Volume Thirty-Nine, Number Four
DIGITAL EDITION

2600

The Hacker Quarterly

Foreign Payphones

Brunei. Half of a pair found in an empty parking lot next to the Royal Regalia Museum in Bandar Seri Begawan, this phone is only set up for calling cards. You can see the old JTB logo on the sign above. The newer TelBru logo can be seen on the sides of the kiosk. There's no sign of the current name, which is Imagine.

Photo by Sam Pursglove

South Korea. Seen in the countryside town of Suncheon, also half of a pair, both of which were fully operational. This close-up view shows how both coins and cards are accepted. Operated by KT, formerly Korea Telecom.

Photo by Nara

Australia. This phone is located at the Waurn Ponds Shopping Centre in Geelong, Victoria. Unlike most payphone companies, Telstra has made their phones completely free for calls within the country. (You can see how someone has scratched off the "pay" part of "payphone.")

Photo by DarkLight

Canada. Spotted at the Northern Store in the remote community of Churchill, Manitoba. Pressing the button gets you a free call to the local taxi company. (We don't know what happened on October 1st.)

Photo by TProphet

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 (Do not send us links as photos must be previously unpublished.)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

Interpretations

Inconvenient Truths

These last few years have been difficult for all of us on so many levels. And we keep thinking we're almost at the end of it when more bad stuff happens. Sometimes it's directly related to the pandemic; other times it's something entirely new. What helps to get us through is support from those around us and fresh ideas on how to tackle these challenges.

As we approach our 40th year, things look especially daunting for us. We've been through hard times before, whether it was another distributor making off with half a year's income, lawsuits from some of the most powerful entities on earth, or unjust and inhumane government prosecutions of those close to us. But what we're facing now is probably the biggest threat we've ever had to our continued existence.

Being a printed magazine has been especially difficult for a couple of decades now. Being one that takes no advertising made that challenge even greater. We saw independent bookstores forced out of business by big chains. And then those big chains went out of business, leaving nothing in their place.

COVID-19 made all of this even worse since lots of the issues we had already printed never made it to the newsstands because they weren't open. And many of them never reopened. Even though people were looking for our magazine, there were significantly less places to find it.

In 2022, things got even worse as the price of paper skyrocketed, which made our profit margin practically nonexistent while inflation drove prices for almost everything else upwards. It hasn't exactly been a cheery time.

One bright spot in all of this has been our Kindle edition, where sales were significant since its launch in 2010. This digital platform offered another way to get *2600* into subscriber hands without the cost of printing. But as we go to press with this issue, we've been informed that Amazon has decided to discontinue magazine subscriptions on the Kindle, except for the biggest mainstream publications. We can't say we're surprised - we always warn our readers about letting big companies call the shots. But this was a case where we were able to reach a great number of people in a convenient manner and it really helped offset the printing expenses, even after Amazon took their cut. This loss couldn't have come at a worse time.

But there is hope. Literally. The last few HOPE conferences have been able to help support the magazine and keep things from becoming too dire. Of course, COVID threw a monkey wrench into that as well when we weren't able to hold an in-person conference in 2020 and were forced to limit attendance in 2022 due to health concerns. Ironically, in 2019 we had thought our biggest challenge would be finding a new home after losing the Hotel Pennsylvania. We had no idea what we were all in for.

Happily, the most recent conference at St. John's University went better than we had ever hoped. We are extremely fortunate to be able to continue and build future conferences in such a venue. But, because of the fact that we had to make things smaller due to the pandemic, we didn't wind up where we needed to be in order to help support *2600*. The timing was just really bad, which seems to be a recurring theme lately.

So how bad are things? They're bad, no question. Those of us who can afford not to get paid haven't been for the past few months. We love what we do and we will make many personal sacrifices if it means that we get to stick around and do this for longer. We may have to make difficult decisions down the road, but we're really hoping to stave that off with the help of the community.

Here's where things can turn around.

We have a great biennial event with the HOPE conference. If we're able to get 1500 in-person attendees and 1000 online attendees each time, most of these problems will vanish. Note that the in-person number is actually less than what it was in past years because we don't want to recreate the overcrowding that occurred back then, even though we have much

more space now. Offsetting that decrease with paid online attendees who participate digitally could add a great deal to the conference, with more participation from all over the world. (We're also not opposed to growing into a bigger in-person crowd in future years as we use more facilities.)

There has even been talk of making the conference an annual event due to how smoothly it went this last time. We won't know if that's doable until we see how the next one goes, but if we are able to reach that stage without overworking ourselves to death, then we will be on very solid ground indefinitely.

But we're more than a year away from knowing if this will be sustainable. 2023 is going to be a pivotal year and we need to come up with more immediate solutions to help get us through all of the challenges that are being flung at us.

Ideally, *2600* should be self-sustaining. While this has become quite difficult with the cost of printing and the shrinking number of retail outlets, it's not impossible. The one thing readers seem to be most adamant about is the continuation of the printed edition. We believe following the trend of many magazines and only having digital editions would be a big mistake for us. People value the physical copies and those tend to live forever. It's a true gift to be able to do this year after year and we really don't want to give it up. But we need to make some serious progress if that's going to happen.

We don't see a way to get *2600* into more retail outlets if there simply aren't any more of them. We experimented with supermarkets during the pandemic and it was a disaster. (Apparently, grocery shoppers aren't interested in magazines about hacking. We know this now.) The loss of so many bookstores, especially the independents but also the chains, has hurt our entire society and we're now living through yet another consequence of that.

More physical subscribers would certainly be a good thing, but due to the volatile costs of printing, packaging, and shipping, it's not really an economic boon for us. What really would make a difference at this point is a dramatic upturn in digital sales. We would need around 3500 digital subscribers to offset the losses from Amazon alone. And since Amazon won't share the subscriber info with us, the only way for us to reach our current Kindle subscribers is through the words in the magazine itself. We hope they're all able to see this and to act upon it. But again, that only addresses the Amazon problem. We still need to add more subscribers to help address the shortfalls brought about by everything else described above.

We believe this is doable, as there are so many people who react with amazement and enthusiasm when discovering that we are in fact still around. Since we don't advertise and since so many establishments where we were displayed have disappeared, it's very easy to lose track of our existence. The entire zine community has been hit with this reality and we're one of the few survivors, which is a painful reality for us. Assuming we make it through this latest crisis, we intend to do everything we can to help other independent publications find new visibility.

At press time, we're still trying to put together a digital subscription option that works the way we want it to. We've actually been trying to do this for years, but have run into software that insists on using DRM (copy control which we do *not* want) or that doesn't know how to generate unique URLs for subscribers. It's annoying, but we're determined to solve this. Hopefully, by the time you read this, we will have.

But what really comforts us is knowing that hacker ingenuity is on our side. There are people reading this now who have ideas that we've never thought of which will prove immensely helpful. The power of the hacker mind, determined to accomplish that which they have been told is impossible, is our greatest ally here and one which we believe will help us solve problems and get the word out.

We've accomplished so much over the past four decades. It's always been a bit of a struggle. But we truly believe we're the right people in the right place at the right time to take on this challenge. While the reality at the moment isn't what we'd prefer, we're convinced we have the power, ability, and intelligence to change that reality into something a little better.

We're ready for the next chapter.

You Can Use the Dark Web for Good

by Djilpmh Pi

One of my earliest memories of trying to figure out how things work and what makes them tick is when I was nine or 10 years old and my parents left me alone in the house. I took a dinner knife and disassembled the Big Ben mechanical alarm clock. It had two windup handles, one to wind the spring to keep the clock running, and the other for the bell clapper. Very cleverly the "quiet alarm" mode had a lever that slipped a thin piece of leather between the clapper and the bell housing so it was not as annoying as a full on alarm. I could see the gears and levers spin and slide; it was wonderful. It kept working even though I had a few parts left over which I could not remember where they were supposed to go back. I only got into trouble the second time I took the clock apart into more pieces, and it no longer tick-tocked. No matter, figuring out how things worked was in my blood, and this hacker never looked back even after my spanking.

Today my Big Ben is to figure out and explain to people how the Dark Web can be put to legitimate and beneficial uses. For too long, it has been yielded to the "dark side" for evil purposes. It is, after all, only a technology and, on its own, tech is not inherently good or evil. Whether something is good or bad should be judged by the motivation of our actions and the harmful or helpful outcomes.

Everybody Knows the Dark Web is a Bad Place

The Dark Web is well known as a playground and hiding place for criminals including drug dealers, sex traffickers, and every kind of bad people. It is painted by popular media as the dark alley everyone should avoid because you will get mugged and worse if you go there. Taking a closer look, it is a powerful tool that can be used for good in spite of its evil reputation.

The U.S. Navy created the technology behind the Dark Web initially to protect American spies in hostile locations. See `en.wikipedia.org/➥wiki/Tor_(network)` for its origins.

Power Tools Have Two Sharp Edges

Power tools and power concepts are two-edged swords: free speech protects hateful speech, anonymity protects privacy but encourages trolls, and airplanes can be used by terrorists to take down high rise buildings. Unintended consequences and uses are the second sharp edge of powerful ideas.

If we say that "good honest people" should stay away from that dirty Dark Web because icky bad people use it, we could also say that criminals use guns, cash, and cars, so honest folk should not use those icky things - who knows where it's been! You have to decide whether the good honest police should use guns or just stick to the billy clubs for law enforcement. Oh wait, criminals use sticks too. As with any power tool, the Dark Web can be used for both good and evil. Unfortunately, its legitimate use by honest people has been overshadowed by its icky reputation.

Good Honest People Can Benefit

Good honest people who don't want their network activity to be tracked, victims of domestic violence, and whistleblowers can all benefit from using the Dark Web.

Anyone who is interested in privacy can use the Dark Web to protect their personal information. These uses will be explained below. Having a basic understanding of the Dark Web, or Tor (the technical name is "the onion router") can be helpful to understand how and why it works. Recognizing the imitations of the Tor software is as important as understanding its power. For an explanation and resources see `torproject.➥org`.

Use Cases for Dark Web (Tor)

These are my hacks of the Dark Web, figuring out how to use it for the benefit of honest people in these ways:

1. Avoiding tracking: protecting the privacy of your Internet use
2. Protecting the location of victims of domestic violence
3. Protecting anonymous whistleblowers

Standard Disclaimer

Seek professional advice and talk with people you trust. You are responsible for your own actions. Be skeptical and verify anything important.

Tracking and Privacy

Tracking collects information about your Internet use, what you search for, what you buy, and what time of day or night you use the Internet. That information is sold to advertisers who pay very well for that information. If you don't already think it's creepy and invasive, you've missed something basic about intrusions into your privacy.

What Google Knows About You

We've all observed that a random Google search for vacations in Glacier National Park will shortly generate advertisements for tour packages and hotels in the area. The simple explanation is that your free use of the search engine has tagged you as someone who is interested in the area, and that information is sold to the hotels and tour providers around Glacier. Early in the use of tracking and advertising, a parent discovered

their daughter was pregnant because diaper and maternity ads started to appear in the browser and computer used by the family.

Defeating tracking of your every action can feel insurmountable. Corporations already know every intimate detail of your life: what ice cream flavors and brands you like, whether you use ice cream as a celebration or consolation. It's creepy to know that complete strangers - not even limited to your country of citizenship or residence - know everything you buy and read, and at what time of night and which days you like to shop. It should be annoying to people that a website already knows your "consumer score" to set your place in the helpdesk queue and probably to decide what deals to offer you, individually. See `sift.com` and `nextroll.com` for examples.

Private Browsing

To remove tracking of your web searches, it's possible to use a private search engine such as DuckDuckGo or StartPage. Both proxy your search request, so your IP address is initially protected and cookies are not passed through. But if you click on the search result directly, your computer can become visible to both the service provider and the website unless you are careful to use the "Anonymous View" link in StartPage.

Without using "Anonymous View," DuckDuckGo or other search engines connect you directly to a website and your IP address, cookies, and other tracking mechanisms kick right back into action.

If you use a VPN, your real IP address is masked by the VPN provider, but you have to trust them to keep that information private, and VPNs don't do anything to protect you against cookies and other tracking methods.

What If You Had Some Friends...

Defeating tracking can actually be easy. What if you had a group of friends help each other by randomly mixing the traffic up among the members of the group, so it's no longer clear who was shopping for cars, a particular medication, or pregnancy tests? Those searches and connections would be randomly changed and no longer linked to your individual identity. You still have to deal with cookies and other tracking, but your location information is no longer usable to track you.

If your group of friends were distributed all over the world in many countries, that would fool some websites nicely.

Randomizing Internet Connections to Defeat Tracking by IP Address

That group of cooperating friends who allowed you to use their shared Internet connections could make the IP address detected by the Internet web server or store different for each visit. If there were hundreds, or even thousands of these friends, that would confuse the tracking tools to the point they wouldn't know your real IP address or location.

Your New Friends

This is my first hack of the Dark Web. Let me introduce you to your new friends: a group of people who volunteer to do just that for you, for free, because they all believe in and support privacy. Surprise! They operate the Tor (the onion router) relay computers that make up the Dark Web.

Tor is the technical name of the Dark Web, and its only purpose is to hide your real location by passing your traffic through a series of friendly relay routers between your computer and the website you are accessing. Tor does nothing else. But even that little help from your new friends can do a lot to defeat tracking.

Protecting Victims of Domestic Abuse

Some victims of domestic abuse leave town for fear of their safety and for their lives. It is most important to keep their location secret from their abuser.

Finding Someone's Location

If the attacker finds an email that was sent by the victim to family or friends telling them all is well, it is trivially simple to find the IP address from which that email is sent. As explained in `www.lifewire.com/how-to-find-➥email-server-ip-address-818402`, this method can be used to check the authenticity of an email message, or flag it as suspicious in origin. If your cousin lives across town, why are they sending email from Norway?

Sadly, the same method can be used by an attacker to find the location of their victim. Geographic location is used by website and online store owners to validate the physical location of a potential visitor or buyer, so if an order is connecting from France, it would be inconsistent to have the item sent to Iowa, or vice versa. At least it would be worth getting additional verification that the purchase is legitimate. A diligent website owner could use geolocation to reduce fraud. Another example would be comments on a political activity website of users claiming to be local residents that are traced to geolocations in Eastern Europe or Far East. `www.➥iplocation.net/` and `en.utrace.➥de/` are examples of many free online services providing the physical location of an IP address.

Protect Victims From Real Harm

If a victim left town to escape an abuser, revealing even the town or suburb of their current location has made all the effort a waste of money, time, and energy. Such exposure puts victims in real harm's way.

My second hack of the Dark Web is this: using Tails or at least a Tor browser can keep the IP address of the sender private and protect the real location of the victim. Of course, if the email contents describe an address, no technical

solutions will protect against sloppiness of their security.

The best strategy would be to completely isolate from previous contact with family and friends, but that discipline can be hard to keep forever, particularly during significant times such as holidays, family births and deaths, or birthdays. If communications were attempted, at least try to avoid leaking the location of the victim.

Protecting Whistleblowers

Whistleblowers protect our democratic society by shining a spotlight on evil. They are an essential part of revealing abuse of power, avoidance of responsibility, and other things that destroy the civilized part of our modern society. By revealing information about such abuses, they put themselves at great risk of reprisal (snitches get stitches, rats get bats), so it can be helpful if a whistleblower can remain anonymous. Any accusation has to be proven to be true or false by investigation and other information and testimony: that is the responsible action of a conscientious citizen.

If you came into possession of some documents or information that proved illegal, immoral, or unethical behavior of powerful people, what would you do? Many people think twice about being identified as the source because they correctly fear the anger and reprisal of those powerful people and their unthinking followers. This is the case whether the issue is in your neighborhood, in government, or in a large corporation.

It's Hard to Be Anonymous

It is very hard to be an anonymous whistleblower. Conventional email contains the IP address (and thus location) of the sender's computer. What would you have to do? First, get a wad of cash: credit cards and checks will be traced back to you. Pay someone - preferably a stranger or homeless person - to buy a smartphone or laptop from a pawn shop or used computer store. If you enter the store yourself, you will be on the surveillance video for the store. Use your device outside the library and use their Wi-Fi out of view of the surveillance cameras.

Is that enough? Probably not. But it's a good start. What is a better way? Use the Dark Web, in the same way American spies communicated with their home team.

Better to Use Tor (the Dark Web)

If you use the Dark Web and avoid the known pitfalls, you can be as anonymous as it is possible to be today. Tails is a USB-based operating system that boots from the USB drive and does not touch the host computer's hard drive, and leaves no footprint revealing that you were even on the computer. Tails can be obtained through `tails.boum.org/` and is free. It is the method recommended by news organizations worldwide for submitting tip information anonymously.

This is my third hack of the Dark Web: helping whistleblowers stay anonymous if they wish.

Media Outlets Use SecureDrop

SecureDrop is Dark Web software that allows whistleblowers to send information to news outlets and exchange messages between the whistleblower and the journalist. Many global news and other organizations use it - the list is found at `securedrop.org/`.

Thorns and Roses

The sweet smell of roses in the world of privacy comes with its own thorns.

Removing tracking from your Internet use by using Tor does give you better privacy. But it can be inconvenient. Because Tor relays are spread out over the world, you might see a French language landing page because the last relay was in a French speaking country. Web pages take more time to load because all the traffic is passing through several additional routers instead of going straight between your browser and the web server.

Loss of discipline in correctly using Tor can leak your anonymity; for example, if you give your real identity to a website.

It's Still Worth It

In spite of these drawbacks, it is necessary and important to support the use of Tor in the protection of everyone's privacy.

Private communications are essential for resistors under oppressive regimes. Syrians fighting Assad cannot use ordinary email systems; they would be found out in no time. Iranians organizing resistance to their government would be wise not to use conventional messaging tools offered by local companies.

Just as free speech is important to a free society, it allows some to express hateful ideas. In the same way, privacy can be used by good people and abused by bad ones. But in the end, the value of free speech is higher than what it allows, and the value of privacy is higher than what the abusers can make of it.

Degradation as DRM

by Nikolaos Tsapakis

Information available is for educational purposes only, views expressed are my own and do not necessarily reflect those of my employer.

Long time ago, while I was searching for interesting Digital Rights Management systems on games, I came across FADE[1]. The protection allows the player to use the game normally. Then it gradually degrades certain game features over time, like decreasing the accuracy of the player's weapons, eventually rendering it unplayable. It seemed to me like an interesting exercise to introduce a similar custom protection as a binary patch in a game. I selected *LZDoom* [2]. After downloading, you need to place a .wad[3] file inside the main game directory in order to start the game.

The idea is to drop the game frame rate on a computer which is different than the game owner's computer based on an event. That event is the player typing the "idkfa" cheat string during game play. A different computer is been detected by the CPUID[4] instruction. That hardware check is not very strict, but I believe it is fine for the purposes of the current article. In order to discover which game code triggers on player cheat string input, I started the game and entered "idkfa", then noticed the string "Very Happy Ammo Added" on top of the screen. Break pointing for read access on that particular string pauses game execution on code which gets executed in an event of a player cheat string input. For dropping the game frame rate, I found the game's main loop and introduced a delay. Delay may be introduced in different places inside the game's main loop.

The file for binary patching is `lzdoom.exe` having an MD5 value of `61a2cd931fd➥3aaaae976e4131c512728`. Binary analysis and patching was done using x64dbg[5]. Running tests between two different computers was done using a physical and a virtual machine on VBox. Following are the patches, description, and file raw offsets to patch. You may use any hex Eeditor to apply the patches.

patch_1:

```
; file offset 0x281FD6
;  goto  patch_2  player  cheat
➥string input event check
E9290F4500  jmp  lzdoom_____
➥prot.patch_2
90 nop
continue_2  :  <original  game
➥instructions>
```

patch_2:

```
; file offset 0x6D2F04
; save original registers
50 push rax
66:9C pushf
; rax points to cheat string
; compare string with "Very"
813856657279  cmp  dword  ptr
➥ds:[rax],0x79726556
;  if  no  string  matches  then
➥continue game
75  0F  jne  lzdoom_____prot.
➥continue_1
; if string matches then get delta
E8  00000000  call  lzdoom_____
➥prot.delta
delta:
58 pop rax
;  rax  points  at  the  end  of  data
➥section
48:05 DC745700 add rax, 0x5774DC
; set flag for later h/w check
C600 01 mov byte ptr ds:[rax],1
; restore original registers
continue_1:
66:9D popf
58 pop rax
;  execute  stolen  code  due  to
➥patch_1
48:8BF8 mov rdi,rax
48:85FF test rdi,rdi
; continue game
E9  AFF0BAFF  jmp  lzdoom_____
➥prot.continue_2
```

patch_3:

```
; file offset 0x253C0
; go to patch_4 hardware check
E9  67DB6A00  jmp  lzdoom_____
➥prot.patch_4
90 nop
90 nop
90 nop
90 nop
continue_4:  <original  game
➥instructions>
```

patch_4:

```
; file offset 0x6D2F2C
; save original registers
66:9C pushf
50 push rax
53 push rbx
51 push rcx
```

```
52 push rdx
E8 00000000 call lzdoom _ _ _ _ _
➥prot.delta _ 2
delta _ 2:
58 pop rax
48:05 B9745700 add rax,0x5774B9
; check if flag set by cheat string
➥check
; If not set then continue game
➥else check h/w
; processor info and feature bits
8038 01 cmp byte ptr ds:[rax],1
75 17 jne lzdoom _ _ _ _ _ prot.
➥continue _ 3
48:33C0 xor rax,rax
48:FFC0 inc rax
0FA2 cpuid
; If h/w check fails introduce
➥frame delay
81F9 0322989E cmp ecx,0x9E982203
74 07 je lzdoom _ _ _ _ _ prot.
➥continue _ 3
B9 00101101 mov ecx,0x1111000
frame _ drop:
E2 FE loop lzdoom _ _ _ _ _ prot.
➥frame _ drop
; restore original registers,
➥execute stolen
; code due to patch _ 3 and continue
➥game
continue _ 3:
5A pop rdx
59 pop rcx
5B pop rbx
58 pop rax
66:9D popf
57 push rdi ; stolen code
48:81EC 80000000 sub rsp,0x80 ;
➥stolen code
E9 5C2495FF jmp lzdoom _ _ _ _ _
➥prot.continue _ 4
```

[1] forum.exetools.com/showthread.
➥php?t=13232
[2] github.com/drfrag666/gzdoom/
➥releases/download/3.87b/
➥LZDoom _ 3.87b _ x64.zip
[3] github.com/Akbar30Bill/DOOM _ wads
[4] en.wikipedia.org/wiki/CPUID
[5] x64dbg.com

by Oscar T. Grouch

We Love Trash

This is a tale of caution. Most all of you hacker-types reading this already know to always wipe any old hard disk before disposal - ideally, multi-pass drive wipes follow by partitioning as a LUKS volume with drive encryption. These baselines are out of scope for this article, to tell you the real story.

When I found this data on the Windows trashed laptop, I wrote my findings in a notebook, then multi-pass wiped the laptop disk. These files were not even deleted, so no NTFS recovery needed to review drive contents.

Enter the Dragon

This tale starts by my walking home from working in a major metropolitan city near the East Coast. Walking along, I saw a trash management employee giving someone else a laptop.

I went over to learn more. Talking to the sanitation workers, they told me people throw away multiple laptops all the time. They noted seeing a dozen laptops a week in the trash, easily. I struck up a conversation and was given a free 17 inch HP laptop running Windows 7 with a dead laptop battery. Two minutes later as I loaded lappy into my backpack, they found a matching power supply. I added that into my bag.

Game On! Time to go home and check this out!

I got home, grabbed one of my favorite Linux Live USB sticks (Ubuntu, Kali, Tails, TempleOS, Hannah Montana Linux).

Once booted up, your favorite hacker mounted the Windows volume, then browsed the "C:\Users\%username%" folder.

These details are facts I obtained. I was so stunned that I called my wife over to confirm this event was real. This is the story of a restaurant with zero data integrity.

The disk was reviewed and wiped in September 2019 (pre-COVID - the world seemed so simple then).

The Goods

I recognized the company name. I ate dinner there a few months ago and laughed

when I recalled why the place sounded familiar.

On the desktop, files of note:

- `check.jpg`: The back of a signed check. Front account and routing numbers visible.
- `HVAC.pdf`: Floor plan for HVAC install.
- `Desktop\Drawings`: Building plans, high definition AutoCAD design files, building engineering documents.
- `Desktop\Employee Documents`: Current and past employee info, full names, driver licenses, scanned copies of Social Security cards, W4, I9, and direct deposit forms.

The archive data went from 2015 to February 2018. Digging more, this laptop had been in use since 2013.

Data, Data, More Data

Found an advertisement for Valentine's Day 2018, food menu specials, and payroll details for January 29, 2018 to February 11, 2018 - names, positions, hours worked, hourly pay, net pay.

- $3.00 an hour for servers.
- $9.00 an hour for bussers.
- $12.00 an hour for counter employee.
- $13.00 an hour for food runner.
- `January 2018 Sales Report.pdf`: $29,101.35 grand total. Including GC, SC, tips $31,882.07.
- Back to the desktop folder, we have `Desktop\Music` which was empty.
- Old Catering Menus. TeamViewer 10 was also installed.
- `Desktop\Permits`: Deck and outdoor business permits. Address of the business owners.
- `Finance Docs`: Scanned checks, client catering agreements.
- `Heather\Bank Statements`: AMEX, PNC Card processing statements going back to July 9th, 2012.
- Equifax report.
- Fire inspection documents.

Pause to reflect. This is a ton of data and I have more. Please wipe business and personal details. I could have committed tons of fraud with this data.

I still have a few more cringe details to wrap this article up. I appreciate your patience as a reader.

- `incident report.doc`
- `insurance questionnaire.pdf`
- Quickbooks (but only has the 2009 templates).
- W2 reconciliation Dec 2015
- Symatec folder with a CD key and a bunch of 80s music.
- Taxes: Tax returns, payroll taxes in .xls files dated from 2010 to 2015.
- `VerizonUSerID.docx`
- Comcast business contract
- Credit card statements.

Some files ask for a password to open, most files do not.

