Jason Lenny

Croatia. Seen in Sabunike, this is about as colorful a model as we could have hoped to find. It looks like a natural part of the landscape, as all phones should. Coins are not welcome here.

Photo by Ivan Sabljak

China. There's something about the way this phone stares at you that makes you think it knows a lot more than it's letting on. Spotted in Suzhou, home of the "Leaning Tower of China."

Photo by Sam Pursglove

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

The Back Cover Photos

Congrats to **Jean-Philippe** for discovering our secret phreaking center facility in the heart of Quebec City. It's especially cool that this building is host to something called TelOps, complete with a weird looking eye. We'd probably have lots of fun here.

Oh *hell* yeah. We always heard rumors of a school like this, where hackers are trained at an early age and then sent into the world to be creative and cause all kinds of mayhem. But this is the first actual sighting of the prophecy, found by **Kenneth Hensley** in Mountain Home, Idaho.

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.