- `discover.csv` (for listing of transactions).
- Residential leases agreements from October 2011.
- `Local Inquirer Ad.pdf` dated January 29th 2012.
- `koldwalkInCooler.pdf`
- `Landlord Letter.docx` (vouching for tenants).
- Commercial construction building contract.
- PR statement from August 6th, 2013 grand opening.
- Zagat 2013 review.
- `Tag Organizer.pdf`
- PNC bank settlement documentation.
- `scan.pdf` (inventory of office cleaning cups).
- Even more direct deposit and bank details found in a bank details folder.
- Health inspections.
- `staff.xlsx`
- `monthly.pdf` (February 2017 generated nearly $80,000 in one month).
- Scanned Documents. 164 files.

Writing this out was longer than I expected. May this article go easy on the *2600* editorial staff. Redact names if necessary, but I felt sharing that I had both owners' names solidifies the concern in the discoveries. *Wipe* and/or encrypt your disks.

Might I suggest amateur forensics to learn more.

Also, if using Linux, create a LUKS volume with an encryption passphrase to encrypt the whole disk. You can then create ext4 data volumes.

12 NEW *2600* T-SHIRTS!

You read that right. We now have an additional 12 (!) shirts in a variety of sizes for your wearing enjoyment.

Each shirt has the full color artwork from one of our covers that was printed in the past three years. People have been asking us to do this for years, but it wasn't until now that we were able to accomplish it in a way that we were happy with. And we're certain you too will be quite pleased with these shirts.

They all contain an entire cover image without any masthead or barcode. Whether you choose the Ukrainian payphone picture, evil social media image, ransomware message, or any of our other designs, we're quite confident that you'll be happy strolling around town wearing what might be the coolest, most provocative t-shirt in miles.

This is also another way of supporting 2600. We intend to design more hacker-related shirts in the months ahead if we get a decent reaction to what we've released so far. Please be sure to send us your feedback!

All shirts can be seen and ordered at ***store.2600.com*** *along with hats and sweatshirts!*

This is only the beginning.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I'm on Shaw Island, one island over from the home of ToorCamp, and it is snowing. That's rare here, but it has been an unusually cold winter so far. There have been windstorms and snow and ice, all of which have wreaked havoc on our aging and rickety outside plant. I'm here tasked with figuring out what, exactly, we're going to do about it. Who am I kidding, though? The answer is probably nothing.

A phone line, conceptually, used to be a single copper pair, which ran all the way from your phone to the frame in the central office. In reality, it was far more complicated than that: you owned your inside wiring (which was your responsibility), which would interface with the telephone company's outside plant at the SNI or TNI (typically a box on the side of your house). On the telephone company's side, a drop cable would run from your premises to a splice enclosure (these usually look like a post, serving multiple houses in a neighborhood), which will then connect via a distribution cable to a serving area interface (these are the green boxes you typically see at the entrance to a neighborhood), which then connects to a feeder cable and finally to the central office frame.

So, it wasn't really just one cable - it was a patchwork of cables spliced together, which formed one continuous circuit between your telephone and the central office. That's a long way to push electrons. It might be five miles or more. Both resistance and capacitance exist. Cables are twisted, and this causes further attenuation because the distance is about three percent greater than if cables went straight through. We're also, due to runaway global warming, seeing higher temperatures in the Pacific Northwest than networks were designed for (and this is *every* network, from electricity to cable TV to telephone to wireless networks). In our case, higher temperatures cause deterioration of cable sheathing at an elevated rate. It used to be that five percent of the time, a fault was in the aerial or underground portion of a cable, and 95 percent of the time, a fault was at an interconnection point. That's no longer true; it's now closer to ten percent of the time that the fault is up a pole, or somewhere underground. These faults are harder to find and much harder to fix. Why? Nearly every outside plant component of the telephone system - from poles to cables and beyond - is past its useful life.

What's more, there are capacitors inline throughout the network and, if you own an old electronic device, you have probably experienced a capacitor that has failed from age. This happens in the telephone system too. Fortunately, these failures are easier to find, but due to supply chain disruptions, the parts can be very difficult and expensive to come by. Naturally, phone companies dramatically reduced inventories of spare parts to save money starting in the early 2000s. I have heard of cases where outside plant technicians will, when faced with a shortage of spare parts, borrow capacitors from a part of the network with fewer subscribers (potentially causing an outage) in order to restore service in an area with more subscribers.

Overall, it's really complicated to run a network that is outside in the weather, with trees falling on it and deer pissing on it and the occasional meth head stealing copper from it (yes, this really happens). Funny story about that. One genius thought it was a good idea to cut a 2400 pair PE-89 cable. These are 24

gauge, filled with icky pic, and weigh over ten pounds per foot. When his buddy cut it, it dropped straight down and clocked him in the head, splitting his forehead open. The techs found him in the gutter, bleeding, and out cold. Miraculously, he survived.

If all of this sounds unsustainable, it is. And naturally, the company doesn't really want to invest much (if anything) in fixing problems because the network is obsolete. They don't make money selling traditional telephone service. All of the money is in selling broadband these days, which is not only unregulated, it mostly relies on different technologies. Fiber to the node is going in everywhere. The way this works is that new, fiber-optic cable is run from the central office to each serving area interface, where a DSLAM and SIP gateway are installed. The existing copper cabling is used for "last mile" connectivity to nearby buildings. It sounds great in theory, but this plant is still decades old and has been deteriorating as much as the rest of the network (arguably even more), so it's a stop-gap solution at best. Then again, telecom executives seem to be treating fiber optic cables as a future-proof technology that will never wear out or require maintenance, which is completely inaccurate. The lifespan of fiber optic cable is lower than that of copper cabling! All of this stuff will need to be replaced in 30 years, if technology hasn't already passed us by prior to that.

What's the future? Well, right now, on places like Shaw Island, it's the present, which is essentially the past. This will be among the last places to get much additional investment. There's not much here: a couple of convents, a community center, a ferry dock, a general store, and some houses. It'll be far down the priority list. As beautiful as the place is, I really wonder what I'm even doing here.

A more fun outside plant implementation, operated by phreaks at the ToorCamp hacker camp this year on neighboring Orcas Island, was presented by Shadytel. These folks show up and operate a virtual phone company, offering free landline telephone service allowing hackers to make phone calls from their campsites (assuming they solve a puzzle required to initiate service). Two AT&T Definity PBXs were installed, serving as central offices, one each at upper and lower camps. Two trunks ran between them (T1, digital, for switching between exchanges, using HDSL as transport). This provided both redundancy and spare capacity in the event of anticipated hacker shenanigans (such as attempting to ring every telephone at Toorcamp at once).

For local distribution, T1s were run to multiplexers distributed throughout the camp, which were equipped with line cards (up to six per mux, supporting two T1s in total). Each line card supported up to eight subscriber lines, which were then run over Category 5 cable to distribution points throughout each camping area. From there, campers would run their own phone lines to connect to the network.

Naturally, many of the same problems that occur in the real world occurred at Toorcamp. Splicing caused constant headaches. Splices could get damp, or contaminated with dirt, or attacked by raccoons, and connectivity would be lost - potentially to large parts of camp. Power could be interrupted (occasionally by campers unplugging network equipment to run kitchen appliances). Aging equipment sometimes failed under the extreme conditions. Fortunately, the HDSL equipment was equipped with LEDs to monitor the state, and the equipment was colocated with Shadytel operations. When a connection dropped, it was visibly evident: the LED would turn red. Fortunately, copper theft was never the root cause; hackers are a friendly crowd.

And with that, it appears I have a new nemesis: a squirrel. One has evidently packed a splice enclosure full of nuts, and this is the root cause of the outage I'm dealing with. Have a happy and safe winter, don't forget to check your tires, and let the gentle hum of a dial tone be your spirit guide. I'll see you in the new year.

Friendly Fraud

by Lee Williams

Greetings. Lee the Agent here. By now I hope you can recognize my writing style across editions of this magazine and figure out who I am even though I've been writing under different pseudonyms. Now, let's get to the article.

When someone fraudulently takes money out of your bank account, most of the time you have almost nothing to worry about. The bank, whoever that is to you, is required to keep your money safe. When your money goes missing, the bank is never allowed to say "sucks to be you" and then leave it at that. They *have* to insure your money. Therefore, banks have these processes called "disputes" that allow the customer to get their money back when shit hits the fan. You see a fraudulent charge on your account, you make a dispute with your bank, and if you're being honest, they will place the money back in your account.

This goes beyond unauthorized transactions. If a merchant scams you, you can actually go to your bank and tell them that. If you order two snacks at the vending machine but it only gives you one, you can go to your bank and tell them that. The bank has the option to side with you, and if you're being honest, they will. So I went to the vending machine, bought two candies, but only one came out. I told my bank this, and I received half of the money back into my account. That's when it hit me: I can steal with this. If I can file a fraudulent dispute, I can get away with not paying for shit.

There's one specific bank, the one I bank with, who will *always* side with the customer when dealing with disputes. I'm not going to say the name of the bank, but it's one of the largest banks in the United States. Let's call it Digital Dash National Bank. What this means is that when you file a dispute, nothing else matters; They're on your side. My current love interest has family who actively does fraud with Digital Dash National Bank because the bank just enables it. This happens all the time. People realize that when you dispute a charge you get your money back, so people take advantage of it. They would make huge purchases and then dispute the charge.

I found out that my bank sides with the customer when I bought a partially broken knife at a gas station. It broke the same day I bought it. It was partially functional, enough that I still wanted to keep it. I went straight to my bank to tell them that the merchant (the gas station) sold me a broken product. The man on the other end of the phone told me that they're taking my side, and they always will. My bank, which was actually one dollar in negative balance, had the money spent on the knife back in my account, and I was no longer in debt. But there's a catch.

When you do an honest credit card dispute, you have to also, in good faith, make an effort to resolve the issue with the merchant first. When the merchant *won't* help you, then you make a dispute. But I technically skipped the step of trying to resolve the issue with the merchant and went straight to the bank. My bank was in negative balance. Afterwards it wasn't. The knife was partially functional. I just skipped the step of trying to resolve the issue with the merchant. This is around when I realized what I did was technically fraud. Whoops. Thankfully, nothing ever came of it, but I never did it again.

The merchant, however, is allowed to argue the dispute and keep the money. If they don't make a good argument or don't respond fast enough, the customer wins the dispute. Most banks follow this protocol.

This happens all the time, where people will do fraud without serious malicious intent. Perhaps they did what I did, and just skipped a step with no ill intentions. My goal wasn't to steal from my bank; I just wanted my money back. People will dispute charges by accident, or skip steps, and end up committing a crime. But with my bank, there seems to be no chance of them siding with the merchant in a dispute. So what's stopping me from consistently disputing charges, stealing from both the merchant and the bank, a real 21st century heist?

The Blacklist.

Not many people really know *exactly* how the anti-fraud algorithms work except for the bank. But we all know that the algorithm isn't stupid. There are certain things that we know will tip it off, like having a VPN or your zip code, but there are other times where the algorithm just somehow knows that you're doing something wrong. Among other things, the algorithm pays attention to your disputes, how often they happen, when they happen, and other pieces of context about them. There's really no perfect ratio to successfully do a fraudulent dispute. It's more of a guessing game when your intention is to do fraud.

"But Lee, you said your bank sides with customers all of the time! How will they stop fraud? Why haven't they stopped your lover's family?"

Well, even though they side with you, the algorithm can still figure out you're doing fraud.

Once they finally catch on, risk analysis at the bank determines that you're a threat to them and other financial institutions, so they place your social security number in a database I refer to as *The Blacklist.* Other people also refer to it like that; I just like the dramatic effect of *The Blacklist* in italics. Once your SSN ends up in the blacklist, you won't be able to get approved for a loan or a mortgage, and you won't be able to set up bank accounts. You could end up in that database forever, and you're basically fucked for life at that point, as no financial institution will want you because they think you're going to steal from them.

The reason her family hasn't gotten caught is most likely because they successfully fooled the anti-fraud algorithm. If I'm being honest, I don't know the exact details of what they're doing, but it's definitely more than just disputing charges. Thankfully, I'm not in the blacklist, but I almost ended up in the blacklist one time and can no longer bank with a separate major bank. I'm lucky they didn't sue me or press charges, but at that time they thought it was not a malicious act of fraud, but rather I had gotten scammed so it makes sense why no action was taken. That's not actually true, but I'd rather them think that it is and then close my account.

Here are two real life scenarios:

Scenario One: You go to Walmart in another town and buy a burner phone with cash. Then you walk to a cafe, log into your bank on the burner phone, and purchase a brand new pair of black Air Force Ones. Then, a day later on your main phone, you dispute the charge.

Boom, you're in the blacklist because the algorithm knew that you were up to no good, or you messed up somewhere, or some other reason on the incalculable list of reasons for why it got flagged. Risk analysis deems you a threat, you get blacklisted, and the credit bureaus write your name and SSN down somewhere.

Scenario Two: Your bank is in negative balance. You dispute that meal you ate yesterday, claiming your food never came. The algorithm knew. Risk analysis deems you a threat, you get blacklisted, and the credit bureaus write your name and SSN down somewhere.

There's no way to know if your dispute will blacklist you or not. Once you're in, it's hard to get out and your life will be very difficult from there on out.

That said, the only time you should be worried is if you're doing fraud. And if you do happen to dispute a charge in good faith and the algorithm flags it, you can always make a call to the right people ("the right people" being your bank) and explain the situation to them.

Let's Party Like It's 1989

by Robert Sissco

"It's always a challenge hiding something sensitive that you might need quickly. Any hiding place involves a trade-off between security and access. Hide something in the sewer main beneath your floor and it's secure, but good luck getting to it. Hide something in your sock drawer and it's easy to get to but hardly secure. The best hiding places are easy to get to but tough to find. The do-it-yourself versions are known in the spy trade as slicks - easy to slip something in, easy to slide it out." - Michael Weston, *Burn Notice*, Season 2, Episode 9.

As hackers, access is everything. If we can get into it, or at it, we will. It is in our nature. And this isn't always to cause millions of dollars of damage by *looking* at something (also, fu Sun Microsystems). I remember laughing when I first watched *Freedom Downtime* and seeing the scene where the FedEx truck driver found several cases of beer in a drop box, because they use the same combination on all their drop boxes. Funny and entertaining.

On the other hand, I used to do tech support for the Microsoft point of sale systems, and remember one customer that literally built their server *into* a wall to prevent access to it. But this meant when that server was dying (likely due to overheating due to lack of ventilation), it was frustrating and sad because these people were at a high risk of losing the system they used to run their livelihood on.

But it's our very nature as humans to want to keep our own devices and areas restricted to ourselves. Today this can range from encryption programs to hiding a yellow floppy disk in an air vent in our bedrooms. *But* many governments require encryption programs to register a public key with them in order to do business in their country, and if you need to flee quickly, you may not be able to get that disk out.

But one thing that many people overlook is *compatibility* with modern devices. I still have a 512MB flash drive from college that used USB 1.0 to connect to systems, and will still connect to my USB 3.0-only desktop system. Again, we have used this to our advantage (honey pot USB sticks left in parking lots, anyone?). But this means our tech can be plugged into a system used by those we do not want to have access in order for others to access it. I can still access my late 90s/early 00s buggy C++ and Intel x86

assembly programs with no issues. They are also common and easy to pocket and walk away with (who reading this hasn't "found" a USB drive somewhere and then found it later in their pocket?).

Let's look at the retro. CDs and DVDs are great: stable, easy to hide, hold a decent amount of data, but hard to rewrite. Meaning, in most cases, once your data is written, it might as well be in stone. And yes, I know CD-RWs exist, but honestly, I have had nothing but bad experiences with these, and often by the third rewrite the data is so horrible that it might as well be lost. This puts a barrier on data upkeep.

But wait, I mentioned floppy disks earlier. What about them? Can be written to many times, not the largest amount of storage space, and a bit obscure to use (when was the last time you actually needed to use a floppy disk or even found a system with a reader installed?). And many of the older style disks are rather stable and built to last. The ones from the 90s are often where quality was sacrificed on the altar of profits. However, while it will not auto launch, most systems with a drive can read them, and they still make and sell 3.5 inch USB floppy drives.

Well, wait a moment. Only as long as the disk was written in a compatible system on a compatible drive, can it be read. Anyone from the 8-bit or early 16-bit system days may remember that those who used the same OS (say, CP/M) may not have been able to read disks on a different model system despite running the same code. Sure, there are devices that could be attached to increase compatibility, but can we use this to our advantage? Yes, but even some systems back in the day could get around this.

But if we take it a step further, what if the drives were not compatible because they were physically built differently?

Let's take a look at the most popular system ever sold, the ones built for the masses, not the classes? The Commodore line of systems. Their drives were wired differently (for instance, an IBM 3.5 inch disk drive could not be used in the Amiga systems or the 1581 drive without modification because the pin outs were different).

In addition, accessing a disk in a lot of systems is easy. But while many of those in the scene from the later years may or may not have knowledge of DOS commands, how do you access drives on the Commodore? I am sure many of my fellow Boomer and Gen X hackers may remember the `LOAD "*",8,1` command.

And while you can look this command up, again, the accessibility is not there. Not everyone has a Commodore available. Not many people would keep the old while they move to the new. Heck, the first Commodore I bought was just a few years ago from a pawn shop. I got it cheap because they thought it was only a keyboard. This means that many today may not even recognize the system. So, set up right next to my eight core i7 64GB RAM with two terabytes of storage space I have my one megahertz 64K RAM system with zero native storage.

Now, while many may see a gap, there really isn't. I have cartridges and devices I can plug into my C64 to attach to a LAN to access disk image files on my server, or to get onto my network to access BBS systems. I can communicate between systems *with the proper knowledge*.

And even today, people have designed and developed - and *sell* - systems that allow these older devices to work on modern devices. This means I can access and use my Commodore disk drives on that i7 system I mentioned earlier to read and write files if I don't want to hook up the ole CRT monitor to see what I am doing.

Not good enough for you, you say? Lots of people still have disk drives? How about going even older and using cassette tapes? Needing to remember the counter on the tape to find the specific data needed, and it is *slow*! Worried about people getting files quickly? Yea, not happening, they would need to take the tape, and then you may notice it is missing.

Or go the Amstrad route and use the three inch disks, something I do not think were ever really used on IBM systems (which became modern PCs), adding another layer of access obscurity to your security....

So, by embracing the old in the age of the new, I feel secure in my data since many do not know how to use my data or even what to look for. Between the encrypted USB flash drive I always keep on my person to the out-in-the-open "how do I access this stuff" media, I feel relatively secure in my data. Will this keep a determined individual out of my stuff? No. But I have a higher bar than many because of the obscurity of the mix of media I use.

Want more proof that this is not a crazy idea? Until 2019, the United Staes Air Force used eight inch floppy disks to control systems related to ICBMs, nuclear bombers, and tanker support, because the disks were stable and required physical access to the media and drives to interact with, adding a level of protection between those authorized to use the system and those from outside it who should not have access but may want it. And per Lt. Col. Valerie Henderson, spokesperson for the U.S. Defense Department, "It still works."

And yes, my Commodore can run *Crysis*, because I wrote a BASIC program and titled it "Crysis" just so I can answer "yes" to this question.

Current Bulletin Board Systems: How It's Done

by warmfuzzy

Of all the things I've loved and lost, I miss my board the most,

but now it is back online, and this corner of the net is mine,

the speed is a thousand fold, my storage is even more,

I'm back in the scene, behold my 1337 system is hardcore.

- warmfuzzy

Hosting Benefits: Self-hosted systems (full control) vs. vServers (cheap and reliable) vs. dedicated servers (massive capacity and offsite reliability). Recommended home-based systems are the "nano computers" which are very small form-factor systems that you set up and leave to run. vServers are available at IONOS.com, recommended dedicated servers are available at www.hetzner.com. With all of these hosting options, it is fully recommended that you use the Linux operating system, as it is more capable than the Windows or Mac alternatives.

Storage: HDD vs. SSD (SSD gives no speed advantage due to the limits in the Internet service.) "Toasters" are recommended; they are HDD docking stations that look as if the HDD is toast and the docking bay is the toaster. Recommended model is the "Sabrent 4-Bay USB 3.0 SATA 2.5"/3.5" SSD/HDD docking station (DS-U3B4), which goes for around $100 USD. Recommended HDDs are the Western Digital RED NAS 5400 rpm drives. One thing to note with these drives is that they can get really hot due to the density of the platters, so you may need to buy a fan to cool down the several drives that you should buy. The eight terabyte WD RED NAS drive is recommended, which will cost you around $250 USD or less if you get a deal.

Famous Systems and Personalities:

- *Agency BBS*: Avon, agency.bbs.nz:23(telnet) / 2024(ssh)
- *Black Flag BBS*: Hawk, blackflag.acid.org:23(telnet)
- *Fishingnet BBS*: warmfuzzy, fishingnet.phatstar.org:7777(telnet)
- *HyperNode BBS*: MaxMouse, hypernode.ddns.net:23(telnet)
- *KANSIT WHQ BBS*: cr1mson, whq.kansit.com:23(telnet) / 22000(ssh)
- *Necronomicon BBS*: necromaster, necrobbs.ddns.net:23(telnet)
- *Raiders Inc. BBS*: cr1mson, vintagebbsing.com:1337(telnet)
- *The Bottomless Abyss BBS*: StackFault, bbs.bottomlessabyss.net:2023 (telnet) / 2222(ssh)
- *The Quantum Wormhole BBS*: MeaTLoTioN, bbs.erb.pw:23(telnet) / 45022(ssh)

Echomail Nets (all the below networks use the fresh binkp echomail protocol):

- FSX (Fun Simple and eXperimental), 21:*, Avon, avon@bbs.nz
- AgoraNet, 46:*, Accession, access@pharcyde.org
- Retronet, 80:*, necromaster, retronet2016@yahoo.com
- Whispernet, 316:*, cr1mson, cr1mson@phatstar.org
- Sp00knet Echomail Network, 700:*, society@phatstar.org
- Fishingnet Echomail Network, 701:*, society@phatstar.org
- The Investor's Network, 702:*, crewmate, crewmate@crewmate.tech
- TQWnet, 1337:*, MeaTLoTioN, ml@erb.pw

Art Groups: Blocktronics (blocktronics.org), Impure (and others) (16colo.rs/), and ansigarden.com (custom and stock artwork for a fair fee)

ANSI Editors: PabloDraw (picoe.ca/products/pablodraw/), Moebius (blocktronics.github.io/moebius/), and Mystic BBS's Internal ANSI Editor (mysticbbs.com)

Modding Groups: PHATstar Society (phatstar.net), DoRE (*Dreamland BBS*), Phenom Productions (phenomprod.com/)

Documentaries and Commentaries:

- *The BBS Documentary* (www.bbsdocumentary.com/order/)
- *Back to the BBS Documentaries* (erb.pw/bttb) Al's Geek Lab YouTube also available.
- *TexTalk.news: Going Full-on Mad Retro* (textalk.news), *The Textmode PODcast*
- *Textmode Magazine* (textmodemag.com); a future project that is on hold for the time being.
- TelnetBBSguide.com: The central location for a BBS system directory.

Client Software: NetRunner (www.mysticbbs.com), SyncTerm (syncterm.bbsdev.net), mTelnet (no link)

Server Software: (all of the below software suites work on both Linux and Windows + Mystic's ARM

- Mystic BBS (www.mysticbbs.com) (straightforward configuration and most modable). Recommended for most users as it is basically plug and play with easy configuration

- Synchronet BBS software (www.synchro.net) (easy to use and open source, more difficult to modify)
- Enigma 1/2 (enigma-bbs.github.io/) (excellent for the programming community)

Code Pages:

- CP437/ANSI-BBS (around 250 or so usable "characters" out of 256 characters)
- iCE ANSI (an improved ANSI that offers a greater color selection in place of flashing colors)
- UTF-8 (with foreign language support)
- ASCII (plain and simple text based communications)
- Rarely used protocols: AVATAR, RIP

Plain Old Telephone System:

- SEXPOTS: Synchronet External Plain Old Telephone System. Allows you to receive connections from the POTS and redirect it to any arbitrary Telnet BBS server, works on Linux and Windows.
- Connect your favorite RS-232 US Robotics 56k v92 vEverything External Modem via Serial to USB 2.0 conversion cable. Recommended cable: DTECH USB to RS232 DB9 serial adapter cable 16 with FTDI Chip, DB9 9 Pin USB 2.0 (a converter adapter with the FTDI chipset) which will cost you around $20 USD for a 16 foot cable. Recommended modem: US Robotics 56k vEverything external serial modem which costs around $30 USD plus shipping from eBay.com.

Connection Protocols:

- TELNET: plain text with no encryption, very easy to "sniff" the traffic. It's recommended for speed, but should have no function to login to system functions or the sysop password could be sniffed.
- SSH: commercial-grade cryptographic protocol. Can easily be added to Mystic BBS with a free crypto library.
- RLOGIN: not used very much, but is an alternative for non-standard setups. It is used to connect to the Doorparty door game server.
- RS-232/Serial: the protocol used by POTS modems going into the connecting computer.

Instant Messaging:

- Multi-Relay Chat: at the time of this writing there are over 100 boards that are connected to this instant messaging service. It works quite well and has been a boon for the scene, however there is currently no secure communication capacity in the present version. To fix this gap in secure chat is MeaTLoTioN's Matrix server which is end-to-end encrypted (riot.erb.pw).

Fun Times:

- *[P]hone [i]n [M]y [P]ocket BBS*: MeaTLoTioN's BBS running off of his Android phone Pimpbbs.erb.pw:18023 (telnet) PIMP BBS: *"No pocket fluff was harmed in the making of this BBS."* -ML
- File Servers: BBSes can now connect to file servers through the TELNET-OUT function available in modern BBS software. You connect to your favorite BBS system, go to the "file area," select the server of your choice, telnet with the push of a button to that file server, and you're good to go. Systems include Anonymous Archivers File Distro Network (phatstar.org), Silent Partner FDN (phatstar.org) accessible from AAFDN, and ArchaicNet FDN (sysop@archaicbinary.net).
- Door Game Servers: You can now play online games with thousands of others using a game server where people can log on to a BBS, open the game server portal, and be presented with many dozens or hundreds of games, having all those games in one spot to play with fellow gamers on a single system. BBSLink (bbslink.net) and DoorParty (www.throwbackbbs.com/).
- Quantum Radio: The scene's Chiptunes and Tracked Music streaming radio station (radio.erb.pw/).
- The Weekly MeaTup with MeaTLoTioN on Multi-Relay Chat (MRC) at 20:00 UTC on Fridays. MRC is accessible from BBSes that have the MRC BBS mod installed; this works on all the major BBS software (www.meatlotion.com).

ARE YOU READING THIS ISSUE ON A KINDLE?

There is important information for you in the editorial ("Inconvenient Truths")

Intercepting Google CSE Resources: Automate Google Searches With Client-Side Generated URIs (for free)

by Renan de Lacerda Leite

From an OSINT perspective, Google Search has been an indispensable tool for collecting data about companies, sites, persons, leaks, i.e., any kind of relevant information for countless investigation purposes. Although mostly used by analysts on targeted research, there are actors who would take advantage of developing a fully automated discovery process using Google's search engine as one of its most important sources of data.

Nowadays, Google already offers to the public a service that facilitates the development of automated searches, which is called Google's Custom Search JSON API. In order to use it, one needs to create their own Programmable Search Engine - a very useful Google service, created to help developers embed Google search boxes in their websites, increasing their users' experience by helping with more focused searches - and they must ask for an API key to consume Google's JSON API. However, this API has some free usage limits: after making a hundred (100) queries in a day, you'll be charged a fee of five American dollars per 1000 queries, limited to 10,000 queries a day if one does not want to use their restricted JSON API version.

That's where this article comes in. Exploring a client-side generated API URI, it was possible to consume Google's API data without needing to use any personal CSE API key and, consequently, without being charged for queries, as we avoid its traditional JSON API methods.

In order to consume this observed Google CSE API, a Python proof of concept module named CSEHook was developed, with the help of libraries such as Selenium Wire (a library that enables access to the underlying requests made by a browser) which was used to intercept Google CSE API URIs, requests (an HTTP library) to consume the content of those previously intercepted URIs, and other publicly available resources.

Thought Process

Google's CSE, now called Google's Programmable Search Engine, is not news anymore. It's already well known by web developers who use it to embed Google search iframes in their sites' pages, investigation actors who want to search predefined focused domains in order to collect particularly interesting data, and other kinds of individuals and professionals. This is a useful, widely spread public tool, first made to facilitate the embedding of Google search boxes in sites and the use of more specific, personalized, and focused search engines, but which happens to be an incredible tool for people who have a ton of research work to do.

Despite being truly helpful on its own, there are some things in its bundle that are not so handy for people who depend on heavy automated tasks to do their job: the CSE JSON API limits. For this reason, attempts to find alternative paths, for curiosity purposes, were made in order to contour those obstacles.

All the demonstrations were made with a personal Programmable Search Engine, focused on searching terms on Pastebin site pages.

Observing how the client-side of a Google CSE URI interacts with Google's backend resources, a couple of interesting behaviors were noticed when a query is made:

- A request is sent to an ads URI (`cse.➥google.com/cse_v2/ads`), which responds with advertising content.
- A request is sent to an element's URI (`cse.➥google.com/cse/element/v1`), which responds with text content containing a function call that takes a JSON object as an argument.

Even though the Ads interactions could be consumed and parsed to some extent, what really calls the attention is the second behavior. The response contains a call to a client-side JavaScript function, which receives a JSON object that was sent to the client from a Google server. This function will parse the JSON object, which will always contain up to ten search results at a time (per page), up to ten maximum distinct pages, and exhibit the results in the CSE page that is being used.

Despite the frontend generating an individual URI for each performed query, what was noticed is that those URIs could be reused to query different terms, i.e., there was a possibility to later automate the collection of data by intercepting the generated URIs, changing their query strings, and then requesting new results and parsing the collected content. In order to achieve this, CSEHook was developed.

As the content to be consumed is a response of a dynamically generated URI that depends

on the execution of client-side JavaScript to be generated, it would be useful to use a browser instance in order to generate those interesting URIs. The traditional Python solution to this kind of issue is generally Selenium; however, Selenium alone would not be able to track those client secondary network interactions that need to be intercepted. That is why the Selenium Wire, an extended version of Selenium that monitors the requests that were made by the browser instance, was chosen to help in the effort to catch those URIs.

A ChromeDriver will be needed so the Selenium Wire library can do its work. This driver should fit the installed Google Chrome browser version (used version: 91.0.4472.114 for x86_64).

Additionally, Geonode proxy service was used in order to avoid Google's detection systems and diffuse the requests made to its resources. This was implemented because, during the first implementation tests, it was observed that those URIs had a specific limitation to the amount of requests that could sequentially be sent to it. Apart from limiting the quantity of requests made to those dynamic URIs by re-intercepting those resources from time to time, it was preferred to spread the source IP addresses' geolocation that would be sending those requests as well.

Also, to avoid User-Agent pattern-based detections, a list of Google Chrome User-Agents was picked from tamimibrahim17's repository. This list was utilized in order to randomly choose a User-Agent and place it in the request headers just before sending a request to Google's resources.

Finally, to prove that it would be possible to surpass Google's official CSE JSON API limitations with the approach of this article, the Python library named English-Words was chosen so it could be demonstrated that the CSEHook proof-of-concept could effectively iterate through all sets of English words in a relatively short time, i.e., searching lowercase English words in order to obtain results from the already created Programmable Search Engine without calling Google's detection system's attention.

All the previously specified libraries and resources can be found in the References section. A link to their own respective websites was left there as well.

PoC Structure

To achieve the data collection intentions cited before, the project is structured in the following way:

- A config file, which contains some of the PoC configuration variables.
- A driver directory containing ChromeDrivers for Mac, Linux and Windows operating systems.
- A CSEHook directory, which contains the proof-of-concept necessary modules. Here are found a utility class named WiredDriver, which interacts with Selenium Wire library and ChromeDrivers, and the main CseHook class which contains the main PoC code.
- A *__main__* file, which has instantiations to the previously named classes and iterations through the English Words set in order to search those words with the intercepted Google's URIs.

This structure can be better visualized at the project's GitHub repository.

Configuration

The configuration file has the following variables in it:

- *CSE_URI*, which is the URI of the previously created Programmable Search Engine.
- *DEFAULT_DRIVER*, which is the file path to the downloaded ChromeDriver.
- *USER_AGENTS*, which is a URI to the Chrome User-Agents of tamimibrahim17's project.
- *RENEW_CSE_DEFAULT*, which represents the amount of requests the application can do with the five intercepted Google client-side generated URIs. When the application reaches this limit, it will make more requests to the Programmable Search Engine URI in order to collect new client-side generated URIs. This is tunable, but Google will ban the main Programmable Search Engine URI searches if too many requests are made to the same client-side generated URIs, so this must be kept in mind before altering this configuration.

Wired Driver

This is the class that interacts with the Selenium Wire library. Not too much to detail: an instance of this class will be used in order to interact with the Google Chrome browser so it can be possible to intercept the client-side generated URIs.

CSE Hook

Here is where the main logic is placed. Its explanation will be broken in different fragments in order to detail its functionality.

The class has three internal inherent attributes that do not depend on its initialization:

- *_MAX_PROXY_RETRIES*, which establishes the amount of request re-attempts it could make with the in-memory previously downloaded proxies before requesting for new ones to GeoNode.

- *_STANDARD_SLEEP*, which is just the amount of seconds it would keep sleeping if, and only if, Google expires the client-side generated URIs before the application renews it, which would be unexpected behavior.
- *_TIMEOUT*, which is just the amount of time the Requests library should wait for a response while requesting with proxies.

Inside the class initialized components, there are the following attributes:

- *self._amount_of_words*, which specifies the amount of words to be queried to the main Programmable Search Engine in order to collect the same amount of client-side generated URIs, i.e., if it searches for five words - which is its default value - it will search the main URI five times and intercept five different client-side generated URIs.
- *self._word_size*, which is the amount of characters each randomly generated searched word would have in order to obtain the client-side generated URIs.
- *self._cse_uri*, which represents the Programmable Search Engine URI that will be used so it can intercept the client-side generated URIs.
- *self._is_cse_uri_valid*, which checks if the specified URI is a valid Programmable Search Engine URI.
- *self._wired_driver*, which just saves the specified wired_driver instance.
- *self._cse_api_pattern*, which is a pattern for the first URI characters of the targeted client-side generated URIs so it can identify those URIs in the intercepted URI's list of the Selenium Wire instance.
- *self._cse_regex*, which is a regex that will form the groups necessary in order to catch the JSON inside the JavaScript function call of the client-side generated URI response.
- *self._cse_api_uris*, which is an empty list that will contain the client-side generated URIs intercepted by the code.
- *self._pages*, which just maps the page labels with its *start* required offset.
- *self._proxy_list*, which receives the results of *self._config_proxy_list*, a method that is responsible for requesting GeoNode for new proxies.

The next four methods listed inside the class are responsible for the following activities:

- The method *self._get_modified_uri* is responsible for parsing the received URI and returning a string which is a modified version of the same URI. The query parameters *q* (query) and *start* (start offset/page) are the ones that are changed by this method.
- The method *self._config_proxy_list* is responsible for requesting GeoNode for new proxies. It will return the list of data offered by GeoNode's endpoint.
- The method *self._get_random_words* is responsible for yielding randomly generated words on demand, based on the previously defined attributes *self._word_size* and *self._amount_of_words*.
- The method *self._config_new_cse_api_uris* is responsible for configuring the intercepted client-side generated URIs. It will: iterate through the words yielded by *self._get_random_words*, modify the Programmable Search Engine URI using *self._get_modified_uri* in order to place the word in the *q* query parameter, use the modified Programmable Search Engine URI to query a word just to intercept and collect the client-generated URI, and append the found client-generated URI to the *self._cse_api_uris* list.

The fifth method is called *self._get_response*, and its responsibility is to request an endpoint using the specified URI, headers, and proxies. If the request raises a timeout or any other exception, it will check if the amount of retries - which is passed as an argument as well - has achieved its limit. If this limit is achieved, it configures *self._proxy_list* with a new proxy list retrieved from GeoNode.

The sixth method is named *self._search_page*. This method receives the arguments URI, query, and page and returns the JSON retrieved from the modified client-side generated URI response, i.e., the results from Google that it wants to collect with a specific query term.

This is the most complex method of the class, and what interacts with most of the other already declared methods.

While the response is not received from Google, it will: select a random User-Agent and define it in the request headers; choose a random proxy from the *self._proxy_list*; form the proxies dictionary with the information of the *chosen_proxy* so it can be used with the requests library; get a response using the method *self._get_response*; if the response is not satisfactory, it will pop the *chosen_proxy* from the *self._proxy_list* and increase the *error_count* by one and will continue the loop. The *error_count* is the value passed as the argument *retries* of the *self._get_response* method.

If the response is received, check if the *status_code* of the response equals 403 (HTTPStatus.FORBIDDEN). If it does, return

a dictionary with the key-value pair. If it does not, find the JSON inside the client-side generated URI response with the *self._cse_regex* compiled regex, catch it, and assign it to *api_json*. After assigning, return *api_ json*.

The last method of the class is named *self.search*, which is the only public method of the class - and the one that is used by *__main__*. This method receives both *query*, the term that one wants to search using the client-side generated URIs, and *renew_cse_uris*, which is a boolean that determines if the client-side generated URIs should be refreshed as arguments.

The responsibilities of this method are the following:

- Quote the received query string so it can be correctly placed in the client-side generated URIs.
- If the *self._cse_api_uris* list still has no

```
def search(self,
           query: str,
           renew_cse_uris: bool = False) -> _GoogleCSEIterator:
    """Get Google CSE results using our CSE API URIs.

    Return: an iterable object with all available Google CSE pages.
    """

    query = quote(str(query))

    if not self._cse_api_uris or renew_cse_uris:
        self._config_new_cse_api_uris()

    first_page = self._search_page(
        random.choice(self._cse_api_uris), query
    )

    error = first_page.get("error")
    while error:
        # If we were temporarily banned, return False.
        if isinstance(error, str):
            return False

        # If old CSE API URIs start to fail, refresh them.
        sleep(self._STANDARD_SLEEP)
        self._config_new_cse_api_uris()
        first_page = self._search_page(
            random.choice(self._cse_api_uris), query
        )

    first_result = iter((first_page.get("results", []),))

    if len(first_page.get("cursor", {}).get("pages", [])) <= 1:
        return first_result

    # If more then one page available, yield them all on-demand.
    yield from chain(
        first_result, (
            results
            for p in tuple(self._pages.keys())[1:]
            if (
                results := self._search_page(
                    random.choice(self._cse_api_uris), query, p
                ).get("results", [])
            )
        )
    )
```

The last method of the CseHook class

client-side generated URIs or if it is explicitly told to renew them, execute *self._config_new_cse_api_uris* so it can configure new intercepted client-side generated URIs.

- Request the first page using the *self._search_page* method. The arguments passed to *self._search_page* will be a client-side generated URI randomly picked from the *self._cse_api_uris* list and a quoted query string.
- If the first page already returns an error key, it can mean two things: the Programmable Search Engine URI was temporarily banned or the client-side generated URIs got old and need to be renewed. If the main Programmable Search Engine URI was temporarily banned, return False and pause execution. If the client-side generated URI just got old, renew them and request for another first_page.
- If the cursor returned by the first page says that only one page is available, return an iterator with the results of the first page. If there are more pages to iterate through, proceed with execution and yield the iterator with the first page results plus an iterator with the results for the next pages - only if they return more results.

```
from random import randint, shuffle
from time import sleep

from english_words import english_words_lower_set

from config import CSE_URI, RENEW_CSE_DEFAULT
from csehook import CseHook, WiredDriver


if __name__ == "__main__":
    wired_driver = WiredDriver()
    amount_of_requests = 0
    try:
        cse_hook = CseHook(CSE_URI, wired_driver)

        english_words_list = list(english_words_lower_set)
        shuffle(english_words_list)

        # When reaches 0, its time to renew client-side URIs.
        requests_to_reload_cse_uris = RENEW_CSE_DEFAULT

        for word in english_words_list:
            if requests_to_reload_cse_uris <= 0:
                pages_results = cse_hook.search(word, renew_cse_uris=True)
                requests_to_reload_cse_uris = RENEW_CSE_DEFAULT
            else:
                pages_results = cse_hook.search(word)

            # It returns bool (False) if temporary ban was imposed.
            if isinstance(pages_results, bool) and not pages_results:
                break

            for results in pages_results:
                print(results)
                amount_of_requests += 1
                print(amount_of_requests)

                requests_to_reload_cse_uris -= 1

    finally:
        print(f"Number of requests: {amount_of_requests}")
        wired_driver.instance.close()
```

__main__ file content

Now that all the attributes and methods of CseHook were detailed, there is only *__main__* left to explain.

Main

The *__main__* file contains the instantiations made to WiredDriver and CseHook, along with a few more things.

The following activities are present in this file:

- A WiredDriver instance is created.
- An *amount_of_requests* counter is initialized as zero (0). This will serve to count the amount of requests made to client-side generated URIs and to exhibit the number at the terminal, so the amount of requests can be monitored without needing to store all the results locally.
- A CseHook instance is created by specifying a previously created Programmable Search Engine URI and a WiredDriver created instance.
- A list containing the English words in lowercase is initialized and shuffled afterwards.
- A *requests_to_reload_cse_uris* counter is initialized with the *RENEW_CSE_DEFAULT* (38) configuration value. This will serve as a negative counter so it can ask the CseHook.search method to renew the client-side generated URIs (intercept new ones and save them in a class list).
- Like cited previously, if the *requests_to_reload_cse_uris* count reaches zero, renew the client-side generated URIs and set *requests_to_reload_cse_uri* to *RENEW_CSE_DEFAULT* again. If it is still bigger than zero, proceed requesting with the already intercepted client-side generated URIs.
- If the returned *pages_results* is False, break the execution because the Programmable Search Engine was temporarily banned. If it is an iterator, proceed with iterations.
- For each iteration made through *pages_results* - i.e., for each requested page, print the page results, sum one to *amount_of_requests* and print the variable value. Next, after requesting a page, subtract one from *requests_to_reload_cse_uris*.
- When the code is interrupted, print its final *amount_of_requests* number.

Obtained Results

To prove that the intercepted client-side generated URIs could be explored on a large scale, the code was left running for 24 hours to see how many requests could be made without interruptions or banishments within

that time frame.

Surprisingly enough, even though GeoNode proxies were used - and a lot of them were not even functioning correctly, which delayed the amount of iterations/requests that could be made in the same time frame without these obstacles - 15,706 requests were made to Google resources, all of them containing real and valid Google results just before the execution was interrupted. It means that the PoC would iterate through all the lowercase English words in less than two days - given that the set has 25,480 words in it.

It also means that it has surpassed the daily quota limits (10,000 a day maximum) allowed by the official Google CSE JSON API - the one without Restricted JSON - by a lot, and surpassed even more the Google CSE JSON API free usage limits (100 a day maximum).

Conclusion

The PoC demonstrated that, within a time frame of 24 hours, 15,706 requests were made and successfully returned Google CSE page values using the intercepted client-side generated URIs as a facilitator, in order to obtain JSON format results. With basic user-agent randomization, client-side generated URIs' frequent renewal and proxy changes, one could avoid Google's detection mechanisms and consume its data without the need to subscribe for its JSON CSE API fees.

References

Selenium Wire: pypi.org/project/selenium-wire/
Requests: docs.python-requests.org/en/master/
User-Agents: github.com/tamimibrahim17/List-of-user-agents/blob/master/Chrome.txt
Geonode Proxies: geonode.com/free-proxy-list
Google CSE: programmablesearchengine.google.com/about/
English-Words: pypi.org/project/english-words/
Regex101: regex101.com/
Custom Search JSON API rules: developers.google.com/custom-search/v1/overview

The Infosec Professional Song

by aestetix

This should be sung to the tune of Gilbert and Sullivan's "Modern Major General"

I am the very model of an infosec professional
I've mastered all security, from digital to physical.
My expertise and training can tell if a threat is credible,
And I'll ensure that my exploits are plausibly deniable.
Blue Team hackers always try to hold bad guys accountable,
In this my record of success is really quite remarkable.
When playing CTF it's true that my teams almost never lose
Because I always know the best and latest hacking tools to use.

It is important that my skills are always up to date and thus,
I passed my CISSP in record time with little fuss.
In short, in making things secure, from digital to physical,
I am the very model of an infosec professional.

I turn on stack protection when I set up a new Linux box
My SSH port knocking sequence comes from Russell's paradox
I'm fluent in syscalling and can speak directly with D-Bus
I write C code with objects and I only need a single plus.
My custom CFLAGs harden code to make the strongest binaries
My system structure layout is superior to systemd's!
I'm so elite that often times my daily life can be a bore -
When I get sick of normal work, I hexedit my Linux core.

I used to be a cracker once but I decided to reform
So now I spend my day job reading Hacker News and Packetstorm
In short, in making things secure, from digital to physical,
I am the very model of an infosec professional.

The Hacker Perspective

by m0xya

I have always known from an early age that I was different, that I (as others have so eloquently put it) was "not normal." My interests from an early age were different to my peers; they were mainly technical in nature. My father was an electronics engineer and the house was always scattered with devices and piles of components. I grew up surrounded by soldering irons, oscilloscopes, and bundles of wires.

He also had a garage/workshop where he had a machine shop. He would tinker away rebuilding cars, boats, even an airplane at one time. Let me tell you, every house should have a lathe. They come in very handy.

I was always encouraged to have a go at things, to play with the tools and equipment, even when I had no idea what I was doing with them. I was always carefully watched, but I was free to play, free to try things, and to make mistakes. I was lucky enough to have been born before the blight of helicopter parenting, where all risks are mitigated and environments sanitized to keep children safe. It was not that my parents were uncaring; in fact, it was quite the opposite. They understood the need for space to grow and gave it to me in abundance.

This level of freedom was very different when compared to some of my friends and their families. However, for me at the time, I did not know any different. Many of my friends had their childhood micro-managed and planned out. I doubt my parents actually knew what they were doing; they were doing what felt right and natural. I was given the space to develop in my own time and in my own way.

One of my very early memories was from Christmas 1981. I was about four years old, and my parents had bought me a Sinclair ZX81, the one that came as a kit and needed assembling. I knew it was from them and not Father Christmas, for two reasons. I knew where things were hidden, as I had found the hiding place one day when exploring. Also, receipts were kept on a spike on their desk, and I could read.

So there I am on Christmas morning, surrounded by small bags of components and with a soldering iron in my hand. My father talked me through what each of the components were and how they worked in very basic terms. I was four after all, and it didn't make much sense to me, but I knew even then that it was fun and that I wanted to know more. It was my first computer and I had built it myself. I would play on it for hours and hours. Typing in example programs from the manual, making mistakes, and trying to work out what had gone wrong. They were my first steps into the world of computing.

In the years that followed, I progressed on to other computers, a Commodore VIC-20, a BBC Micro Model B, and a BBC Master 128. Looking back on it, neither of my parents had particularly big incomes and so must have scrimped and saved to buy these for me. In the early 80s, there was a big drive by the British government to train the next generation in computing and, thanks to my parents, it paid off.

Academically, I suppose I was middle of the road, with a "could do better" being the usual feedback from my teachers. I enjoyed school, with science and math being my favorite subjects. I was also quite good at art and design. Despite all this, I felt detached from my classmates and teachers. I had a constant sense of alienation, that something was wrong. That same feeling of being different, of not being normal.

Even then, I could see what was happening. We were being taught to pass tests, not to think for ourselves, not to question. We were pegs, slowly forced

into the uniformed rack of society. Anyone not quite the right shape would be smoothed out. They would have their rough edges knocked off as they passed through the system. The others who did not fit in were abandoned.

I managed to get into college and university, however, the system was still the same. You fit in or you failed. That sense of being different peaked at university. It had a massive impact on my confidence. That daily reminder of not being good enough, of not meeting expectations, of not being like the others, not being normal. It put me off formal education of any type. It was obvious it worked for the majority, but utterly failed others.

I graduated, just. I have never looked back....

It is at this point I must introduce someone else who had a major influence on me. One of my oldest friends lived nearby in a big old house with his parents and three older brothers. It was always a busy and noisy place, with each member trying to outdo the others. In the middle of this whirlwind of chaos was a very quiet man, my friend's father. He was a medical doctor; however, at the time he ran the medical computing department at Manchester University. He was mildly eccentric and massively into computers. He always reminded me of Doc Brown from *Back to the Future*.

He was also an amateur radio operator. He had huge antennas hanging off the roof and feeder cables running throughout the house. I would spend countless hours sitting on a stool next to him, watching what he was doing. I can still recall the peace and quiet of his room, while from every other direction there was madness and noise. It was an oasis of calm and computers.

You can understand my annoyance then, when at regular intervals my friend or one of his brothers would come rushing into the room saying something like "Come on Dad, he doesn't want you boring him to death." I would be dragged away to do something else, to play a game or run around making noise. I was not bored, I was enthralled, and when I had the opportunity I would sneak away and head back.

At the time, it did not dawn on me, but my friend and his brothers were revealing more about themselves than they realized. They found what their father was doing to be boring and uninteresting, so therefore, so should I. How wrong they were.

Both of these men, my own father and my friend's, gave me the opportunity to explore technology without it feeling like a lesson. I could work things out in my own terms and at my own pace. I could try things out and make mistakes.

It was not until I left formal education that I actually started to learn things. I could study what I wanted, how I liked, and in my own way. There were no teaching plans or targets to reach, no exams to pass. Just learning the way it is meant to be. Fun.

From the age of about 21, I studied whatever subjects and ideas I wanted to. I read up on massively varied subjects: art, medieval architecture, physics, psychology, anything and everything that interested me. However, there was always one subject which drew me in more than any other: computer science.

I had always had a computer of one sort or another, and it had never even dawned on me that I should study it at college and university, something for which I am eternally grateful. My love of the subject would have probably been killed by the formality of education.

You see, I do not learn by rote. I need to understand at a fundamental level what it is I am trying to learn. I am reminded of something Richard Feynman once said: how you can be taught the names of a bird in every possible language, but that you will still not know what the bird is. All you have is its name; your knowledge of the bird is still the same. I need to know more than just the name of a thing.

It is at about this time that I got my first job as a programmer. The interview did not initially go too well. One of the interviewers did not understand how I could do the job without a university degree. He was so blind to the possibility of someone being capable of learning independently that he voted against me. Luckily for me, there were others on the panel who did not share his point of view.

I had been able to answer most of their questions. However, the thing that

gave me the edge, the thing that tipped the vote in my favor was my ability to draw on other subjects. If I had been formally educated, the path would have been narrow. Learning objective A leads on to B and C, etc. During the interview, I had discussed in detail many different technologies and applications. I was not blindly following the path of ABC. I could see connections that were not obvious, as I had both a deeper and broader understanding of the subject. I knew more than just the names of things and their order.

This technique of learning has stood me in good stead and I have not stopped in my quest for knowledge. If anything, it has accelerated since then. It has been almost 20 years since that first interview. I have moved on; I have never stopped learning new things.

Despite not having any formal education in computer science or engineering, I am currently working as a senior security consultant for a global cyber security company. I am drawing on an eclectic range of skills and knowledge that I gave to myself. This allows me to work on a vast range of jobs, from infrastructure and web app reviews to hardware and reverse engineering. I am surrounded by a group of colleagues who all share similar interests and ideas. It is a great mixing pot of knowledge and experience.

Do I still have that sense of being different? Yes.

Do I still have that sense of not being good enough? Yes.

Let me share with you a little secret. It is the same secret most of my colleagues share, but would be unwilling to admit to. That feeling of inadequacy never leaves you; it is always there. It even has a name: "impostor syndrome."

However, it is how you manage this condition that is important. You could give up and accept the fact you don't know enough. You could pretend to be like everyone else and hide away in the crowd. Keep your head down and let that feeling of resentment grow.

Alternatively, you can use it to your advantage. So what if I don't know enough? I can learn new things. Thank you for highlighting that gap in my knowledge. Tomorrow I shall come back knowing more than I do today.

I shall finish off by leaving the reader with a few words of advice. Make of them what you will. They have served me well.

I forget its origin, however, there is a rule I try to follow: "You should always try to be the person in the room with the least knowledge or experience."

That way, you always have the opportunity to learn from others. If you're the master holding court with a room of minions, what chance do you have of growing or learning? Yes, it is a great ego booster but, other than that, I see no benefit.

Try to let go of your ego and let humility be a guiding force. I have noticed as I have aged that being humble opens more doors than it closes. Humility is not to be mistaken as being weak - far from it. The stronger you are, the less you have to prove yourself. You also have a greater chance of people opening up to you and sharing, be that experiences or knowledge.

Accept the fact that you will never know everything (see humility). It is a thrilling sensation, as it means you will never stop learning.

Above all, be yourself. Do not worry what others think of you. Most of the time people are only thinking about themselves, not you.

If you are presented with a problem with no obvious solution, don't worry about thinking outside the box and making alternative suggestions. That ability to think differently, to step back and see the big picture, to not be normal gives you the edge.

I embrace my difference.

m0xya (Phil) works/tinkers at a global cyber security company. He is a HAM radio operator, and in his spare time enjoys repairing old computers and Land Rovers. More information can be found at: https://m0xya.net/

HACKER PERSPECTIVE *SUBMISSIONS STILL CLOSED - STAY TUNED!*

YouTube Is Not a Safe Space

by Men Without Hats

The last few years have been extremely stressful. Given all the scary things going on in the world, sometimes we need levity and a good laugh. To this end, there are a number of themed channels on YouTube, one of which produces family friendly pranks. Recently, no videos from that prank channel were showing up in the general feed. Upon deeper inspection, it turned out that the YouTuber running the channel had had his most recent video flagged by YouTube for not being "safe." The algorithm had determined his video contained both sex and nudity, although it clearly had neither. He appealed, hoping for some common sense, and within 15 minutes the appeal was denied. He expressed a lot of frustration at this, including doubt that a live human had actually reviewed his appeal. He then declared that, after 15 years on the platform, he was jumping ship to another video platform that was algorithm-free.

While the impact of algorithms is not limited to this YouTuber, and seems to be non-partisan and non-opinionated, it is the latest in a decades-long series of attempts to "solve" complex problems with simplistic solutions that look good politically but have all sorts of far reaching negative consequences. In this article, we'll take a look at this history, then at the actual problem YouTube is trying to solve, and see if we can come up with any alternative solutions.

In the 1980s, according to right wing media and talk radio, Satan worship among teens was on the rise. There were allegations of hidden messages in rock music, including rumors that if you played the B-side of a record backwards, you would hear a personal message from the Devil. In response to this "Satanic Panic," Tipper Gore (wife of former Vice President Al Gore) spearheaded an initiative called the Parents Music Resource Center (PMRC) in 1985. The idea was to place labels on rock music to warn parents that it included lyrics that were explicit or worse, so that parents would be able to protect their children from Satan worship.

Naturally, musicians revolted, angered that government imposed labels on their lyrics (their free speech) were preventing sales and creating unfair judgments on their words. This led to a congressional hearing in which musicians such as Frank Zappa brilliantly stated their cases for free speech and made suggestions on how to solve the issues at hand without compromising their art. While the legacy of these hearings left us with the now-familiar labels on music CDs noting explicit lyrics, this is by no means a settled matter, and the arguments at play then are completely applicable today. Ironically, the hearings are also available on YouTube.

The ugly head of "save our children" reared itself again in the 1990s with the rise of underground raves. At the dawn of rave culture, we saw free expression in the form of music, art, and in many cases, free love. Soon, another kind of freedom arrived: drugs. While the vast majority of people were responsible with their use (or non-use) of drugs, a small minority suffered high profile overdoses and even deaths. This terrified parents, who did not want their children doing drugs, and the parents demanded accountability from their politicians. As a result, strict laws began going into place to punish not only the organizers of raves where drugs were used, but also the venue owners, who often did not know the nature of the events. One of the final results was the RAVE Act, passed in 2002, which remains a prime example of a government overreach that is destructive in the name of safety and causes many more problems than it solves.

It's also important to recognize that during this time, the rave community developed a number of self-policing solutions, such as ensuring event organizers had basic CPR training. There were even community-run organizations like DanceSafe that did pill testing at raves to make sure the drugs did not contain poison. A key lesson emerged during this time: many people wanted to use these solutions and claim that they were practicing "safe" drug use. However, others recognized that there is no such thing as safe drug use, and coined the phrase "drug harm reduction." This small but significant clarity of language recognizes an important truth from which YouTube could surely benefit.

Finally, we need to state that those who forget the lessons of the past are doomed to repeat them. After 9/11, many extremely absurd and unconstitutional laws were passed in the U.S. to "keep people safe," including the creation of the Department of Homeland Security, which included the TSA. If the end goal of the TSA is to ensure that airports and air travel remains a "safe space," it is one of the greatest failures of domestic policy in American history. In addition to the endless absurd rules, such as checking ID (challenged in court by John Gilmore),

taking off shoes, or not allowing "liquids" to pass through security checkpoints, the only thing the TSA has been successful with is ensuring that air travel is an absolutely miserable experience that brings lots of profit to corporations funding ineffective security machines at taxpayers' expense. If we attempt to make sense of the endless spider web of contradictory and ever-changing regulations, we are looked upon with suspicion by contracted goons who LARP as law enforcement and somehow have the power to deny our ability to fly on a whim. Another fine example of extreme over-correction in the name of "safety."

We can see from this historical account that what YouTube is doing is not new, but simply the latest in a long line of hammers trying to smash anything that looks remotely like a nail. But in all of this, it's important to ask what a "safe space" is. Perhaps if we clarify this, we can understand where YouTube is coming from.

For our purposes, we'll define a "safe space" as a controlled environment where someone is able to explore difficult or challenging topics without judgment, usually with the assistance of a trained/licensed professional. For example, if we have a fear of frogs, a therapist might play sounds of frogs croaking, show us pictures of frogs, and slowly get to the point of actually seeing and touching a real frog. The idea here is to slowly introduce things that gradually push us out of our comfort zone and make us stronger.

However, this is the opposite of what YouTube is doing. YouTube seems to want to play protector in the name of safety. To really expose this, we need to reframe how "safety" is being used, and show exactly who is being "protected." When George W. Bush was president, he created "free speech zones" to allow people to peacefully protest his illegal invasions of Iraq and Afghanistan. Often these "zones" would be a considerable distance from his entourage, and anyone attempting to voice their free speech outside of these zones would be arrested. In another example, and one that is making an unfortunate comeback, banning books to "protect children" usually helps parents who don't want to deal with concepts they find uncomfortable. This is marginally better than, but not so different from, governments banning books to prevent people from considering certain ideas that might upstage political power. In these examples, both the free speech zones and banning books create a "safe space," but one that is only helpful to a select few.

But maybe we should ask what YouTube is trying to achieve here. After all, why is sex and nudity a problem? Indeed, "safe space" seems to have multiple interpretations. To a Big Tech company like YouTube, it seems to mean a puritan and sterile environment in which to sell ads. But to many people, the exact same phrase means a place to show nudity, whether it be classical artwork, porn, or anything else. And if YouTube is actually trying to use this "safe space" concept to make money from advertisers, have they forgotten the historical mantra that sex sells? Or maybe they are afraid of getting sued by the same people who seek to impose book bans.

We should also take a moment to reflect on what "safety" is. The truth is, just because we feel safe does not mean we *are* safe. Take computer antivirus companies: they ask us to pay a monthly or annual fee to run virus scans periodically. What they do not mention is that the only "safe" computer is one that is turned off and unplugged. Antivirus software can certainly help reduce your chances of getting a computer virus, but the reality is that they are selling the *feeling* of being safe from viruses, much like an insurance company. YouTube seems to be trying to do this too. In using their algorithms to flag and remove unrelated videos in a broad stroke, by the law of large numbers, they will also catch a few videos that are actual offenders. This is a bit like a fisherman who has a huge net that catches 100 old boots and a single fish. Technically, he was successful at fishing, but the reality is that he probably needed a better net.

How can we solve this? It's a hard problem, not least because YouTube is completely non-transparent. Right now, based on experiences like the opening anecdote, we really don't have much reason to trust anything they say. While demanding the algorithm be made public is a bit much, they could produce a weekly or monthly report showing how many videos the algorithm took down, and what percentage were appealed. If we had a history of reports like this, and we could see trends - such as a reduction in appeals - it would help build confidence in their system. If we were able to put this data alongside public anecdotes, and we found similar trends, that could be enough to create sufficient confidence, and YouTube would not have to worry about pretending to be a "safe" space.

What Do You Mean You Don't Have a Responsible Disclosure Program?

by Sp3nky

No product is perfect. You can have security involved from the beginning with the dev group, and something will be missed. This is still going to happen when you have a fully developed, mature DevSecOps group and program in place. While impressive, it doesn't matter. The group may have a checklist they work through as part of the procedure. While this is not optimal, there will still be people who want to check the box and not be creative with their solutions. Looking forward, we can't predict future technological advances. Soon, a present vulnerability which may not have been thought of may be detected and exploited. This has been experienced in the past, unfortunately. New technologies being implemented also provide for new attack methods, which are created frequently. These methods may be applicable to being applied against earlier products. Knowing all the advances that will be created in the next 10 to 15 years is not plausible.

With unknown future attacks that may be applicable to your product or services, the prudent move would be to attempt to plan for any future attacks. This may take many different paths for an organization. A CISO may want to put some process or procedure in place to meet the issue head-on. Any process in place well before an incident clearly would be beneficial. When there's an issue, it is always better to follow a plan. In the alternative, there's always the reactive model, which is never a good thing. The CISO would need to magically come up with a plan on the fly, which is critically needed, in an instant without having the opportunity of putting a couple of weeks of thought and vetting into it. Searching Google for a plan at the last minute isn't exactly the best situation.

This is where a responsible disclosure plan comes into play. When a researcher or third party finds one of these pesky vulnerabilities in your product, with a responsible disclosure process in place, the issue is manageable. This encourages the testing process to remove as many of these issues as possible up front. The company has their staff working on security, along with researchers throughout the nation and other countries also rooting these out. The researcher or lab finding the vulnerability has a road map to follow when disclosing this. There is a certainty with the process and the people involved have a method of showing the lack of malicious intent and clear focus of helping the industry and company with improving their product.

While this isn't the most glamorous topic, responsible disclosure programs are pertinent and a tool to give researchers some level of assurance that at least no legal action will be taken. What brings this about is the workplace recently completed a limited scope pentest of several consumer products (e.g. testing eight hammers from different manufacturers). Through the test, too many vulnerabilities were found. There was no data leakage between these. Each of the manufacturers was contacted individually (again, no cross contamination of test results), asking them what their responsible disclosure program was. Each email included the lab and possibly had information to communicate. This seems easy enough. Each manufacturer was emailed, letting them know that their product may have issues, and we wanted to communicate these to them in whatever format and method was best for them. Help me to help you. Very simple.

Well, not so much. It turns out manufacturers did not put an emphasis or much thought into this. There were two manufacturers who had something in place. One was mature, and the other not really, but they were moving in the right direction. The general response was in two forms. There was a lack of

response, which is bad. This lack of attention to a valid issue speaks volumes as to the weight and care placed with their products' cybersecurity.

The other general response received was more generic, not addressing there being an issue. These appeared to be more of a copy/paste from another document. This fit the circumstance like a square peg being forced into a round hole. The manufacturers were all contacted at least seven times, except for the two who had some form of a plan in place.

We all know the value of getting ahead of an issue. Handling a minor issue is so much easier than when it explodes through the network. We've seen what happens when the organization is not proactive. One issue with cybersecurity as a task and function is that it's difficult to quantify the benefits. These aren't tangible as this is with other disciplines (e.g. tax accounting saving the company six million dollars). The same problem occurs with the responsible disclosure programs. Management may view this as a money pit, with the labor, overhead, and any perks provided to the researchers.

There is a need for these programs. The researchers need to know they can do the research and testing for the product and provide real results for free, and there will be no legal repercussions. The alternative is to treat the non-malicious researchers as quasi-criminals. Naturally, the researchers would not want this and may move towards releasing their findings anonymously or in other venues with no notice.

The responsible disclosure program is a prudent avenue to follow. The company receives valid tests to help them with their product from researchers for free or with some bounty. In comparing the bounty amount with how much it would cost the company to be surprised with an exploit, the bounty and its benefits are clear.

The Coolest Hacker Multitool On the Market: The Flipper Zero

by Andrew "OGSkeltal" **ogskeltal@pm.me**

I am not affiliated with the Flipper Zero team, but have found substantial positives to using the product. I believe security professionals will benefit from owning one, so I wrote the below short piece advocating its uses. With wider adoption, there could be an increase in competing products, allowing users greater choice. The Flipper Zero opens a lot of possibilities for unique hardware devices targeted at, and made by, the hacker community.

Introduction

Imagine a device where you hack almost any wireless (IR, Sub-gHz, Bluetooth, RFID cards) and hardware device. It fits in your hands and it's fun to use. It seems almost science fiction, but it exists! It is the only type of device I have found that does this.

I recently purchased a Flipper Zero device and was fortunate enough to get it quickly, considering difficulties in shipments. I can say - without a doubt and for lack of a better word - this device is the coolest piece of technology I have seen in a decade. It is billed as a "hacker multitool" and lives up to its name. The Flipper Zero can work with various wireless technologies and has GPIO pins for hardware exploration.

Physical Device Features

The Flipper is slightly larger than a credit card and can easily fit into a pocket. It has GPIO pins for testing and expansion boards, a micro-SD card slot, and charges via USB type-C.

Modules

Sub-GHz transceiver - With the official firmware you cannot transmit, but the team behind the Flipper Zero allows custom firmware. Customization turns the flipper zero into a "baby Hack-RF." You can easily do rolling code attacks and signal analysis in the SubGHz range.

125kHz RFID Antenna - With this, you can access low frequency proximity cards, which are used in many access control systems.

Near Field Communication (NFC) - Read, write, and emulate high frequency tags. I have used it to read the chip in my credit cards - spooky! As more applications are developed, more functionality will be added.

Bluetooth - I have not used the Bluetooth functionality often, but the Flipper Zero website has the following to offer on the subject: "Flipper Zero has a built-in Bluetooth Low Energy module. As with other Flipper wireless features, we will be providing an open-source library for

adding Flipper support to community-made apps. Full BLE support allows Flipper Zero to act as both a host and a peripheral device, allowing you to connect your Flipper to 3rd-party devices and a smartphone simultaneously."

I have used the Bluetooth module to update my Flipper Zero, since the application on Android and IOS is already out.

Infrared Transceiver - Supports transmit and receive. If you remember the old days of the IR blaster prank device, this is similar. Large amounts of codes already exist that can be pre-programmed (more information is provided at the end of the article). Additionally, the Flipper can "learn" the codes and you can attempt to manipulate the device you are working on. I have used this to annoy my wife by turning off the TV!

Hardware Exploitation - Per the website: "Firmware flashing, debugging, and fuzzing. It can be connected to any piece of hardware using GPIO to control it with buttons, run your own code and print debug messages to the LCD display. It can also be used as a regular USB to UART/SPI/I2C/etc adapter."

One Wire Keys (ibutton) - 1-Wire connector to read iButton (aka DS1990A, Touch Memory or Dallas key) contact keys. This old technology is still widely used around the world. It uses the 1-Wire protocol that does not have any authentication. Flipper can easily read these keys, store IDs to the memory, write IDs to blank keys, and emulate the key itself.

BadUSB - The flipper Zero supports BadUSB and has a module for it. Many scripts have already been converted for use.

U2F - The Flipper can act as a universal second factor authentication key. It is currently only supported through USB, but Bluetooth is in the works.

Technical Specifications as per Website:

MCU (Microcontroller Unit)
Model: STM32WB55RG
ARM Cortex-M4 32-bit 64 MHz (application processor)
ARM Cortex-M0+ 32 MHz (network processor)
Flash: 1024 KB
SRAM: 256 KB
Display
LCD Monochrome
Resolution: 128x64 px
Controller: ST7565R
Interface: SPI
Diagonal Size: 1.4"
Battery
LiPo 2000 mAh
Seven days approximate working life (have tested this, it works as advertised)
Sub-1 GHz module
Chip: TI CC1101
TX Power: 0 dBm max
Frequency bands (depends on your region):
315 MHz
433 MHz
868 MHz
915 MHz
Note: Unlocked firmware exists, so if you flash the device you can RX/TX on all of these frequencies. If using official, you cannot transmit, and only receive on bands depending on region.
Near field communication (NFC)
Frequency: 13.56 MHz
Supported cards:
ISO-14443A/B
NXP Mifare Classic/Ultralight/DESFire/etc
FeliCa
NFC Forum protocols
RFID 125 kHZ
Frequency: 125 kHz
Modulation: AM, PSK, FSK
Supported cards:
EM400x, EM410x, EM420x
HIDProx, Indala
GPIO
3.3 CMOS Level
Input 5V tolerant
Up to 20 mA per digital pin
Bluetooth LE 5.0
TX Power: 0 dBm max
RX Sensitivity: -96 dBm
Data rate: 2 Mbps
Buzzer
Frequency: 100-2500 Hz
Sound Output: 87 dB
Type: Coin
Vibration Motor
Force value: 30 N
Speed: 13500 rpm
Infrared
TX/RX range: 800-950 nm
TX power: 300 mW
Ibutton 1-Wire
Operate modes: Reader/Writer/Emulator
Supported protocols:
Dallas DS1990A
CYFRAL
Physical
Size: 100 x 40 x 25 mm
Weight: 102 grams
Body materials: PC, ABS, PMMA
Operating temperature: 0 ~ 40 °C
GPIO pinout can be found here: `cdn.➥flipperzero.one/6xboq.png`
Official link: `flipperzero.one/`
Collection of official and unofficial software: `github.com/djsime1/awesome-➥flipperzero`
BadUSB Flipper Zero converted scripts: `github.com/I-Am-Jakoby/Flipper-➥Zero-BadUSB`

Ramifications

Issue Feedback

Dear *2600*:

This morning I read E.V. Rhode's article about self driving cars ("Will You Let Your Car Drive Itself?") in 39:3: "After explaining my previous experiences with the cruise control, my companions agreed to trying it, and to watch closely should anything happen. After engaging, we drove for 20 or 30 minutes without incident - until my car suddenly slammed on its brakes... driver behind us swerved... no obstacles or vehicles ahead of us."

This one resonated with me personally. This feature has saved my or someone else's life at least once in my Pacifica (2020). But I always posed this very question... what happens when the software thinks there is danger when there isn't and *creates* danger?

I'm following up with the writer and the NHTSA (National Highway Traffic Safety Administration) to find out if this is next part is accurate:

"This office has received 758 reports of..." this exact same thing. I too have almost experienced this. My car thought there was danger, alerted me, and started to slam brakes. I was driving normally - no cruise control. Yet my car almost caused a serious incident because the road curved and there was a breakaway to the left to allow people to turn.

I still believe in this tech... but this one I thought important to note.

Jeffrey

There are certainly going to be issues as this technology continues to experience growing pains. The real question is whether it eliminates more issues than it causes. We think there's great promise here, but this all has to take place in an open environment where such stories aren't covered up or suppressed. We look forward to hearing more.

Dear *2600*:

Super happy with the back issues I've gotten so far. I'm curious about the cover of the Spring 1989 issue - seems to be some sort of reference to global politics and the Middle East with the classic Abbey Road imagery, but I'm not sure how it related to any of the articles in the magazine itself at all. Any insight on this? Great work on *2600* y'all!

jae

Covers don't always reflect the content of the issues, but oftentimes are based on what's happening in our world at the time. We don't usually do this, but for you we'll reprint the explanation of that cover as outlined in our Hacker Digest *compilation for Volume Six (1989):*

"Spring 1989 featured an Abbey Road *takeoff with a Salman Rushdie flavor. It was in February that Ayatollah Khomeini issued a fatwa against Rushdie, the author of* The Satanic Verses*, a book seen by some as spreading blasphemy against Islam. The idea of someone being put on a hit list for the words they wrote was true blasphemy to writers and free thinkers everywhere, ourselves included, which led to the idea behind this cover. The Ayatollah himself is pictured, dressed in black, as the first of the four men crossing the street to Rushdie's house. In his hand is a copy of the Holy Koran (as it was spelled in English then). The turbans of the three assassins following him are Sikh rather than Arab, which served as a bridge to the Beatles' embracing of Indian culture (Hinduism in their case). As in the Beatles' famous album cover, different footwear is apparent in those crossing the street, and one of the four is out of step. Of course, we had to insert a British payphone in the distance. Even the license plates had meaning, with staff and their friends hiding their addresses there and 7383USAF being an allusion to someone we knew named Pete (spelled out on a touch tone dial) joining the Air Force. As for the mini-cover, there was a picture of a guy, possibly actor Raymond Burr, next to an excerpt from* The Freedom Fighter's Manual*, a propaganda leaflet dropped over Nicaragua by the U.S. government in the 1980s. This particular excerpt contains instructions on how to sabotage telephone lines. Finally, the mini-cover corrected an omission from 1988 - the Spring issue of that year had failed to carry on the tradition of having an exclamation point on the cover of the first issue of the year. So, for Spring 1989, we included two of them."*

Yes, those of you who subscribe to The Hacker Digest *get that kind of detail for each of our covers! Plus a whole lot of other details we would never have room for here.*

Dear *2600*:

In 39:1, the author 75ce8d3ff802ff42 suggests in "Harnessing Cryptocurrency Miners to Fight Climate Change," something that's a very old and tired misconception about misappropriation of resources in general, and often suggested to support cryptocurrencies in particular.

If the author has time, I suggest they read Hazlitt's *Economics in One Lesson: The Shortest and Surest Way to Understand Basic Economics*, specifically the first applied lesson: "The Broken Window."

Since many cryptocurrency advocates are not interested in learning existing economics before they attempt to replace it, a shorter version is to watch *The Fifth Element*, and realize that "construction from destruction" (what the author is proposing) is the motivation of the film's villain.

Do you want to be the villain?

SB

We eagerly await the response.

Queries

Dear *2600*:

Hey everybody! I might sound quite stupid! But I was checking into buying the yearly subscription of the actual magazine, but I'm not so sure how many

magazines I'll receive! It's not specified on the website! If anyone can help me out by explaining, it would be awesome!

Ricardo

We are quarterly! So a yearly subscription will get you four issues! (Exclamation points are contagious!)

Dear *2600*:

Why does the MOTD (message of the day) on your IRC servers have a text about the importance of firearms, credited to some C.S. Wheatley? Why have that as an MOTD of an IRC server for hackers?

Tiago

The quote we see now is: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety" attributed to Benjamin Franklin. While some view that as having something to do with firearms, it's far more relevant for the concept of actual freedom, such as the right to privacy, which is always being sacrificed in the name of safety. However, the quote itself is said to have been addressing a tax dispute and is actually closer to advocating the opposite of what it's commonly used to justify in the present day. (If there was another quote there, we're not aware of it, but the one that's there now seems to fit.)

Dear *2600*:

Has anyone tried calling via the dime line recently? I'm interested in this bit of telecom history. I notice that the dime line now seems to have a seven digit code.

CK

We really wish you had sent us more info, such as what the number is. We'd like to know more of its history as well.

Dear *2600*:

I have a friend that passed away and his family obtained a court order to unlock his phones but Apple refuses to assist. Any ideas? Thanks in advance.

NP

According to Apple, they can help remove their feature known as Activation Lock, which is designed to prevent phones from falling into the wrong hands by disabling them remotely. However, they claim not to be able to get around passcodes users assign to their phones: "Please note that devices locked with a passcode are protected by passcode encryption, and Apple can't help remove the passcode lock without erasing the device." If there's another way, we'll certainly share it.

Dear *2600*:

I would like to know if *2600* is on the Columbus, Ohio smart city project or if it is listed among any of the California vendors that support it as the phone hacking may be of interest to the government office copied. The phone hacking can damage public offices.

+1614

We have no idea how we could be a part of this, nor how we would possibly be a California vendor. But we're certainly interested in the phone hacking.

Dear *2600*:

I found a great way to sign up for trial services with a credit card over and over: privacy.com virtual single use credit cards. Unfortunately, my account got flagged after seven or eight uses for the same merchant. Does anybody know of another company, service, or method - ideally free - that I can use as an alternative?

AB

It seems pretty obvious that if you're going to use this method of getting a free trial period that lasts much longer than it should, you'll need to make new accounts as frequently. We find privacy.com to be highly rated for keeping your identity and address out of the hands of merchants. If you somehow managed to get blacklisted from their service, we'd sure like to know the details. Some alternatives to privacy.com are skrill.com, ramp.com, and payoneer.com.

Dear *2600*:

Can I purchase a link insert on a specific page of 2600.com? If yes, please let me know how much it costs. Thank you.

P.S. Also, do you have other sites that offer paid link insertions?

Chad

We exist in a completely different universe than much of the web. More than three quarters of our office staff didn't know what a link insert was. One hundred percent didn't care.

(So, the answer is most likely no.)

Dear *2600*:

Does anyone know how to produce a true random number in any programming language? I have been trying for over 20 years but have not achieved it. Every random script that I have ever analyzed can be reverse engineered to predict the outcome, so I'm wondering is it even possible to create a true random number?

DN

From The Algorithm Design Manual*: "Unfortunately, generating random numbers looks a lot easier than it really is. Indeed, it is fundamentally impossible to produce truly random numbers on any deterministic device. John von Neumann said it best: 'Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.' The best we can hope for are pseudo-random numbers, a stream of numbers that appear as if they were generated randomly."*

We probably can't say it any better than that.

Dear *2600*:

How does one stay anonymous and private in 2023? Yes, the mini-computer in my pocket that also makes phone calls is very convenient to entertain me or immediately answer any question I may have, yet isn't it also keeping a record of my thoughts and movements? Can you even get a pager anymore? And when you get paged, how do you call people back? (Keep a phone off and only turn it on when necessary? Then you are still revealing your location once you connect and how do you know the phone is really fully off? Use a stranger's phone? Then they still pick up the location. Also, can't "they" install a secret battery that powers GPS/location tracking without the user

knowing?) Or maybe this is a point where we realize that with Internet-connected cameras and satellites everywhere, there really is no option of staying off-grid. Bigfoot, Loch Ness Monster, and Abominable Snowman all don't exist or else we would have found them already with current technologies. Then again, maybe this is just wishful thinking I see in the movies because criminals still get away with crime. If the technology is open and available, why not let the robots track down every criminal and dissident?

GC

At some point, we need to accept where technology is and figure out ways to manipulate it to our advantage. If we have to jump through hoops just to live our lives, we've already lost. There are always going to be clever ways of subverting the system and of polluting databases with bad and/or inaccurate data.

But we also don't have to always be tied to the devices we're told we need. We get to decide if, when, and whether they're needed. So many of us have a phone on us at all times and are always on call. But there's no law that says anyone has to do this. So why don't we unplug more often? The fear and anxiety we feel whenever we don't have our phones are programmed into us. We can train ourselves to not need most of the devices we're told we can't live without. And when we succeed in doing that, we take back a good degree of control of our lives and take it out of the hands of those who want us to submit, always be available, and constantly have our whereabouts be known.

As for pagers, apparently there are still over two million of them in use in the United States. We suggest visiting pagersdirect.net if you want to go down that road.

Dear *2600*:

Hello, I'd like to submit an article to *2600*. What format do you take and do you have length guidelines?

Karl

We can pretty much handle any format, so send us what you're most comfortable writing in. As for length, the sky's the limit. Our editorial staff would prefer longer, more detailed articles, but that doesn't mean short ones aren't also welcome if they adequately cover the topic they're focusing on. The address to send submissions to is articles@2600.com.

Possibilities

Dear *2600*:

We are reaching you once again as regards the estate of Late George, you were made one of the beneficiaries of his estate. Do get back to me at your earliest convenience.

Trustees

Guys, seriously. You need a proofreader. It's not even the .kr (South Korea) domain. It's everything else. Give the guy a last name; it's highly unlikely his first name was "Late." Don't say "me" when signing in the plural. And this was your first email to us, so why are you saying "once again?" We can help you get this right. We'll continue emailing you until you agree to hire us. Let's get this done before the will is read.

Dear *2600*:

I'm following up to confirm if you are interested in acquiring the registrants/attendees list for Information Security Conference BSidesDayton (Dayton, USA, 19 Nov 2022). Attendees Counts: 1,000. Awaiting your response, so that I can share the cost and additional details.

Iliana
Event Coordinator

In case anyone gets such an email, be assured that BSides is not selling or sharing their attendee lists. This is a scam and it comes from all different official-sounding domains. We're told BSides has even gotten this email for their own conferences with claims of a much higher attendee count than the actual number. There is no shame.

Dear *2600*:

Ahh, what to do, what to do... I found this flash drive on the ground at a gas pump driving down the New York State Thruway. The top was caved in; it had been run over. I took my pocket knife and straightened it out enough to fit into a USB slot. Since I was in a rental car, I figured that plugging it into the radio would be something they wouldn't notice when I returned it, so I did, and it started playing marimba dance music. (There were five videos in the root folder.) But do I dare plug it into a computer?

Dave

It looks like you've replicated exactly what this drive was intended for by using it to play music in your car. But on the off chance there's something more, it's always a good idea to have a cheap laptop somewhere that never connects to any other machines so that you can experiment with drives that literally fall off a vehicle.

Dear *2600*:

I am here representing the sale of the "GetSmartCars.com" domain name for $99 on behalf of our client. The domain name is something I believe will be profitable for your business. If interested, kindly let me know your thoughts. Have a great day ahead.

Emily Jones
Domain Consultant

You put one Smart car on a cover (2005) and you're forever hounded by these people. But we're going to adopt "have a great day ahead" as our standard greeting from now on. At least we got something out of this.

Dear *2600*:

Last night I had a dream that I got to a technical interview, and they gave me an easy problem to solve in Python. But I had to cut my code into a sheet of PVC and make stencils of it. Then I had to make pancake batter out of limited ingredients and with no recipe. The pancake batter was then pressed onto t-shirts with the stencil I had made. I had to bake the shirts and send them to the interviewer by USPS. I had seven minutes.

As someone who is very new to this field, are these realistic interview expectations?

Joshua

This indeed seemed quite realistic until you introduced USPS as a means of quick delivery.

Dear *2600*:

I get frustrated with the whole YouTube thing... I already raised this question with others in the hacker community. It will be nice to avoid YouTube, but I am not asking for that. To avoid loss of history, please sync your videos to Odysee, PeerTube, or even archive.org. There are many reasons, but here are a few:

YouTube/Google etc. own the platform. It is not a public space. It is private and they can and *will* ban you eventually; you should not have to change your personality for anyone, not even YouTube unless you're doing things with a bad intention.

Lots of us in the hacker community try to avoid YouTube and other similar centralized sites. It goes against the hacker ethics of decentralization and openness, which is why we build the fediverse and other open, libre, decentralized tools.

Give options to people; do not close them into a monopoly. I know *Off The Hook* is not because of the MP3 and RSS feeds, but what about the HOPE videos? They used to go to archive.org and we used to show them from there to avoid promoting evil sites like YouTube.

I get that you are frustrated about YouTube issues, but get disappointed that nothing is done. But these tools are already there and made by hackers.

Rek2
***2600* Madrid**

It's great to hear of these developments. We want to see all of the new options test driven by the community to see what works and what's sustainable. We support having our videos pop up on all of them, but we can't commit all the extra time required as we're super busy just creating content in the first place. We suggest people check these out and let's see what develops. We're not sure you're aware that Odysee was acquired by Google, but their site is odysee.com while PeerTube (still independent) can be reached at joinpeertube.org.

Dear *2600*:

There is an app called Instacode that tells you the combination or key code for padlocks. It costs $10 a month. Wouldn't this be a very finite amount of information that could be looked up and kept in a text file?

Peter

It would be a pretty big file and it would have to be updated almost constantly. People who have reason to be doing this sort of thing would likely find the app more convenient.

Dear *2600*:

This transaction is secret to protect my job. I contacted you for a reason, I am a bank manager here in Cambodia and one of my late customers who has the same name as yours. He died ten years ago and left a huge amount of money in his account. Since then no relatives have come to claim his money.... I think we can work this out together for mutual benefit. I will give you more details on hearing from you soon.

smey

This actually came in to our articles email address. Imagine their surprise upon hearing there was someone else out in the world named 2600 Article Submissions. And that this coincidence was enough for them to be able to get that person's fortune.

Dear *2600*:

With all the fuckery going on at Twitter, how likely (or possible) is it that they get completely pwned? Lose control of the site completely? I don't mean it breaking, I mean something like North Korea taking it over.

PXD

Doesn't North Korea have enough problems? And we're not sure how it would be any more managerially unhinged in that scenario than it is already.

Conclusions

Dear *2600*:

Snowden granted Russian citizenship? Sounds good to me. Now that he is Russian, he can be conscripted and sent to Ukraine to become sunflower fertilizer. It'll be the most useful thing he's ever done.

AM

We hope you at least understand that Snowden did not choose to be in Russia. He was stranded there when the United States canceled his passport back in 2013. So if the implication here is that he fled to Russia, it needs to be corrected. Snowden has often said he would willingly face trial in the United States if he could be assured of a fair one. People who want him imprisoned tend to be the only ones who claim to believe this is possible.

Dear *2600*:

Wow. The fact you support Ukraine speaks. Volumes. You're def not you were 20 years ago. Sorry that you aren't.

NB

Please enlighten us as to who we were. Because if we weren't the type of people who stood up for the underdog and fought back against bullies and oppressors, then we probably wouldn't like ourselves very much.

Dear *2600*:

Hacking, to me, has always been about finding a way to get things done. Whether that be thinking outside of the box, pushing items to their physical or virtual limits, or probing and testing to see where weaknesses are... the end goal being "to do what I need it to do, even if it wasn't intended to do that..." and it's not just "things" either. I grow with each experiment/experience. Each failure is just as important as each success. I've seen some pretty hot topics recently that turned into political fights. I just wanna remind everyone that while we don't all agree on everything, we should all strive to see what makes us the same, instead of the differences that drive us apart.

Using myself as an example, if I told you I loved solar power for the freedom it offers, some would paint me as some hippy liberal bent on destroying

fossil fuels. If I told you I owned military vehicles that will happily burn virtually any combustible liquid (gasoline, kerosene, diesel, waste motor oil, etc.), you'd call me some right wing doomsday nutjob hell bent on destroying the environment. Surprise! It's possible to believe in both things.

Point being, we don't have to label everything. It all doesn't have to be a fight. Not everything has to fit into nice little corners with labels and all that. If you really wanna learn about things, ask questions. That's why I'm a huge fan of the Socratic method. Always strive for the truth, and make sure you have citations to back up your data. If you have an opinion not backed up by data, that's fine too, but realize it's just an opinion, and not factually based, and should not be asserted as fact. Just my 3.7 pennies (adjusted for inflation).

Robert T.

Typical logical letter writer, if we're going to assign a label here.

Dear *2600*:

I've been questioned about why I don't use a password manager, pressured to use one, and, heck, even made fun of because I don't use one. I do not use a password manager, and the recent hack of password manager LastPass is one reason why. If you use a password manager and it gets hacked ("experiences a breach"), your account could be compromised and the hacker/s would have *all* passwords you have "linked" with that manager. How is that better/safer than not using a password manager?

Bryan

No matter how good an idea may appear, poor security will quickly negate any advantages. That's why it's always good to ask questions and never believe everything you're told. There's always something that hasn't been thought of. If you can come up with a system that works for you, then don't let anyone talk you into one that you're not comfortable with. Just remain open to new possibilities and ways of improving your security.

Inspiration

Dear *2600*:

Ten years ago I became disabled. I literally used a computer just for the web and maybe a torrent or two. No background in tech. Maybe jailbreaking iPhones or whatever. Out of boredom and the desire to tinker, I installed Gentoo Linux on an old iMac. After distro hopping for years, I settled on Arch. For seven years, I've been using my Btrfs Arch workstation with i3wm to run Debian seedboxes, play with pentesting, and run/network *lots* of containers and VMs. Anyway, last month I put together a resume, just to see what happened. Being a writer, the only credentials I had to list were my handful of published open source and cyber security articles and a strong hacker ethic. Today, I was offered a job as a Linux support engineer with a web hosting company. No degree. No fancy certs. Just a passion for hacking and a near neurodivergent commitment to open source. Job is 100 percent remote and more salary than I've ever reasonably believed I'd be getting. Goodbye Social Security. Hello world.

Joseph

This is a great story of triumph in the face of adversity. We hope it inspires many more.

Meetings Around the World

Dear *2600*:

Hello, I am currently living in Santa Fe, Argentina, CP 3000 and I would like to know if there is a *2600* meeting in my city. Also, I travel frequently to Buenos Aires, so if there is a meeting there, I would like to know where it takes place. Thank you in advance and have a nice day.

P.S. I subscribed to your magazine for the first time last month and I'm delighted with the quality of your job!

Nicolas

Welcome aboard. We've recently added meetings in two districts of Buenos Aires. We don't have any in the Santa Fe area, but you can try and start one by following the guidelines on our meetings page (www.2600.com/meetings) and letting us know. That's how meetings all over the world get started.

Dear *2600*:

I would like to know what days you do your meetings. I live in New York City and I see you have a meeting in the city but I see no time or days.

GM

As stated on our web page, "All meetings occur on the first Friday of each month, starting at 5 pm unless otherwise noted." If there's another place you're seeing a listing without this info, please let us know where that is. We hope you enjoy the meeting!

Dear *2600*:

I showed up for the Seattle meeting at Cafe Allegro this evening, and asked the staff about the meeting. They indicated that the cafe has been closing before 6 for the last couple of years, and there haven't been any meetings at that time at least for the last few months. I don't see a way to contact anyone in the community around here yet. Would you mind checking in with any of the Seattle folks to see if a meeting is happening anywhere else?

cathos

You're not the only one who's pointed this out. The meetings now have a new location.

Dear *2600*:

I was seeking a *2600* meeting near me and found one in my state a bit of a ways away. I was just wondering if you had any points of contact that I could reach out to in order to get more information regarding the meeting. Thank you for your time!

Christopher

We don't give out any personal contact info. But if you go to our meeting list at our website (or look in the back of each issue), you'll see links to Twitter accounts for those meetings that use that service. (We hope to see enough meetings put up their own websites that we can also link to.) That should enable you to reach out to people who know more specifics.

Dear *2600*:

So today was fun.

The past two times here in Stockholm, it's only been me and a friend from work: an infosec expert who's been learning Linux. Our deal was that if no one else came, he could ask me Linux questions.

But today was different.

My regular work friend joined and I managed to bring an old crypto architect from work who said "Oh that old mag, I used to read it back in the day." And another guy who we met at SEC-T also joined. We talked tech and we talked about finding a better meeting place. Then, an hour and a half in, something really unexpected happened: a woman came by who was originally from the New York City *2600* meeting and who has been to meetings in different cities. This was our very first encounter with *2600* visitors from other cities. She gave us a lot of good info on how to find a better meeting spot.

And then, completely by happenstance, the group decided we should form a Signal group chat. This thing is starting to move on its own.

/Psychad

That is truly the magic that can come from the meetings. If you stick with them, inevitably new people will show up and oftentimes travelers who happen to be in town that day. The connections that are made can be priceless and long lasting.

Sheer Stupidity

Dear *2600*:

Gotta love Coinbase, lost access to my old phone number, went to change it. Guess what they do. Automatically text the old number a login code. Went through all of the ID verification and, yup, the account is cleaned out and still tied to the old phone number. Forced two-factor authentication is absolute trash; can we stop doing that?

Taylor

No matter how good a security concept is, it can easily be unraveled by bad policy. This is another shining example.

Dear *2600*:

How to kill a Fortune 500 company's stock in five minutes: Open a verified Twitter account for $8, pretend to be that company, and then tweet something ridiculous.

MP

We think everyone in the world knew that already. Except maybe one person.

Dear *2600*:

Just got a new vacuum at work and found out that management is making us download an app in order to use it because the vacuum does not come with the ability to control itself. I feel as though this crosses a line. I'm just not sure where that line is.

Pjotr

It most definitely crossed the line into absurdity. Why on earth would you need an app to control a vacuum cleaner? It sounds like a fun thing to experiment with, but then someone went and took it way too seriously, making it into the normal method of operating such a device. Of course, you didn't tell us anything about this vacuum, so if it's some kind of robotic device that humans don't actually operate, an app might make a little more sense. But if multiple people have access at the same time, it could quickly devolve into pandemonium. Now that we've thought about it, we think this might be really fun to play with.

Injustice

Dear *2600*:

Hello! My name is Tamara and I'm from Serbia. On Friday, a big Internet scam happened and I, like many others, lost money. We desperately need help. I don't know if this is a stupid thing to try and if I'm even turning to the right address, but hope dies last.

Tamara

It's unlikely that we - or anyone - can do something that helps with the immediate situation. But what we can do is help spread awareness and keep others from being victimized. For that, we need actual details. If knowing those details would have protected you from being scammed, then it's a certainty that sharing them will save others. And we're sure that karma will come back to visit you at some point.

Phone Phun

Dear *2600*:

I admit that I am old school and haven't done much in the way of messing with phones since the days of POTS, payphones being common, and various "colors" of boxes, and I haven't been keeping up with telecom technology and techniques for messing around in the VoIP world. That being said, I have an interest in accurately tracing phone numbers. What's the best way to accurately (if possible) trace phone numbers of scammers, spammers, and just people pulling pranks these days?

Jason

There are as many tricks in getting someone to reveal their true number as there are tricks in keeping it hidden. Caller ID is easily manipulated to display virtually any number the caller desires. Often that will include local numbers to make it seem as if a neighbor is calling. More sophisticated scams involve spoofing a number already known to the called party, which adds a level of believability to the call. In other words, you should never take as gospel anything you see show up on a Caller ID display, landline or cell phone. That said, there are methods of getting true numbers to show up, most of which are because of technical flaws that haven't been discovered. For instance, sometimes a spoofed Caller ID will reveal the actual number when the caller leaves a voicemail message. This also can happen on various follow-me services where a call first goes to one line, then another in an attempt to find the called party. We've seen the spoofed number show up at the first location but the unspoofed one show up at the second. This is likely due to Automatic Number Identification (ANI) being passed along at the point of transfer instead of the Caller ID data. ANI is harder to spoof and tends to be used when calling toll-free numbers of anything where the billing number needs to be known. Caller ID, on the other hand, is only used to identify a number to a subscriber.

Dear *2600*:

In the 1990s, I programmed a game on very expensive (at the time) answering machine equipment that was used for telemarketing. It's an audio adventure where you just point the direction you want to go and hit the * (asterisk) button to do anything in any of the rooms. The objective is laid out when you first log in (call it). Only one person can call it at a time. So, call back later if you do not hear "Welcome to my answering machine." If you get killed in the game, it hangs up on you. The system takes about 30 seconds to reset before someone can connect again. You can call it at 630-847-5241 with any touch tone phone.

Dino

Well, at last, a reason to make phone calls again. This is almost as much fun as our old voice BBS, also from the 1990s, which we have been working on archiving. There are maps available online for this audio adventure game or you can make your own.

Dear *2600*:

Does anyone remember using a safety pin stuck into the wire connecting the handset to a payphone to get a dial tone without a coin? It worked in the early 1960s on rotary phones by touching the pin to the finger stop. The cords back then were just insulated; there was no metal shielding on them.

George

This is similar to the famous WarGames *trick that's demonstrated early in the film where the detached top of a soda can is used to connect the inside of the unscrewed mouthpiece to the phone's keyhole, applying ground to the ring wire, and thereby getting a dialtone. In places where you couldn't unscrew the mouthpiece, sticking a paper clip into one of the holes and touching that to a metallic surface would also do the trick. We're told that many payphones throughout the country had holes in the mouthpiece that looked like something had been crammed into them many times, so it seems likely this remained commonplace for as long as non-dialtone-first phones existed.*

Dear *2600*:

I got a text from PayPal with a code to reset my password, so I called T-Mobile about my SIM card possibly being cloned. The first support lady tried to sell me a new SIM card and charge me an activation fee. I asked to get transferred to tech support. The tech support guy not only put an alert on my account for new IMEIs/phones, but was willing to let me turn off the phone and verify that my E911 information was correct first. I didn't have to do any social engineering or anything - this dude was just super excited to give me the physical location of a SIM card hijacker and deliver some "street justice" (his terms). It seemed like he'd been waiting his whole career for this moment. That's why having one of the most ghetto phone carriers rules.

Zach

We can't argue with that statement.

Experiments

Dear *2600*:

Just now, I made a post on Facebook and included the words Climate Change. The post had nothing to do with climate change. After hitting Post, Facebook showed a pop-up informing me that Facebook will add links to articles about climate change. After posting, another dialog pop-up told me my comments will be posted as soon as they are ready. I'm wondering if this is a new thing. Just never seen this before.

Bob

These little features are typical of social media companies trying to act socially responsible. They can be annoying and are certainly easy to mock and, as you did, falsely trigger. Of course, the real issue is the fact that not only are outright lies and harmful calls to action being posted, but that they're being spread rapidly on these networks. No matter how clumsy the companies' reactions are, the real problem is the poison and venom that's being given life in these environments. Regardless of how we feel about the reactions, let's continue trying to find an effective solution to what they're reacting to.

Oh, and climate change is real, by the way.

Suspicion

Dear *2600*:

I just had an interesting/disturbing thought. I switched Internet service from cable to AT&T fiber a few months ago. Cable throughput per speedtest.net was decent, but the new line is downright spectacular; typically 360 down/350 up and 25-35 ms ping for rated 300 meg service, any time of day or night, local network idle or with a streaming TV or two operating. Impressive, but the speed plus strange consistency got me to wondering: Could AT&T be pulling a VW and optimizing/prioritizing their network to maximize speed tester throughput? Maybe even hijacking the DNS requests and routing to an in-house lookalike server? If they are, is there any way to detect that kind of trickery? Reality check: I doubt they're actually pulling stunts like this. But if they are, and the actual non-speedtest rate is half the rated speed, how would I know?

Richard

You are right to be suspicious, but we doubt they would be able to get away with such shenanigans for long. Everyone has the ability to run different tests and share their results with everyone else. But you touch upon an interesting point regarding speed upgrades. Oftentimes, it's really hard to tell if your speed has actually improved, apart from the higher numbers on the various speed testing sites. This is because you may be running into caps imposed by sites you visit or due to wiring deficiencies in your home or office which result in a weaker signal to some areas and a slower overall speed. A connection is also only as good as the links it follows, so if there are any non-dependable hops along the way, that will adversely affect speed. Our advice is to keep on top of this so you know right away if you're not getting the results you're paying for.

Remembering

Dear *2600*:

Thinking about the old days... there was a year or two in the 90s where BBSes and the Internet

coexisted. In 1995 through 1997, the Internet wasn't yet in most homes so a good way to gain BBS clout was to download files off the Internet and upload them to BBSes. If you noted in the file description that it came from the Internet, it was just that much cooler.

Eddie

Then people began to read the actual content and suddenly BBSes didn't look so bad.

Dear *2600*:

Can anyone tell me how call tracing and *57 worked in the landline days? I remember getting harassing calls and being told they could only be traced if you dialed *57 after the fact. What did *57 do in terms of logging the call that wasn't already happening?

Adam

*This was basically a scam perpetrated by the phone companies. By dialing *57, you would get to pay them $1.50 or so for them to tell you that they had traced the call. You would then have to follow up by filing a police report. You would never find out the number, but they would supposedly contact the calling party to tell them to stop calling you. (It's unclear whether they would be given the number of the person complaining, which would make this doubly insulting.)*

*The phone companies were already making money by selling Caller ID, which allowed numbers to be sent in the first place, and *69, which allowed people to call back unblocked numbers that had called them (for another fee, of course). *57 was designed for those numbers that were blocked, using either all-call blocking or *67 before dialing. Intense lobbying from consumer rights groups kept the phone companies from charging yet another fee to keep your number private.*

What phone companies didn't readily tell consumers was that annoyance call bureaus existed for the sole purpose of tracking down malicious callers effectively and with no charge to the complaining party.

Dear *2600*:

I can still remember file names and complete web addresses from 20 plus years ago and can't remember why I walked into the kitchen....

Paul

In the end, which of those is actually more important?

Privacy Intrusions

Dear *2600*:

Is there any way to protect one's address and privacy from voter registration databases? I am generally good with avoiding junk mail. In fact, I've removed myself from the DMA and other databases and am usually prudent about whom I give my address to. But one loophole I've been unable to plug is the voter registration database - specifically in California. I recently got a handwritten letter begging for my vote from some politician who scraped my address from a database. Then I sent an angry email expressing my annoyance and frustration to said politician and how her intrusive letter actually guaranteed that I'll never vote for her... along with a request to stop doing it. Her solution was for me to stop voting altogether so that my address isn't scraped for marketing purposes. Some questions for ya'll: 1. Excluding a P.O. box, is there anything one can do to prevent this? 2. Where is this open database of voter records located and how does one access it? Is there a link? Thanks.

DM

The rules are different for every state. Some actually allow anyone to download the database free of charge. Others restrict it to state residents. And there are a few that charge exorbitant prices. (For some reason, Alabama charges $37,000 while Florida doesn't charge anything.) Each database is also structured differently, with some including phone numbers and/or email addresses. But it's very hard to avoid having your street address appear to anyone looking through it. Some states restrict the sharing of information of individuals in certain professions, such as police, judges, and people who work for reproductive justice, so it's certainly possible to not have that info be displayed to everyone. But then there are also "enhanced voter records," which are marketed to political campaigns and can include even more personal info, such as religious affiliation and social media profile details.

You are right to be concerned about this. We believe this will become an even bigger issue in the years ahead.

More Feedback From A New HOPE

(Note: Here are a few more letters that contained feedback for A New HOPE and, as per tradition, we thought they might be of interest to readers. Names have been omitted since we didn't explicitly tell writers that their comments might be printed.)

Dear *2600*:

I would like to provide the following feedback for A New HOPE.

Please stop using Zoom. Zoom was also used for HOPE 2020. We are hackers and need to set a good example for everyone in the world and using Zoom does the opposite of that.

Please stop using YouTube. I'm sure everyone on your end is aware that big ol' g00g shut shit down on their end.

Please have a Matrix chat room to engage those in-person, those remotely attending, as well as the others who are financially struggling and could not afford a ticket this year (but have supported *2600* and HOPE financially in the past). It would benefit all of us to help build our community both before and after each HOPE. This is important with everything going on around us today.

A New HOPE Attendee #13

All good suggestions, but all unfortunately are affected by reality. We spent a considerable amount of time working with numerous different programs, apps, and services with the exact goals that you outline. In the end, though, we have no choice but to go with what is most accessible and easiest to use for our attendees. And often, this is not the same as what we would ideally like to use in order to make a statement.

We've been down this road many times. Do we stop using Amazon and not put out a Kindle edition? Do we make a statement against independent bookstores being forced out of business by not supplying Barnes and Noble? Had we taken those higher roads years ago, we indeed would have made a statement, but we wouldn't have survived in order to make any more. And we would find ourselves in a similar place of high virtue but low audience if we stopped using those outlets that everyone else uses. We're not thrilled about it, but it's reality.

But instead of bemoaning this state of affairs, we have the opportunity to reach more people and help inspire them to create tools that can do a better job. While you may believe that those tools already exist, what we found was that they just weren't as easy and intuitive to use for those who aren't really good at this sort of thing. And if we ignore those people, we believe it's a bigger disservice than choosing software that doesn't check all our boxes.

We notice you didn't criticize Matrix which we assume means you approve of it. We have received a lot of positive feedback on that front and believe they are a better fit than something like Discord. We'd love to be able to give out free access to that part of the conference, but we have way too many expenses to make that feasible. We already publish all talks for free online, which is more than what most other conferences do, and much more than what we were able to do in the past.

Dear *2600*:

I stayed on the St. John's campus in a townhouse, and found it perfectly fine for the price and ease and location on campus. The talks were fine, and a few were absolutely outstanding. There were talk overlaps as always, and I await the recorded sessions. Which, after everyone recovers or comes back from a well deserved vacation, will be up for sale or on a thumb drive, if not on the *2600* site or YouTube channel.

Even the hot weather was mitigated by the campus mighty air conditioning units. The onsite Starbucks was fantastic, and the expertise behind the conference to make it run was top notch.

Well done, all!

Maybe next con we could rent electric scooters?

A New HOPE Attendee #14

Thanks for the comments. As we used a couple of different buildings with potential to use even more in the future, the idea of scooters or possibly golf carts to ferry people around has come up.

As mentioned, we were hit by a severe heat wave that weekend, but the university did a great job keeping the insides cool, far better than Hotel Penn ever did. In fact, some people asked us to turn the temperature up a bit!

We had everything up online within a couple of weeks after the conference and better quality non-DRM versions remain available on thumb drives as well.

Dear *2600*:

Thanks for A New Hope! Wanted to say it was great to be back at the con!

A few pieces of feedback:

Track Four was pretty great and I appreciated the announcement post with the calendar over the constant checking of that room in the corner of past cons. Would be great if we could get these into the schedule app so we can get full schedules and notifications like everything else.

I noticed that remote talks were called out well on the paper and app schedules, but *not* on the website which I used when initially planning my time.

There was some great RF content, but did not notice any representation from local clubs. Wondering if anyone does outreach to them as part of the con.

Overall, great con and looking forward to 2024.

A New HOPE Attendee #15

Outreach is always where we fall short. So many people and groups have contacted us after the conference, frustrated that they missed out. We do our very best to get the word out, but the social media giants make it very difficult to go viral.

Remote talks should have been indicated on the website, especially if they were in the printed program. That may have been a software issue which we'll look into.

Dear *2600*:

First, thank you for the awesome conference!

I think next time it would help if we can get a bunch of food trucks somewhere on the campus close to the talk venues. When it was at Hotel Penn, it was very easy to go get a bite and come right back. Here at St. John's, it was quite a walk.

I think food vendors would also make some really good money, so it is a win-win for everyone.

A New HOPE Attendee #16

We agree 100 percent and that's one of the things we'll really push for next time. While there were a lot of really good places a block away, we know that in the middle of a conference, even that can be too far. Now that we've done this once, it's a lot easier to make these suggestions to the university and make the whole event that much more pleasant.

Dear *2600*:

Thank you! Genuinely. Over and over and over. *And,* again, particularly for live streaming and having the Matrix up and running for all of us unable to attend in person.

My first HOPE was The Last HOPE in 2008. My husband (who lives in Canada) and I met at HOPE X, and we've attended in person and virtually since.

We were incredibly looking forward to this year in person, but I got hit with the virus a week prior. My husband decided to stay up north, and even as I tested negative, I chose to play it safe and fully recuperate. It wasn't fun, laying low whilst only a bikeable distance from all the action at St. John's, but walking around the 3D virtual hub, watching and even just listening to fascinating, useful, and entertaining sessions was a boon for my mind and for my recovery (I'm convinced).

Mad respect and appreciation to you all; every volunteer; and the incredible, greater hacker community.

A New HOPE Attendee #17

It means so much to us, as well as everyone who helped make this event happen, to hear stories like this one. If there's anything positive that came out of the past few years, it's the realization that the HOPE crowd is no longer limited to just those who can attend in person. Through Matrix, people are able to attend in a different way and experience much of the same enthusiasm and inspiration that in-person attendees have been doing for decades. And paid virtual attendees have become crucial in keeping the conference and the magazine going. We hope you're able to attend our next event in person, but it's great to know that online attendees are also getting so much out of HOPE.

Dear *2600*:

I had a great time at HOPE and met a bunch of awesome people! Can't wait to see you all again! Hack the planet!!

A New HOPE Attendee #18

We received variations of this sentiment more times than we can print. We couldn't ask for anything more.

Dear *2600*:

Thank you for all the work everyone put into this conference. HOPE has long been my favorite conference, as the people are always friendly and I do not see that cliquey behavior so common at other conferences.

The feedback I have is: I understand venues are challenging and while the campus was lovely, honestly it was the middle of nowhere with limited things to do. Over an hour by public transportation to get to Manhattan for a show was unfortunate and getting to or from a place now had to be a big consideration for planning.

In the July heat, the con at a hotel where you do not need to go outside unless you really want to is a major plus. The weather was horrible.

Again, thank you for the wonderful conference and for everyone's time and efforts!

A New HOPE Attendee #19

We understand the challenges and it sounds like a mixed bag of good and bad for you. We have a few suggestions that might help.

Assuming you're from out of town, we don't suggest trying to pack in too many activities during a HOPE weekend. Going to a show in Manhattan is certainly going to take away from the fun you have at the conference. We had activities going around the clock and there were certainly all kinds of places to go to in the surrounding neighborhoods. We need to do a better job directing people to those places, which is one of our main goals for next time. The venue is most certainly not in "the middle of nowhere" and is considerably livelier than the main parts of other major cities. But at the same time, the campus provides a nice level of insulation for those who just want to focus on the conference.

Obviously, we can't control the weather. But having an entire multilevel building to hold the conference in meant many of us never had to venture outside. But we are looking into ways to make it even easier for those who choose to wander around the campus and surrounding neighborhoods.

Dear *2600*:

Thanks to all - your team, the speakers, the volunteers, the venue, the sponsors, etc. - for a wonderful celebration of all facets of hacker knowledge, culture, and fellowship.

I wish I could have attended in person, but the live streams were an excellent gift to the larger community that could not be present. I really appreciated it and camped out all weekend at my terminal with HOPE in one monitor and work in the other.

So many great topics with variety of content, skill levels, and personalities.

I'm hoping the talks will be posted on the YouTube channel so I can recommend some to peers, others to friends, and rewatch my favorites. Will that be the case?

The only sad part of my feedback is that the YouTube copyright system ruined the hacker movie panel since it kept flagging (then banned) the channel right as we arrived in the early 90s. Wish I could have seen that presentation in its entirety - so much fun, nostalgia, and laughs.

The new venue seemed great and the concluding ceremony was also very fun/interesting.

A New HOPE Attendee #20

As you probably know by now, everything has been posted and we won our appeals to Google. Their paranoia ruined the ability of attendees to go back and view previous talks on that stream during the conference. But it was our fault for allowing them to become the main stream for the conference, a mistake we will not make again. We also used the opportunity to educate many others on these issues and we dare say it made a difference with a bunch of other events. We're glad this hiccup didn't detract from your enjoyment of the event. In the end, they tend to be learning experiences which make us all better informed.

Dear *2600*:

Thanks for a really great event! I'm interested in volunteering next time.

A New HOPE Attendee #21

We've received many similar inquiries and this is really key in keeping the conference successful and growing. It's simply not possible to pull this off without the efforts of our many volunteers. And what's really cool is the fun people have while volunteering and helping to make the conference even better. We look forward to working with you the next time around.

Dear *2600*:

Just wanted to say thank you so much for a great conference. The location was top notch, the team were amazing helping me get set up for my talk, the location for my workshop was perfect - and that's before getting into the rest of it.

Great range of really interesting talks and workshops, everyone was amazing. The whole conference was fantastic.

Was a privilege to be invited to talk and run a workshop and be part of it.

Thank you all so much.

A New HOPE Attendee #22

We really did have such a terrific lineup of speakers and workshop presenters. For the first time, we actually had enough space to accommodate them! And it's great to have access to working resources, everything from audio/visual to network tools. So a big thank you to everyone who played a part in the presentations.

Dear *2600*:

I've been hearing and reading about HOPE since The Last Hope in 2008 and have been wanting to go since then; due to various reasons this was the first time I was able to attend. Being my first time, I feel I should share my opinions on how I felt it went. I know you all probably have a ton of these to read through, so I'll try to keep this down to a simple pros and cons list to keep this short and to the point.

Pros:

- Many good talks, many good speakers, I learned a number of new things.
- COVID protections seemed very well implemented.
- The combination of vax check and masks definitely made HOPE feel a lot safer than other cons I've been to.
- It was great to catch up with old friends and meet new ones.

Cons:

- The hotels chosen were very far from the con.
- I have foot pain issues so this was especially bad for me personally.
- I felt uneasy walking alone in an area of New York City that I didn't know. I have to assume this feeling was amplified for women who also didn't know the area well.
- The venue for the con did not seem like a good fit for our crowd.
- The Christian school and banning of alcohol definitely set a specific tone, and it was not one that I or anyone I spoke with seemed thrilled about.
- There didn't seem to be any good dedicated "hang out" areas to set up laptops and do some impromptu hacking/learning/teaching/experimenting.
- Being central on the campus meant the nearest restaurants were quite a walk to get to.

All in all, I had a great time and learned some new things, but if the next HOPE is scheduled to be at St. Johns, I likely would not come back. I would much rather see the ticket price increase and do a location where everything was close by, we could be ourselves, and we could all enjoy drinks together if we wanted. I understand that more expensive tickets could make the conference inaccessible to some, however things like student discounts could help to resolve these issues.

A New HOPE Attendee #23

We're glad you appreciated the COVID restrictions and we're thrilled that everyone respected them and still managed to have a great time. Unlike many other gatherings at the time, there were no reports of infections related to HOPE. That really was our biggest worry and it was why we put a cap on attendance, even though we really needed a bigger turnout to make the whole thing viable. Being responsible was far more important.

The issues you raise are well worth addressing. The main hotels that were affiliated with HOPE were the closest ones to the venue. But if you stayed on campus, you really couldn't get any closer. We know that not everyone wanted to follow the no alcohol, same sex dorm policy on campus, but that was the tradeoff for staying onsite. If you stayed at the hotels, there were no such restrictions. (Many of our attendees were happy not to have alcohol at the event as it's always caused problems in the past.)

Concerning spaces to hang out, we had more of those this year than ever before. Whether it was at the coffeehouse, the fireside lounge, the place with all of the desks by registration, or the numerous areas in hallways and gathering points, this was probably our biggest gain from our previous space. In fact, there were many outdoor locations with chairs and tables where people had impromptu gatherings after midnight! Space is a wonderful thing to have.

The religious background of the school had no bearing on HOPE whatsoever and we found the staff to be far more open and accommodating to us than Hotel Pennsylvania had ever been. (It was also nice to not be paying Vornado as they helped destroy that part of the city.) Hackers have held conferences at military sites, Communist Party headquarters, and casinos. We can handle an occasional church bell.

The possibility of having a conference at a venue in midtown Manhattan or equivalent is one we explored tirelessly for years after it became clear that Hotel Pennsylvania was no longer an option. For that to work in the few places that have adequate conference space, ticket prices would have to double or triple, assuming we could even get the same number of people to attend. And offering student discounts wouldn't help the situation if they weren't funded somehow. The cost of taking or sharing a brief cab or Uber ride from the hotels near St. John's to the conference would be negligible compared to such a huge price increase.

We miss Manhattan too. But the hacker community is nothing if not flexible and adaptable to change. We managed to create something entirely different when we couldn't meet in person at all in 2020. And we believe this new location for 2022 and beyond has opened a completely unprecedented and unique chapter for all of us. The overall reaction was far more positive than we had hoped for, so we're eager to start working on ways to make this event even better.

Dear *2600*:

To make more money on t-shirts, sell us the brightly colored ones like the volunteers got (bright

blue, purple green) after the conference. There is more to life than black t-shirts.

The workshops and the hacking room were awesome for keeping 17-year-olds entertained and educated. Hurray for lockpicking, soldering, and Arduinos!

Maybe we just missed it: Shout "Enter by Gate 6!!!" in a prep email soon before the conference and put a "Go To Gate 6!!" sign at Gate 1.

In that same prep email, a note that you can park first, and *then* come get the permission yellow form. We were very nervous parking, and wasted time driving around.

There must be some way to get all those musicians onto the stage for the talent show - someone local brings a keyboard and some guitars? The place was literally dripping with musicians....

There must be some solution to "we can't read the slides because you made them tiny to also show the speaker's face on the stream." (Tell everyone to log into talk on computer and zoom in. That's what we finally did. Maybe should have been obvious.)

A New HOPE Attendee #24

All good suggestions. Much of these little frustrations came about because all of this was a first for us as well. We pride ourselves in never making the same mistakes twice. What we need to work on is not making too many new ones.

The way talks were presented on streams was a choice. We don't have to do it that way in the future if another method is preferable.

Dear *2600*:

Thanks for yet another great HOPE! I'm glad HOPE survived the pandemic and the loss of the old Hotel Pennsylvania. It must have required a mammoth effort from the HOPE team. Here's some feedback on A New HOPE:

I liked the St. John's venue! Since the HOPE staff was so conscientious about keeping the talks and Q&A to 50 minutes, there was always plenty of time to walk between buildings and get some sun. I stayed at the Sheraton LaGuardia in Flushing Chinatown, left my car in their reasonably priced garage, and took the bus to/from St. John's most days - two nice walks to bookend the days and a bus tour of everyday life in Queens. This location might be a bit far to make your list of hotel options, but it worked for me. Not every city has a system where busses run reliably every ten minutes; people unfamiliar with New York may be surprised to learn that this is a convenient option.

I became a fan of the "Sup" Thai place on Union Turnpike. At one point in mid-afternoon, I was the first of a series of at least three HOPE attendees to arrive at Sup. We arrived at ten minute intervals and each took up a table. If I had thought of it ahead of time, I would have looked for or started an effort to organize a table-sized group on the conference chat to avoid DOS-ing the restaurant's limited space. This might be something to suggest at the next opening ceremony.

My favorite talks are the ones where the speaker is obviously grateful to have finally found an audience that appreciates whatever peculiar thing it is they like to hack, and they go on to explain some interesting exploration or problem-solving. Sometimes these talks are a useful alert that the cost of the tools needed to play has shrunk to the point where I might consider jumping in. Other times they're simply an opportunity to vicariously enjoy something I'd otherwise never have heard of.

John and Laura Leita's talks on urban exploration at The Fifth HOPE and HOPE Number Six are my go-to examples of this kind of talk. There's no way I'm going to explore an abandoned New York State mental hospital, but they had fun doing it, they were obviously having fun sharing their experience, I had fun listening to them, and everybody at HOPE had fun. I thought many of this year's talks were fun in the same way: Davide Semenzin's talk on book scanning, Joshua Fried's talk on his music-making, Steve Bossert and Joe Cupano's talk on radio experimentation, the Dunin-Jacobs-Schmeh talk on cracking 19th century encrypted ads, and the Peon/Clamp talk on filling in the blanks were some good examples.

I also enjoyed Vlado Vince's talk on Yugoslavian retro-computing; HOPE does good work in keeping the hacker community in touch with its roots. Brandon Roberts' "Hackers Can Help" talk deserves special mention for identifying interesting challenge problems towards which people looking for a project might direct their efforts, work hard, gain some expertise, and ultimately come to a future HOPE and share with everyone.

The hope.net schedule table was excellent; I used it to choose talks on my phone through all three days.

Many thanks, and see you next time!

A New HOPE Attendee #25

Thank you for all of that acknowledgment, particularly for the speakers who really brought so many interesting and unique topics to the audience, not to mention the world through the HOPE archives. (All talks for all HOPEs can be found at youtube.com/channel2600.)

We're glad to hear of another solution for places to stay. This is how others can be guided in the future. As hackers, we sometimes have to think creatively to make something work well and it seems like you did just that.

We hope to do a much better job in the future of guiding people to food places, as this location is right smack in the middle of one of the most ethnically diverse urban areas in the world. We found there to be many great food options on Union Turnpike alone (one block away from the campus) and all of the marvels and late night activities of what many call the biggest Chinatown in the world are only ten minutes away.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind. As you can see, we're open to a wide amount of opinions.

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

EFFecting Digital Freedom

by Jason Kelley

Killer Robots Are Coming, But We Can Stop Them

San Francisco is known worldwide as a progressive city, but those values were put to the test recently when the San Francisco Police Department tried to pass a new policy that would give them permission to use manually-controlled robots equipped with explosives. By the time most of the city heard about this, it seemed almost too late: the city's supervisors voted 8-3 to allow the policy on its first reading.

We scrambled into action, because the policy needed to pass its second reading as well. The "killer robots" were covered by news outlets around the globe, for good reason: militarization of police has been a longstanding problem, but something about attaching weapons to robots that were originally created for disarming bombs and sending them into a California city of 800,000 didn't sit right with most people who heard about it. The world was watching to see if a diverse and politically lively city would allow its police to kill with robots.

In just a week, activists and residents across the Bay Area worked together, made their voices heard, and even staged a rally early on a Monday morning. Thanks to their hard work, and the hard work of city leaders who never backed down on this issue (Supervisors Preston, Rosen, and Board President Walton), there was a stunning reversal on the policy's second reading: the San Francisco Board of Supervisors banned the SFPD from using deadly force with remote-controlled robots, by the same 8-3 vote that initially passed the policy.

The fight isn't over in San Francisco. The board sent the killer robot policy back to its Rules Committee for revisions and more public comment, and it could be taken up again in the future. But in one week, San Francisco and the greater Bay Area rallied, and that rallying cry was so loud and undeniable that it was impossible for the board, and the world, to ignore.

This battle is part of a history of militarization of law enforcement, and a sign of things to come. The weapons of the United States military - drones, mobile command centers, sound cannons, and more - have already been handed off to local law enforcement for years. The transfers have equipped police departments with the ability to redirect surveillance tools and the weapons of war designed for foreign adversaries toward often-faultless targets in U.S. cities.

More and more dangerous surveillance technology and military-style equipment is coming down the line - whether it's robots and drones manually controlled by law enforcement operators, or automated robots like the Knightscope variety of autonomous rolling machines. The slope is slippery, and we've been sliding down it for a long time. Knightscope robots are already patrolling our streets, parks, malls, and grocery stores. ShotSpotter's high-powered microphones that purport to detect and triangulate gunshots in order to alert police have been in use for years, despite their inaccuracy. Now, the company has said they are teaming up with a drone company to dispatch autonomous drones to fly automatically to the presumed site of gunfire.

But with the battle over killer robots, we have seen that there is a line that people do not want police to cross. Law enforcement agencies will want to cross that line, as they did in San Francisco, and we can stop them and, with work, even roll back some of the dangerous, ineffective, and overused surveillance technology and military weaponry that have been in place for years now. If you consider yourself part of the fight for digital rights, this is one of the next frontiers.

What can you do to help? For starters, push for transparency laws around police use of technology, and processes for community input and control. California is unique in having recently passed a law, A.B. 481, that requires democratic control of whether California state or local law enforcement agencies can obtain or use military-grade tools, whether they are received from the federal government, purchased, or utilized via some other channel. Through their elected officials, the public can say "no" to military surveillance and other technology, and it won't be allowed to come to town.

This is the sort of law that just makes sense - it's important for there to be more transparency into law enforcement practices, and for communities to have democratic control of surplus military transfers, particularly for high-tech surveillance equipment. The law was modeled on Community Control of Police Surveillance (CCOPS) laws adopted in over a dozen communities across the country. Most law enforcement agencies around the country don't have to go through a policy proposal process to obtain permission to use killer robots, but those laws can be implemented in any city around the country. And if you're in California, you have at least two agencies currently going through an A.B. 481 process - your local police and sheriff - that you can follow.

Second, continue to push back against surveillance tech in the hands of police by educating yourself and others about it. Our street-level surveillance website shines a light on the advanced surveillance technologies that law enforcement agencies routinely deploy in our communities. These resources are designed for members of the public, advocacy organizations, journalists, defense attorneys, and policymakers who often are not getting the straight story from police representatives or the vendors marketing this equipment.

Third - and this may be the easiest way to help - make sure you understand what's happening in your community. Usually, records are out there in the form of news stories, social media posts, press releases, or documents buried in government websites, about what equipment law enforcement and city officials are using in your area. Our atlas of surveillance project collects much of this information, but it's a big task and represents only what our team documented after a year and a half of research. You can always volunteer to help by sending a message to `info@eff.org`.

This moment is a turning point for pushing back on the use of dangerous technology by police. We hope you'll join us in making sure that killer robots never come to the town where you live - or anywhere.

Cyber Security Frameworks

by fsu_tkd90 AKA Bill

The last article I submitted to *2600* was printed in 27:3 (Autumn 2010). Back then I wrote about my biggest problem at work: spam. Now I am writing about a dizzying problem for all corporations: all of the cyber security frameworks a company could be subject to.

Let's start by defining what cyber security is. Cyber security is not to be confused with information security. Information security is intended to protect data from any form of threat regardless of being analog or digital. Cyber security is meant to protect attacks in cyberspace such as data, storage sources, or devices. Cyber security usually deals with cyber crimes, cyber frauds, and law enforcement. A cyber security framework is, essentially, a system of standards, guidelines, and best practices to manage risks that arise in the digital world. They typically match security objectives of corporations.

It's important to understand why the cyber security frameworks are so important. Cyber attacks are now coming from nation-states as a part of war. Iran nation-state attackers typically use remote exploitation, password spray, and phishing man-in-the-middle attacks. Russian state-sponsored advanced persistent threat (APT) actors have used tactics including spear-phishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security. Chinese state hackers are using open-source information and common exploits.

Some of the largest attacks in the USA were the Colonial Pipeline, Brenntag (a chemical distribution company), Acer, JBS Foods, Quanta (Apple's business partner), and the National Basketball Association (NBA). The two new top trends malicious actors employ are automating ransomware with a human on keyboard, and "ransomware as a service." Ransomware as a service is inexpensive and readily accessible. "Cyber crime as a service" companies now have human resource departments and operate from countries with limited extradition laws. An example of this is the ransomware gang Conti, which operates no differently than a legitimate corporate business. They maintain salaried employees who are provided bonuses, performance reviews, employee referral incentives, and the coveted spot of "Employee of the Month." The employee of the month receives a bonus equal to half their salary.

Any of the cyber security frameworks takes years to implement and this article is not meant to explain each in detail. Rather, it is meant to make you aware that they exist and to give you a basic understanding. The cybersecurity frameworks all promote good basic cyber hygiene. Some of the frameworks are listed below.

ISO 27001 is composed of 18 sections with 114 total controls. ISO 27001 is a framework that helps organizations "establish, implement, operate, monitor, review, maintain, and continually improve an Information Security Management System (ISMS)". It is a joint operation between the I.T. department and the human resources parts of the business. ISO 27001 certification demonstrates that organizations have invested in the people, processes, and technology (e.g. tools and systems) to protect an organization's data and provides an independent, expert assessment of whether your data is sufficiently protected. Reports and policies must be proven to be effective to the auditors.

Information Governance

HIPAA is composed of five main elements and the CFR Part 164, Parts C, D, and E. First, let's define information governance (IG). It is the process of aligning the management and the control of information with business objectives and regulatory compliance requirements. IG in healthcare sets corporate principles for addressing data-related challenges, such as ensuring the confidentiality and security of patients' data. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. HIPAA improves efficiency in the healthcare industry, improves the portability of health insurance, protects the privacy of patients and health plan members, and ensures health information is kept secure and patients are notified of breaches of their health data. HIPAA was based off of The Health and Clinical Health (HITECH) Act. It encouraged health care providers to adopt electronic records and improve privacy and security protections for all of healthcare data. HITECH was enacted under Title XII of the American Recovery Act. It has five goals: to improve quality, to improve safety, engage patients in their care, increase coordination, and improve population health status. It was enforced by the Office of the National Coordinator (ONC).

CIS Security Controls

There are 20 sections (sometimes called the SANS Top 20) with 178 sub-sections. CIS 20 is a prescriptive, prioritized, and simplified set of cybersecurity best practices.

How are CIS Controls implemented?

Step 1: Take inventory of your assets.
Step 2: Measure asset controls.
Step 3: Perimeter defenses.
Step 4: Detect and respond to incidents.
Step 5: Evaluate the most critical gaps.

Step 6: Plan and implement your controls.
Step 7: Train and monitor users.
Step 8: Test your controls.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is composed of 12 sections with 288 controls. The PCI DSS is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment. The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The major credit card schemes are: American Express, Mastercard, Discover, Visa, and JCB. The PCI standard is mandated by the card brands but administered by the Payment Card Industry Security Standards Council. The Card Holder Data Environment (CDE) is comprised of people and techniques that store, process, or transmit cardholder data or sensitive authentication data.

Federal Financial Institutions Exam Council (FFIEC)

This is a framework (cyber assessment tool) for measuring cyber security risk and preparedness in the financial industry. The FFIEC provides a cyber security assessment tool to help organizations better understand and address their cyber security risk. It is a five member agency responsible for establishing consistent guidelines and uniform practices and principles for financial institutions. FFIEC guidelines provide financial institutions with expectations for compliance.

The below is not framework but recommended models:

FedRAMP - Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a framework that saves costs, time, and staff required to conduct redundant agency security assessments. FedRAMP Ready indicates that a third party assessment organization (3PAO) attests to a CSP's readiness for the authorization process, and that a readiness assessment report (RAR) has been reviewed and approved by the FedRAMP program management office (PMO). Because FedRAMP is mandatory for all cloud services used by federal agencies, you won't be able to do business without getting your FedRAMP authorization. Your organization is potentially missing out on a lot of revenue if you choose not to pursue compliance.

The below is a not a framework but a standard:

Federal Information Processing Standards (FIPS) was developed by the National Institute of Standards and Technology (NIST) in accordance with the Federal Information Security Management Act (FISMA) and is a set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies. FIPS 140-2 has f levels of security:

- *FIPS 140-2 Level 1.* Level 1 has the simplest requirements. It requires production-grade equipment and at least one tested encryption algorithm. This must be a working encryption algorithm, not one that has not been authorized for use.
- *FIPS 140-2 Level 2*. Level 2 raises the bar slightly, requiring all of Level 1's requirements, along with role-based authentication and tamper-evident physical devices to be used. It should also be run on an operating system that has been approved by Common Criteria at EAL2.
- *FIPS 140-2 Level 3.* Level 3 is the level the majority of organizations comply with, as it is secure, but not made difficult to use because of that security. This level takes all of Level 2's requirements and adds tamper-resistant devices, a separation of the logical and physical interfaces that have "critical security parameters" enter or leave the system, and identity-based authentication. Private keys leaving or entering the system must also be encrypted before they can be moved to or from the system.
- *FIPS 140-2 Level 4*. The most secure level of FIPS 140-2 uses the same requirements of Level 3 and desires that the compliant device be able to be tamper-active and that the contents of the device be able to be erased if certain environmental attacks are detected. Another focus of FIPS 140-2 Level 4 is that the operating systems being used by the cryptographic module must be more secure than earlier levels. If multiple users are using a system, the OS is held to an even higher standard.

In conclusion, all of these frameworks are important because criminals want cash, things that can be turned into cash, and information someone else would find valuable. In 2021, REvil's domain was hacked by another gang, Emotet returned with Cobalt Strike, and BlackMatter used tools from Darkside, Revil, and LockBit. SquirrellWaffle was observed using office documents that infected systems with Cobalt Strike. To defend against future threat actors, Microsoft purchased Section 52, which is a world class team of defenders, IoT/OT security researchers, and data scientists.

I'll end with a couple of acronyms: The CIA Triad (Confidentiality, Integrity and Availability) is a common model that forms the basis for the development of security systems; The DIE Triad (Distributed, Immutable, Ephemeral) serves as an alternative to the CIA Triad that reduces our security burden, enables us to achieve true resiliency, and move towards anti-fragility.

Music in Ones and Zeroes: A Memory of Streaming Soundscapes

by Matt Johnson
ech0plex88@protonmail.com

It was an impulsive purchase in Orlando's Virgin Megastore that opened my ears to electronic music. I was 18 years old and a high school senior in the fall of 2000. Visiting from northern Minnesota for an academic conference, the music store was a chance to discover new tunes outside my three-year addiction to Nine Inch Nails. On that day, I ended up taking home DJ Krush's *Kakusei*, Chris Fortier's *Trance America* and Aphex Twin's *Selected Ambient Works Volume II*. The first album was enjoyable for a longtime drummer, the second was like a soundtrack for science fiction, and the third was an unsettling but captivating hallucination.

Soon, I was digging through CDs at Sam Goody, where I found Ministry of Sound's *Global Underground* series. Not only was this an expansive collection of trance music from a variety of artists, but each double-CD's liner notes gave enviable details on the location, attendees, and generally euphoric atmosphere of each event. Club nights for the young, rich, and famous; a far cry from the life experiences of a Midwestern teenager. Still, I could live vicariously through the music. Trance held my interest through college, where I collected hundreds of tracks and mixes by John Digweed, Paul Oakenfold, DJ Tiesto, Ferry Corsten, BT, Amoeba Assassin, and others.

Aside from enjoyable listening, I also found the music especially helpful with writing. Creative writing was a fun hobby I'd started during an English class at age 15. At first, I listened to whatever classical pieces were playing on public radio. Generally calming, sometimes thunderous, the music helped me focus and inspired me when describing a scene's atmosphere or character emotions.

Electronic music took this beyond simple short story background tracks. I'd already been interested in extracting music files from games like *StarCraft*, *Fallout*, and *Diablo*. Later, I'd do the same thing with *American McGee's Alice* and *Return to Castle Wolfenstein*. These new albums (particularly Aphex Twin) were perfect for driving, studying, chores, and even replacing the muted music of whatever game I was playing. Sometimes hyperactive and intense, sometimes softly flowing and moody. These experiences were not soundtracks, not popular songs referencing specific life events. They were soundscapes - as much a part of my environment as wind rustling trees and tall grass, or the dripping of melting snow; in some cases, directly sampling those sounds.

Then I started college in the fall of 2001, and two innovations expanded my exposure to free music of all genres. A modern campus interconnected with T1 lines, and file sharing sites. Napster, LimeWire, Audiogalaxy, even Live365 for streaming radio. I had all the music I could ever listen to, without ever needing to buy another CD. Out of all these options, one streaming music site stood out.

Site and trademark registration for `musicforhackers.com` (MFH) appears to have occurred on Thursday, September 7, 2000. In the registration, the site is described as providing "Entertainment services, namely, providing a radio program in the field of IT Security and Electronic music via a global computer network."[1] [2] The earliest versions of the site can be found via the Internet Archive. It appears under construction in the first snapshot dated February 29, 2000.[3] This is followed by a June update referencing an IRC connected to *2600 Magazine*, and a predicted debut of April 2001.[4] Through the remainder of 2000, the site progresses through beta versions. It offers 32kbps and 56kbps streams, broadcasting 2600 Magazine's *Off The Hook* radio program.[5]

The July 21, 2001 snapshot presents MFH in the form I first used, version 1.0. A nicely rendered graphic is centered, depicting the MFH server (hosted on Live365)[6] passing data through a firewall into the 32kbps dial-up and 56kbps cable/DSL streams. Along the bottom row are links to client applications used to play the streams. As a Windows user at the time, I listened with the wonderfully customizable Winamp (it really whips the llama's ass!). Linux users could access via the X Multimedia System (XMMS) while Mac users had iTunes (not even a year old at this point). Finally, there is a link for users of BeOS, a discontinued operating system which was developed in 1990 and sold to Palm Inc. in 2001. Stacked along the left side of the site are links to `/streams` (depicted center-site), `/playlist` (current and three previous tracks), `/home` (the main site) and `/null_news`.[7] This was MFH's form as I discovered it while searching for electronic music stations in the spring of 2002, the intriguing tagline "Soundscapes for Compromising a Remote

Host" drawing me in.

The news page provided links to such gems as:

"All your base are belong to us" - *The Register*[8]

"Microsoft Obsecurity"[9]

"Britney Spears' Guide to Semiconductor Physics"[10]

"Gary Coleman Talks About Priority Queuing"[11]

"Something Awful" - *BetaNews*[12]

"Hack1ng f0r D09z"[13]

How to describe being absorbed into a soundscape? I'm writing a scene in a personal creative writing project - genre: corny, paranormal romance. I'm chugging through calculus homework. I'm skimming news articles and looking for new games to try. Winamp ingests the 56kbps stream and deposits music. Maybe it's "The Shield" by Biosphere, or "UT1-Dot" by Polygon Window, or "Kalpol Introl" by Autechre.

Mentally, you enter an ocean current. Maybe a thought "slipstream." Your brain is taken along for a ride, swiftly and smoothly. Surroundings fade. There are only the *task* and the soundscape. It causes an incredible sense of focus, an out-of-body experience. Then there is the inevitable interruption. Roommate returns, or the stream disconnects.

Returning to the regular conscious world causes mental turbulence. It's a jarring effect, like suddenly slamming the brakes. The dizzy disorientation of standing up too quickly. Forcefully d-r-a-g-g-i-n-g your consciousness out of the soundscape like hauling a boot out of thick mud. There's a re-calibration period as you adjust to your surroundings and the room takes shape. That's true focus.

The final "first generation" screenshot comes from April 23, 2003. An addition along the left hand side is a link to Jinx Hacker Wear: "Swag for Hackers and Geeks."[14] After that, the site goes dark until 2011. It returns in an updated form, featuring a list of album art and a single "listen.m3u" streaming link. This form lasts for two years, disappearing in 2013.[15]

An mp3 horde replaced streaming music for me in the years between 2003 and 2015, when a hard drive crash cost me thousands of tracks (*back up your data!*). After that, it was YouTube and sites like Nightwave Plaza that satisfied my growing interest in synthwave and vaporwave. These days, I get my soundscape fix from Soma FM, an Internet radio site that, interestingly enough, first went online in 2000. Genres and sites come and go, but I'll never forget the life events that were enhanced by the strange sounds of Music For Hackers.

In retrospect, probably the strangest connective tissue from MFH began with a track called "Seven Day Galaxy" from the 1999 album *Oedipus Brain Foil* by Randy Greif, Robin Storey, and Nigel Ayers. Looking into other works by those artists, I discovered Robin Storey's (under the name Rapoon) album *What do You Suppose? (The Alien Question)*. A well-crafted example of ominous droning ambiance, it featured several samples of a man giving a lecture on Cold War-era alien and secret government conspiracies. Those words and music were perfectly complementary. After some research, I discovered the lecturer was 1990's shortwave radio host and conspiracy theorist extraordinaire William Cooper. The late Bill Cooper, whose program *The Hour of the Time* covered New World Order concepts in exhaustive detail, was perhaps most notable for writing the tome "Behold a Pale Horse." Strange journeys across wild lands, indeed.

[1] alter.com/trademarks/
➥musicforhackerscom-78024924

[2] trademarks.justia.com/780/24/
➥musicforhackers-com-78024924.html

[3] web.archive.org/web/20000229121447/
➥http://www.musicforhackers.com/

[4] web.archive.org/web/20000604080520/
➥http://www.musicforhackers.com/

[5] web.archive.org/web/20001206210300/
➥http://www.musicforhackers.com/

[6] web.archive.org/web/20010604040125/
➥http://www.live365.com/
➥stations/173099

[7] web.archive.org/web/20010721153755/
➥http://musicforhackers.com/

[8] www.theregister.com/2001/02/22/
➥all_your_base_are_belong/

[9] www.bbspot.com/Features/2001/02/
➥obsecurity_server.html

[10] britneyspears.ac/lasers.htm

[11] web.archive.org/web/20001109102400/
➥http://www.routergod.com/
➥garycoleman/

[12] web.archive.org/web/20011205053504/
➥http://somethingawful.efront.com/
➥jeffk/

[13] web.archive.org/web/20010629010627/
➥http://www.meydabbs.com/hack4d0gz/
➥main.html

[14] web.archive.org/web/20030423203357/
➥http://www.musicforhackers.com/

[15] web.archive.org/web/20110207102117/
➥http://musicforhackers.com/

Cryptocurrency - Busted!

by lg0p89

When we hear of cryptocurrency, we think of bitcoin and making millions overnight - and then losing millions the next day. While this is the outward focus, there is still a backbone of technology. This houses the vulnerabilities that we exploit. Historically, the general attack has been the 51 percent among others. There have been variations of this and others. Recently a newer attack has become more prevalent in certain configurations. This ingenious attack deserves a greater level of attention and applause.

This attack by far is not the first and certainly won't be the last. In 2022, there was an attack where over two billion dollars were liberated from a company. Many of these attacks had been perpetrated by persons and groups in North Korea.

This time around, the target was the Binance coin. This wasn't their first rodeo. In 2019, the company was successfully attacked. This time the amount involved was approximately seven thousand bitcoins - or 40 million dollars. In this round of "We Pwned You," the compromise was initially valued at 100 to 110 million dollars. The updated estimates were changed to the attackers liberating two million BNB tokens, valued at around 568 to 570 million dollars.

With this attack, the focus was on the bridge between the blockchains. For this, they were targeting the BSC (Binance Smart Chain) token hub.

The bridge is pretty much like it sounds. There is a link between two blockchains. This acts like a bridge between the two to facilitate the communication. The communication across the bridge allows for the tokens to be transferred from one blockchain (platform) to another blockchain (platform). This attack point has been a focus for some time.

Pre-attack, the group would have reviewed a threat assessment. The blockchain attacks usually take time and resources, so the weak points would have been looked at more closely. The bridge process provided this with multiple points to attack.

Once this was compromised, the attackers were able to move the tokens off of the Binance network. This vulnerability leveraged an issue with the smart contract. This allowed the attacker to create fraudulent transactions and have the tokens sent to their crypto wallet. Since the smart contracts don't require human interaction to execute (by definition), this was done relatively quickly.

After the attack, they began to move the funds across different liquidity pools. This acted to move the BNB into other assets and quasi-clean it. Only an estimated 70 to 80 million dollars were taken off the blockchain. The remaining money stayed on the blockchain and is not accessible to the attacker(s).

After noticing the anomalous activity, Binance temporarily halted activity and new blocks on the BSC. After the heist, the co-founder of Binance announced the issue was contained. Of the stolen funds off of the blockchain (70 to 80 million dollars), approximately seven million dollars had been frozen.

The attack, while interesting on its own, does highlight the need for creative minds to test and re-test any company's processes and infrastructure. We have to stop only using a checklist and hoping we are good. Without a proper and robust pentest, companies will continue to have issues.

WRITERS NEEDED!

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

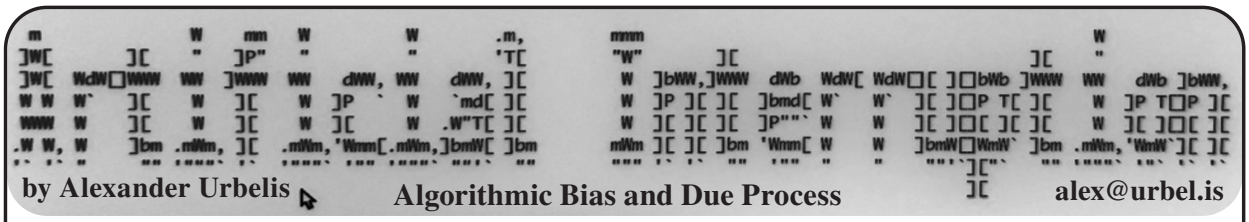
Send your articles to us via email at **articles@2600.com**

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

For those without Internet access, our editorial department can be snail mailed at:

2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

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



by Alexander Urbelis

Algorithmic Bias and Due Process

alex@urbel.is

In December 2021, New York City passed a first-of-its-kind law regulating the use the artificial intelligence in the employment context. That law bans employers from using artificial intelligence or algorithm-based technologies for employment-related decisions - such as hiring, recruiting, retention, or promotion - if an independent third party has not audited those technologies for bias.

Ordinarily useless, banal, behind the times, and out of touch with the people it serves, it seemed like the New York City Council actually passed an ordinance that was worthwhile, on the right track, and protective of New Yorkers' rights against discrimination and bias, even if a machine was responsible for the prejudice. I applauded this legislation. And because it comes into effect in January 2023, I have been helping numerous companies navigate this audit requirement and prepare their disclosures about what, if any, bias results from their AI or algorithm-based employment screening decisions.

As a matter of fundamental fairness, it should be universally agreeable, and even self-evident, that we would want important decisions to be free from prejudice. And if there exists an AI-based system that produced questionable or biased results because of an identified defect, then we would certainly want to revisit and remake those decisions on the basis of a revised process that was free from bias.

As human beings, our decisions are complex and the result of our experiences, emotions, education, and a range of other nuanced factors and, unless someone is a bigot or racist, we all presumably strive to make our decisions in a manner that is free from bias or discrimination. But the complexity of our emotions does not lend itself to being audited. Bias may creep in despite our best efforts. Someone may not think they are inherently racist, but because of their upbringing or experiences, certain prejudices, however subtle, may affect a decision.

This raises the question: could a well-regulated AI make better decisions than humans? And, if the answer is anything resembling a "yes," then that raises a further question: could an AI that is free of bias or discrimination replace a jury in our legal system? And, again, if the answer is anything resembling a "yes," then that raises a further question, a heartbreaking query this time: could an AI have prevented a tragic injustice that occurred on November 29, 2022, at 7:40 pm, in Bonne Terre prison, when the State of Missouri executed Kevin Johnson?

Kevin Johnson was 37. He had been on death row since he was convicted of first-degree murder 17 years ago. On July 5, 2005, Johnson killed a police officer, Sergeant William McEntee. Johnson was 19 years old at the time.

The facts of what happened on July 5, 2005 are heartbreaking on many levels. They do, however, explain in part why Johnson committed a murder for which he later unconditionally repented and for which he paid with his own life.

Suspected of a probation violation, police showed up at Johnson's home on July 5 with a warrant for his arrest. According to multiple sources, Johnson saw the police arrive, woke up his 12-year-old little brother "Bam Bam," who then ran next door to their grandmother's house. Bam Bam had health issues: he was born addicted to crack-cocaine and had a congenital heart defect. When he arrived at his grandmother's house, Bam Bam's health began flagging. According to the *Missouri Independent,* police officers including McEntee entered the grandmother's residence, after which Bam Bam began to have a seizure.

The officers ignored Bam Bam's distress and seizure. According to various reports, the officers stepped over Bam Bam's limp body and never helped him or called for help. The police officers also prevented Bam Bam's mother from offering any comfort, aid, or to even enter the house despite the ongoing seizure. A short time later in a hospital, Bam Bam died.

Johnson was distraught, kicked his bedroom door off its hinges, and, according to the Associated Press, Johnson had then wandered around his neighborhood furious with McEntee for preventing his mother from helping Bam Bam even as his little brother convulsed. Enraged at McEntee, Johnson screamed "He killed my brother!" as he roamed the streets.

A few short hours after Bam Bam's death, Sergeant McEntee was again in Johnson's

neighborhood, called in this time to investigate someone setting off fireworks. Johnson saw McEntee, pulled a gun on him, and shot him. McEntee tried to flee, and Johnson shot him two more times, killing him.

The State tried Johnson for first-degree murder. A first-degree murder charge requires premeditation and could result in the death penalty. The jury, however, was hung. The jury was not quite convinced that the murder was premeditated as opposed to the result of Johnson's emotional and impulsive state.

In 2007, the State tried Johnson again and convicted Johnson of first-degree murder. That conviction resulted in a sentence of death.

The report of a special prosecutor that the Missouri judiciary appointed to investigate claims of racial bias in that second trial concluded that race played a "decisive factor" in the death sentence, and that the process by which Johnson was convicted was "infected" with racial bias. The government, for one thing, tried to remove all black persons from the jury.

The special prosecutor sought to vacate Johnson's death sentence. This was the first time in Missouri that a prosecutor sought to overturn a conviction tainted by discrimination.

Despite the apparent racism and these extraordinary circumstances, after oral argument, the Missouri Supreme Court refused to grant any relief. The Governor of Missouri, Mike Parson, refused any clemency and would not commute Johnson's sentence to life. The last stop was the U.S. Supreme Court. Though Justices Jackson and Sotomayor vigorously dissented, that institution failed to provide any relief as well, clearing the way to Johnson's lethal injection.

As technologists, we understand the axiom of "garbage in, garbage out" as applied to the input and output of a function or program. As technologists, we know that a flawed system will produce flawed results that cannot be trusted. As technologists, this is why we understand and applaud auditing of AI or algorithms for bias, discrimination, and any kind of flaw that could negatively impact our lives or the lives of others. Why, then, do we neither expect nor demand the same kind of common sense and rigor be applied to our justice system?

How much injustice can this system tolerate in the name of justice before it fails to an insecure state? When evidence that racial bias and discrimination permeated a capital case lies in front of you - and even a prosecutor is clamoring for the sentence to be vacated - how can we countenance those in power when they refuse to act? Those persons in positions of political power assumed an awesome responsibility when they took office, and we cannot allow them to shirk their obligations or to act as if they are somehow allowed to abdicate adherence to basic moral principles.

The irony, of course, is that it was because of politics that Governor Parson refused to intervene and stop an execution that was a well-documented result of a racially biased and discriminatory legal proceeding. It was self-interest. It was borne of his own political ambition. When this is the norm, are not dispassionate, unambitious machines better decision-makers?

I have no idea whether a detached, artificial intelligence would have prevented any of the horrible outcomes throughout the process that led to the State of Missouri taking the life of Kevin Johnson. What I think is crystal clear, however, is that we need to apply the same low fault tolerance levels of the technological systems we design to the justice system of which we are all a part. If we are right to be so cautious about bias seeping into the decision of whether a private company grants a job applicant an interview, then, *a fortiori,* shouldn't we be infinitely more concerned about bias seeping into the decision of whether the State should terminate the life of one of its own citizens?

Auditing AI systems for any hints of bias is not only about identifying and remediating prejudicial algorithms. It is also about accountability for discrimination and prejudice. We demand accountability of private parties, but it is also that which has been missing from our political processes and justice system. So many of our institutions that should have acted to prevent injustice - the prosecutor's ethical obligations, the jury system, the appointment of a special prosecutor, the trial courts, the appellate courts, and the U.S. Supreme Court - turned a blind eye.

No doubt there were many that tried to act, but it was aggressive apathy that prevailed in Johnson's case. With such ample evidence around us that we have created and are perpetuating an imperfect justice system that produces prejudice with no accountability, we owe it to ourselves to prioritize change, especially if we are to continue being the ones to audit AI systems, and not the other way around.

Tales for My Toddler

by macmaniac

Disclaimer: I do not encourage piracy. Remember that some artists are depending upon you paying for their music.

Some time ago, I purchased a music player for my toddler. I mention this because I like the producers' spirit (the producer of the player, not of the toddler - the latter is me). That player is built to last, energy saving by using wav instead of mp3, easy to deal with by toddlers and to maintain by their parents. Last but not least, their answer to "Well, I use Linux..." is not "We don't support Linux." but "Our Linux application is still being developed, but have a look at this script that some customers wrote. Maybe it's helpful."

For months everything was fine as the pre-installed music files were enough for my toddler. But some days it was enough for me. Another day of "Baah Baah Black Sheep" in endless loop - no way! So I decided to put some other stuff on it. If you have mp3 files, you can just convert them to wav and put them on the player's SD card. But getting the desired sound is not too easy, as I found out.

Now I have to mention that I'm from a small country with its own language. Albeit our laws concerning pirating are rather liberal, it's hard to find content in my language. And even harder to pirate kids' stuff. Toddlers and loving parents are not known for being pirates, arrr! So I was looking through my old stuff to find music or tales for my toddler. I found some tapes. But no player. For the blink of an eye, I was thinking of tearing the tape out and getting a pencil to roll it up again. Nah, these were the old days. I came across some compact discs (CDs) with nicely told tales. For DVD ripping purposes, I still own a CD drive. So I was able to rip the tale, convert it to wav, and put it on the player.

The next thing was a song we had watched on YouTube. This was the only source I could find. A video. The sound on its own was not available anywhere. Luckily, youtube-dl[1] still exists and hopefully will forever. It's a mighty tool to rip copyleft videos from YouTube and other platforms. But it also lets you solely extract the audio tracks. As YouTube is so big, you can get a lot of content from there.

Another big thing is Spotify. It doesn't stream videos, but songs. And even lets you save songs offline! But these files are still encrypted. So there's no chance to just copy your favorite songs to another device. I found some dubious browser add-ons and applications that claimed they could de-DRM Spotify. No thanks. There was nothing like youtube-dl for Spotify, reason why I looked for other ways to get the latest Peppa Pig tales on that player!

Audacity came into my mind. Another powerful tool I know from the days I wanted to be a rapper and needed some professional but cheap (that is - free) audio editing software. This tool is capable of recording directly from your soundcard - which means recording without any degradation[2]. The downside: it's like old-fashioned recording - it takes time. And if you record a playlist, you need to split and export the single tracks. It wouldn't be a mighty tool if a manual didn't exist on how to do this the easy way[3].

Wouldn't it be great if some script existed that would automate the whole Spotify/Audacity process? Or even some youtube-dl equivalence for Spotify? I'll leave these tasks to brains that are more skilled than mine.

P.S. The player is called Hoerbert. Have a look: www.hoerbert.com.

[1] youtube-dl.org/

[2] manual.audacityteam.org/man/tutorial_recording_computer_playback_on_linux.html

[3] manual.audacityteam.org/man/splitting_a_recording_into_separate_tracks.html

Raising Generation Orwell: A Guide to Teaching Kids the Human Rights of Privacy

by Worlds_Gr8test_DeFective

I was born at a time where I consider myself both lucky and unlucky to come of age during the analog to digital transformation. I can vividly remember when you could only get in touch with someone if they were home, when staying in touch with your friends was a question of "do you have Internet?" instead of "what's your Insta?", and when I could walk down city sidewalks without seeing CCTV or an Internet-connected camera in everyone's hands or beside their doorbell.

I consider myself lucky because I grew up with a slower pace of communication, with less expectations to have an "online presence," and when privacy in public was the norm. Where I am unlucky is that, as an adult, I have been coerced into an "always on" working culture, facial recognition technology paired with Internet-connected cameras and microphones every square meter that is enough to put your subconscious in a manic state of paranoia, and legislation such as the Patriot Act in the United States constantly expanding its capabilities to abuse the very technology that is meant to bring us closer.

So how does this tirade fit into the title of this article? I remember a time when this was not normal. When it was different. I am conscious of the subtle surrenders of privacy we have stumbled into. Children and teens today are growing up in an increasingly surveilled world which is the norm for them. They will never remember a time when returning to the United States from overseas travel meant you did not have to surrender your electronic devices to Homeland Security for inspection, or entering a country by air travel did not require you to provide your biometrics at a kiosk prior to crossing customs.

So what can we do about this? Legislation is not keeping up with the pace of Internet-connected technology from a security and privacy standpoint, so I believe our best strategy forward is to harden the coming of age generation with privacy awareness. Please consider the following suggestions in how to accomplish this:

- Before taking a photo or video of a child, ask them for permission. Kids now are conditioned to seeing Internet-connected cameras constantly at home and in public. Asking them permission gives them control over their digital footprint.
- Educate kids and teens who use Internet-connected devices on vendor telemetry collection and the monetization of data analytics. This will help them understand that the communication between their source device and the destination is usually more than a two-way connection and involves sometimes up to hundreds of third parties collecting personal and technical data. Do not do this as a sense of paranoia, but as an awareness piece on understanding what information is collected over the Internet as an end user. You can take this a step further by analyzing network logs or using services such as Electronic Frontier Foundation's (EFF) Privacy Badger to visualize data analytics collection.
- Show what surveillance technology your security forces and local law enforcement use in public areas or, in some cases, on private property. Explain how license plate readers can be abused for profiling patterns of life and how Amazon Ring has the capability to back up recorded footage and audio forever. This footage can also be integrated with Amazon's Rekognition or Clearview's facial recognition technology and indexed into a criminal database if an agency integrates these services. A good starting point for this information is the Atlas of Surveillance project by EFF or the work done by The Citizen Lab.
- The most important aspect of this is to not under any circumstances teach kids to be paranoid. It's very easy to fall into the abyss of paranoia when researching how emerging technology invades privacy. You will do them no favors by scaring them into thinking Big Brother is always watching. Empower them to have control over their digital footprint and to understand the privacy risks of attending a protest or sharing photos over social media. Arm them with knowledge and surveillance self defense, not fear.

```
#!/bin/sh

# Consider that perhaps nmap is unavailable to you, but netcat is.
# Netcat has scanning functionality, but it can be a little slow.
# This script will speed things up by running several instances of
# netcat in parallel.
#
#    - Justin Parrott

NUMTHREADS=10
TIMEOUT=3
STARTPORT=1
STOPPORT=1024

usage() {
        echo "usage: $0 [options] host"
        echo "  -s startport        Where to start the scanning (integer)"
        echo "  -S stopport         Where to stop the scanning (integer)"
        echo "  -t numthreads       Number of processes to execute in parallel"
        echo "  -w timeout          Timeout per connect (integer)"
        exit 1
}

while getopts s:S:t:w: opt
do
        case $opt in
        s)      STARTPORT="$OPTARG";;
        S)      STOPPORT="$OPTARG";;
        t)      NUMTHREADS="$OPTARG";;
        w)      TIMEOUT="$OPTARG";;
        \?)     usage;;
        esac
done
shift $((OPTIND - 1))

if [ $# -ne 1 ]
then
        usage
fi
HOST="$1"

tcping()
{
        nc -z -w "$to" "$host" "$port"
}

i="$STARTPORT"
running_threads=0
while [ "$i" -le "$STOPPORT" ]
do
        port="$i" host="$HOST" to="$TIMEOUT" tcping &
        running_threads=$((running_threads + 1))
        i=$((i+1))

        if [ $running_threads -eq "$NUMTHREADS" ]
        then
                wait
                running_threads=0
        fi
done

wait
```

The Search for Life at 300 Baud

by N1xis10t

N1xis10t@protonmail.ch

In *2600 Magazine* 38:3, a letter to the editor was featured in which a person named HC asked if anyone remembered a publication entitled "Life at 300 Baud." The editors said that they didn't find anything when searching for it online. My interest was piqued after reading this exchange, and I set off to conduct my own search for this elusive publication. It took several searches with several different search engines and variations in keywords, but I did end up finding two published items that may be what HC was remembering. One is a full fledged magazine bearing the name of *300 Baud*, and one is simply a magazine column, but it bears the full correct name of "Life at 300 Baud."

When I was looking for this publication, the first thing I did was run a simple search (Life at 300 Baud) though my go-to search engine (DuckDuckGo). Almost immediately, I found a web article that was discussing a magazine called *300 Baud*. I then checked the Internet Archive to see if this magazine was available, and much to my delight, I found the entire limited run. I continued the search by putting my first search term in quotes to look for an exact match in DuckDuckGo, and also ran a search with the meta-search-engine Dogpile. With these two searches, I found an obscure reference to an article in a column called "Life at 300 Baud," and also an interview with an investigative journalist who appeared to have written this article. Interesting. Next, I looked at Google Books, and found a couple more references to "Life at 300 Baud" articles. Armed with some of the information from the interview, I decided to look for the magazine containing this column. It looked like it was a magazine called *ProFiles* that was written for users of KayPro computers. I searched DuckDuckGo for "Kaypro users magazine profiles" (without the quotes), and found this magazine on the Internet Archive. Sure enough, the "Life at 300 Baud" column is featured in many of the issues. I did run more searches, but ultimately didn't find anything more. With all the searching out of the way, I could now study these magazines closer.

The first publication that I found, *300 Baud*, was a periodical about retro computing that ran for three issues, starting in January 2010. It had a good article selection about all sorts of cool stuff, from using the Internet with old computers to soldering without burning your fingers. All three issues are available for free at this location on the Internet Archive: `archive.org/➥details/300baudzine`

The second publication that I found is more likely to be the one we are looking for. "Life at 300 Baud" was a regular column in a 1980s computer journal called *ProFiles: A Magazine for Kaypro Users*. "Life at 300 Baud" was written by the investigative journalist Brock Meeks, and can be found in most issues of the magazine, beginning with Volume 2, Number 3. It makes for fun reading, with many of the articles exploring different facets of the old Internet, and providing interesting insights into different kinds of bulletin board systems. A nice digital archive of the *ProFiles* magazine is available at: `archive.➥org/details/kayproprofiles`.

I was intrigued by HC's missing publication, and when I dug a little deeper into the more musty corners of the Internet, I did manage to find a thing or two. I do hope that one of these publications turns out to be what HC was looking for. Even if this isn't the case, it sure was fun to conduct an in depth search like this, and I am happy to have found some interesting new reading material.

Useful Resources

- Article about *300 Baud* magazine: `www.➥apl2bits.net/2010/07/19/300-➥baud-magazine/`
- Interview with Brock Meeks: `www.➥digitalriptide.org/person/➥brock-meeks/`
- *300 Baud* magazine archive: `archive.➥org/details/300baudzine`
- *ProFiles* magazine archive: `archive.➥org/details/kayproprofiles`

Search tools that I used:

- DuckDuckGo: `duckduckgo.com`
- Dogpile: `www.dogpile.com`
- Google Books: `books.google.com`
- The Internet Archive: `archive.org`
- The WayBack Machine: `web.archive.org`
- WorldCat: `www.worldcat.org`

Hey, I Paid For This Cabin

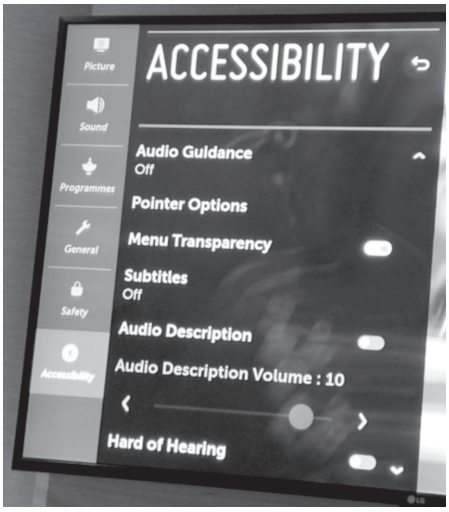
by the6thv3n0m

The information shared in this article isn't some sort of mind-blowing hack, but just serves as an example of what can be accomplished when you have a hacker mindset.

First off, the obligatory disclaimer. This information is for educational purposes only and I bear no responsibility should you use it in a malicious way.

So my wife and I just recently took a cruise. Anyone who has taken one before may notice that the TVs in the room typically have the sleep and/or auto power off timer set to turn off the TV at a set time (typically four hours). This may sound a bit petty, but both my wife and I are used to leaving our bedroom TV on all night at home and tend to get upset when during the cruise, if we happen to be in an inside cabin, we wake up to a completely dark room. While we both have gotten used to the sound, one of the main purposes at home is that it acts as a source of light should one of us need to get up in the middle of the night. Anyway, on most, if not all cruises, they will provide a very generic remote control like the one pictured below. If you've been on a cruise, you may immediately recognize it.

As you will notice, given that it's just a generic remote control, there are no buttons available to provide access to the TV settings. My goal now was to figure out how to access the settings for the TV to allow me to either change or disable the sleep timer and/or auto power off settings. After trying a few various button combinations, I stopped and really took a good look at the remote. I then thought that cruise lines, given the large number of passengers they have to manage week after week, would probably have this set to something that is relatively easy to remember and access, but would not seem as clear to the average passenger. Giving it a bit more thought, I asked myself "what would be the least-used button on the remote?" Given that there is typically an overlay system providing all the features (i.e., viewing account, ordering food, viewing ship activities, etc.) pretty much every button on the remote is used to maneuver except one, the mute button. So I pressed and held the mute button. A colorful circular graphic appeared on the center of the screen and behold, the settings for the TV appeared (pictured below).



I now had access to all of the settings, and therefore full control of the TV, including my primary goal: the ability to now change and/or disable the sleep timer and/or auto power off settings (pictured below). I immediately located these settings and disabled the option, which now left the TV on until either we manually turned it off, or the cabin stewards did.

Performing some additional exploration, I noticed some other interesting things such as the fact that although this was a smart TV, it was not configured with any network information. There was also the ability to disable the overlay mentioned above. On Carnival Cruise Lines, this overlay is called HubTV, for example. When the cruise was over, I restored any settings that I changed. Since they remained unchanged for the duration of the cruise, it wasn't clear if they would be prior to the next round of passengers boarding the ship.

Hope you found this interesting.

Hacking involves a different way of looking at problems that no one's thought of. - Walter O'Brien

An Atavistic Freak Out, Final Chapter

by Leon Manna

This story is a work of fiction.

When they arrested us, I had dyed half of my hair light brown.

"Your honor, I'd like to begin with the fact that a recent malfunction in the FBI offices of the witness we will be having sworn in, Segev Bezalel -"

"You pronounced his name wrong, it's Bitch." This came from the defendant's table, and then a fake cough. The witness snickered from across the room. The judge yelled at me to shut up or I would be held in contempt of court.

Lenny continued. "Segev Bezalel, whose evidence room caught on fire due to a malfunction in the thermostat, has been unable to produce any evidence so far tying my client or I to any of the charges that are currently levied against us."

Some guy from the district attorney's office shouted that he objected for the millionth time that day, and his motion was not sustained, although quite a few were. They ended up calling Moe to the stand to testify. The prosecutor asked him about the intrusion that corrupted all of the computers and servers in his office.

"Yes, somebody installed malware on all servers and computers in my office."

"And who do you think did it?"

"Leon Manna."

"How do you know?"

"A combination of the childish message and Leon's real capabilities to do such a thing. The planning was characteristic of Leon's previous plots, such as Sawtooth."

"Sawtooth, where he was seen doing fraud in person?"

Fuck.

"Yes, exactly."

Fuck, again.

He asked a few more questions. Soon after, Lenny went in on him. "Tell me, Mr. Bezalel, about the IP address that was associated with this attack?" He had a look on his face like he was planning something.

"It was some kind of uh... proxy." He stuttered! Sweet-mother-of-god, here it comes!

"And where, exactly, was this proxy located?"

After a brief pause, he said, "Turkey."

"Were you able to get jurisdiction in Turkey and subpoena this server?"

"No."

"Then how can you be so sure this was tied to me and my client?"

"It was timed with your planned escape."

"Did the exact same attack not happen in multiple other locations nationwide? How can you be so sure that this wasn't some act of planned terror by a greater force and not some vagrant who wanders across the country? My client isn't capable of something that meticulous, at least not in that timeframe." I made sure to do the same thing a bunch of times. Everywhere. A lot of places. As many as I could. I am god. I am not an American terrorist.

"Well... I mean... Technically... No."

"I heard Sawtooth was mentioned, how can you say for sure that it was my client? How do you know?"

"We have CCTV footage of your client in the bank, as well as witnesses." He did not sound confident.

"Have? Or had."

"Have."

"Where is it?"

Segev glared at Lenny. The judge told him to answer.

"We're working on that."

But Lenny continued. "Sawtooth was robbed by a man named Joseph Erickson. As far as we know, Joseph Erickson is dead. And as for your evidence, it was destroyed in an act of terrorism, *from an outside source,* combined with a malfunction in the evidence room. Was it not?"

Moe chuckled, and said, "It was."

"Is that the case? Then how come Sawtooth was unable to recover the footage

from their own system?"

"That information is classified. We don't have to tell you. We're not going to tell you. Leon knows, why don't you ask him?"

Lenny paused, and gave him a strange look. "You're aware perjury is a crime, right?"

Moe continued to give Lenny the death stare.

"I rest my case."

Then they brought in the bane of my fucking existence, Khir, who got on the stand for 15 minutes but was ultimately unable to say for certain that I was the man he saw in the bank. My disguise was so half-assed, but despite what I thought, worked. Thank you, uh... What was his fucking name... Joseph Erickson! Thank you!

Liz denied sitting next to me on the stand due to the fact that there was now no CCTV footage and nobody was present in the room when she uh... *didn't* do this and the prosecution was unable to get anything useful out of her.

They pulled the clerk from the car rental place up. She said she couldn't identify me (I'm a shapeshifter) even though she definitely could, did not feel like ratting me out, and was willing to lie under oath for me. I smiled at her. She smiled back. I didn't technically go in there. Somehow she seemed prettier than before. From across the courtroom, she looked like an angel.

They were unable to get in contact with Aryana. Probably for the best. Hope she's okay, though I heard she still hates me. I think she moved to Europe and found a nice French boy. John Capper refused to testify for obvious reasons. He was arrested on a failure to appear warrant, and was sentenced to 15 years for murder when they tied him to the crime. I think I disabled the script on their server while I was blacked out on bromazepam. I don't remember. May went missing and is presumed to be dead, which *totally* happened and is 100 percent true. She has them fooled though. I think she's a contract killer now, or some shit like that. Unconfirmed reports, but I know it was her. A woman matching her description was seen with several men who later died of cyanide poisoning. Goldstein also did not testify; he was busy testifying for a different case. I think they understood the nature of, well, Goldstein, and gave him a pass on that. Pierre moved to Ireland. Quite often I like to imagine he's still out there somewhere, riding out on the water. Right now he is a fugitive. Ireland did not extradite him, if they ever even found out that the fake identity I set up for him there was a fake identity.

The only charges we couldn't beat were the drug possession charges. A couple misdemeanors, one felony. I spent ten days in a state hospital for an evaluation before they released me on probation, under the conditions that I participate in an intensive outpatient program and if I fail drug tests or fuck up at the IOP, they will send me to jail or a mental hospital. Again. Mountain View State Forensic Hospital. There were people in there who hadn't seen the sun in years.

I got a call from Segev when I got out. "You tryna smoke?"

I said yeah. Even an FBI agent can break the rules.

And in the end, I learned nothing. There doesn't seem to be some kind of moral to the story here. I just couldn't figure it out. I was so close. By only a hair, they got me. But that hair was just in reach.... What if I had done it right? What if I had gotten away to Cuba? What if I hadn't mistreated my ex-girlfriend? Then it hit me like a bolt of lightning.

Hah hah hah.

What if I did it all again? I sat in my apartment for a moment, thinking. Then, in the blink of an eye, my new name is Lee Williams. Lee Williams was born into this earth through a Ring Zero rootkit I installed on an SSA machine a lifetime ago, just like Leon was all those years back, and he was a new man, born again, for a second trial. A fallen angel, if you will. Which you won't.

Then, I reached into my drawer, pulled out a check, and the outworn chase of money continued.

Enjoyed "An Atavistic Freak Out"? Buy Leon a coffee!

`BTC: 39L63B9qAiAnPbqqLZempJQG8xeXVRFvYT`

HACKER HAPPENINGS

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

Events are subject to change. Please be sure to follow all safety protocols that are put in place by these events and venues.

April 14-16
Vintage Computer Festival East
Infoage Science and History Museums
Wall, New Jersey
vcfed.org

April 22-23
CoCoFEST
Holiday Inn & Suites Carol Stream
Carol Stream, Illinois
www.glensideccc.com/cocofest/

May 19-20
THOTCON 0xC
Chicago, Illinois
thotcon.org

May 19-21
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

June 13-14
RVAsec
Omni Richmond Hotel
Richmond, Virginia
rvasec.com

June 23-25
CircleCityCon 10.0
The Westin Indianapolis
Indianapolis, Indiana
circlecitycon.com

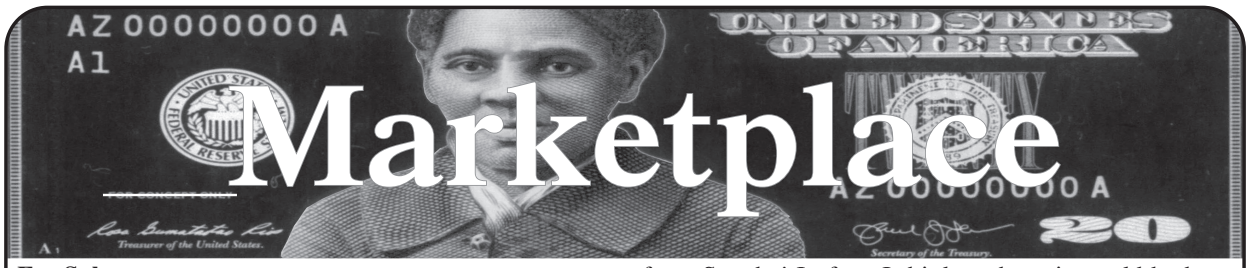
August 2-9
BornHack 2023
Funen, Denmark
bornhack.dk

August 10-13
DEF CON 31
Caesars Forum, Harrah's, Linq, Flamingo
Las Vegas, Nevada
www.defcon.org

September 28-29
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

September 28-30
Texas Cyber Summit
JW Marriott
Austin, Texas
texascyber.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

HACKERBOXES is your monthly subscription box for hardware hacking, DIY electronics, cybersecurity, and hacker culture. Each monthly HackerBox includes a carefully curated collection of projects, components, modules, tools, supplies, and exclusive items. A HackerBox subscription is like having a hacker convention in your mailbox every month. Free online educational material, free domestic shipping, cancel anytime. Visit us at www.HackerBoxes.com for workshops, boxes, merch, and more.

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

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

SECPOINT PORTABLE PENETRATOR. WPA WPA2 WPS WiFi Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports with logo, name in PDF or HTML format. Coupon code 20% off: 2600. https://shop.secpoint.com/

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

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

Announcements

LEAGUE OF EXTRAORDINARY BUDDHIST HACKERS: Calling Buddhist Hackers, Phreaks, Makers, Preppers, Stitchers, Devs, Medics, Biohackers, Graphics Peeps, Videographers, Kind people, any or all of the above, etc. (Actually the last one is mandatory!) I am looking to build a global crew of persons (Kalyana Mitra) male/female/other (I will even consider aliens from other world systems at this point) who identify with the above description. Please only make contact if you have taken the 3 refuges and you are making some efforts to keep 5 precepts (and 8 precepts on Poya Days etc.) + have some sort of attempt at a daily practice - well at least some days! If you are at that sort of level, please contact me ASAP. Also Buddhist Monks/Nuns, I would love to hear from you, but again please only get in touch if you are keeping good vinaya/precepts. Having said that, I think it would be great to hear from Sangha! In fact, I think perhaps it would be best if one of you (Sangha) were running the outfit? Hack the Planet! Hack Samsara! I believe I have found the ultimate hack... TN8FP - but it requires a team effort, no? .,\/(^_^) & <3 from Blebz (open nick) email: blebz@lxbh.org for more info...

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime*, Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at https://modern.technology

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

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net.

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

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at https://doc8643.com.

Services

HAVE YOU SEEN THE *2600* STORE? All kinds of hacker clothing, back issues, and HOPE stuff! We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. It's great for giving out presents with a hacker theme - or gift cards are available for those who'd rather make their own choices. The store is constantly getting bigger and more interesting. Please come pay us a visit! store.2600.com or 2600.store

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 talk to a lawyer who represents me." Remember basic game theory and the Prisoner's Dilemma: nobody talks, everybody walks. This is a public service brought to

you by freedom defense attorney and *2600* subscriber Omar Figueroa. https://www.omarfigueroa.com/2600-know-your-rights/

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

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're 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 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! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

KB6NU's "NO NONSENSE" AMATEUR RADIO LICENSE STUDY GUIDES make it easy to get your Technician Class license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time, give you the answers to all of the questions on the test. The PDF version is FREE, but there is a small charge for other versions. All of the e-book versions are available from kb6nu.com/study-guides. Paperback versions are available from Amazon. Email cwgeek@kb6nu.com for more information.

DIGITAL FORENSICS EXPERTS FOR CRIMINAL AND CIVIL CASES! Sensei's digital forensic examiners hold prestigious certifications including the CISSP, CCE, CEH, CCO, and EnCE. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, theft of proprietary data, data breaches, interception of electronic communications, rape, murder, wire fraud, espionage, cyber harassment, terrorism, and divorce matters. We can preserve, analyze, and recover data from many sources, including computers, external media, smartphones, and social media. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

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

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

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (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.)

Personals

HELLO PITTSBURGH & WESTERN PENNSYLVANIA. I'm looking for like-minded individuals to help relaunch monthly *2600* meetings in this area. I have access to a comfy conference room in a conveniently located suburban shopping center. Send me a letter with everything you think I should know: MARS, PO Box 27050, Pittsburgh, PA 15235. Confidentiality guaranteed.

[NOTE: We have learned that Discount Dave (below) has passed away. We are running his ad one last time as our tribute.]

HEYYY! Discount Dave here. Be sure to check out my website, it's well futile. http://discountdave.neocities.org (I am the master of my subdomain) and please send me any tips on surviving modern life with an iPhone 7. If you see me in my *2600* hat around Boston, be sure to stop me and say hello, unless you are ratbag actor Kevin James.

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 next issue: 3/5/23.

HOPE LIVES ON!

Get The Most Recent Flash Drive From A New HOPE!

That's right, we have every talk that was given at last summer's "A New HOPE" conference on a single 256gb flash drive!

Each talk is available as a video or audio file and can be copied to any device of your choosing or shared with as many people as you wish.

This was our first conference at our new location at St. John's University in Queens, New York City. You can experience or recapture the excitement that was in the air for all three days. A full lineup of talks can be found at xiv.hope.net.

There's an easy-to-navigate digital guide to all of the talks and - while supplies last - you'll also get a printed program and "A New HOPE" badge!

Just $89 (plus shipping) for a gigantic reusable drive crammed full of talks from "A New HOPE." Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

ALL 14 HOPE CONFERENCES!

If you truly want to witness the hacker world grow and change, we recommend getting ALL of the videos from each and every one of our conferences. Yes, we saved it all, and we believe it's a must for the library of anyone with an interest in this sort of thing.

You'll get 9 flash drives packed with all of the recorded talks from each of our 14 conferences:

HOPE (1994)
Beyond HOPE (1997)
H2K (2000)
H2K2 (2002)
The Fifth HOPE (2004)
HOPE Number Six (2006)
The Last HOPE (2008)
The Next HOPE (2010)
HOPE Number Nine (2012)
HOPE X (2014)
The Eleventh HOPE (2016)
The Circle of HOPE (2018)
HOPE 2020 (2020)
A New HOPE (2022)

Each conference comes with an easy-to-navigate digital guide and all talks are DRM-free, meaning you can copy them and view them anywhere (and reuse all of these drives for other things!).

You can get it all for $349 plus shipping. Full details at store.2600.com or write to *2600*, PO Box 752, Middle Island, NY 11953 USA.

"I just want to retire before I go senile because if I don't retire before I go senile, then I'll do more damage than good at that point."
- Elon Musk

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Facebook Team
astrutt, Cryovato, Tina Rose, TechnoMage, danixdefcon5, ItsTehPope, LadyNikon, Osiris

Inspirational Music: Black Star, BACKWHEN, Future Crew
Shout Outs: #42, Mastodon, Welton Chang, Kirby, #10, Arseny, Curiosity Rover
R.I.P.: Jim, Red Balaclava, Jeopardy Jim
Welcome: Luna

***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 - $31 individual, $60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate

BACK ISSUES:
Individual issues for 1988-2022 are $7.25 each when available. Shipping added to overseas orders. All back issues (1984-2022) available digitally as annual digests at store.2600.com

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

2600 MEETINGS ARE STEADILY RETURNING. PLEASE CONTINUE TO TAKE PRECAUTIONS WHERE WARRANTED. KEEP CHECKING THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS INFO ON HOW TO START YOUR OWN MEETING!

ARGENTINA

Buenos Aire: Bodegón Bellagamba, Armenia 1242. 1st table to the left of the front door.
Saavedra: Pizzeria La Farola de Saavedra, Av. Cabildo 4499. 7 pm

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 7 pm

JAPAN

Tokyo: The HUB, Shibuya Center-Gai. 7 pm

PORTUGAL

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

RUSSIA

Petrozavodsk: Good Place, pr. Pervomayskiy, 2. 7 pm

SPAIN

Madrid: Maldito Querer, C. de Argumosa, 5. 7 pm

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.
Stockholm (@2600Stockholm): Urban Deli, Sveavägen 44.

UNITED KINGDOM

England

Bournemouth (@bournemouth2600): The Goat and Tricycle, 27-29 W Hill Rd. 6:30 pm
London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm

Scotland

Glasgow (@Glasgow2600): Bon Accord, North St. 6 pm

UNITED STATES

Arizona

Phoenix (Tempe) (@PHX2600): Hurts Donut. 2161 E University Dr. 6 pm
Prescott: Merchant Coffee, 218 N Granite St.

Arkansas

Fort Smith: Fort Smith Coffee Company, 70 S 7th St. 7 pm

California

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

Colorado

Denver (@denver2600): Denver Pavilions. 6 pm
Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

Farmington: Barnes and Noble cafe area, 1599 South East Rd.

Florida

Boca Raton: Barnes and Noble on Glades Rd.
Jacksonville (#Jax2600): The Silver Cow, 929 Edgewood Ave S.
Titusville: Krystal, 2914 S Washington Ave. 6 pm

Illinois

Urbana: Broadway Food Hall. 6 pm

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Nifty Nate's, 246 North St.

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

Missouri

St. Louis: Arch Reactor Hackerspace, 2215 Scott Ave.

New Hampshire

Jaffrey: Cafe 532, 79 Hadley Rd. 6:30 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm
New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.
Rochester (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Transfer Co. Food Hall, 500 E Davie St. 7 pm

Oklahoma

Oklahoma City: Big Truck Tacos, 530 NW 23rd St.

Pennsylvania

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell. 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm
Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.
Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm
San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

Salt Lake City: 801labs Hackerspace 353 E 200 S, Suite #B. 6 pm

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Washington

Seattle: Merchant Saloon in Pioneer Square. 6 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, *2600* meetings begin at 5 pm local time. Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle or hashtag so we can stay in touch and share them here! To start a meeting in your city, DM us or send email to meetings@2600.com.

NOTE: Please do not come to meetings if you're not vaccinated. This is for your own safety. Proof of vaccination is not required but we hope that common sense prevails.

www.2600.com/meetings

Artistic Payphones

Germany. Seen in a museum in Düsseldorf, this is an actual work of art by the artists Christo and Jeanne-Claude. The notes next to the exhibit say the payphone "was an important object" during their time in New York City when "they had to communicate with numerous people." We concur.

Photo by Kai Kramhoeft

United States. This working phone is directly outside the Buncombe County Courthouse in downtown Asheville, North Carolina and is used by people without cell phones who are going through court proceedings. The positive and comforting messages here have likely helped many through difficult times.

Photo by Will Hazlitt

Poland. This relic was found at the Klubokawiarnia KEN54 pub in Warsaw. The phone itself would qualify as a work of art, but the surrounding decorations certainly add to the atmosphere.

Photo by Sam Pursglove

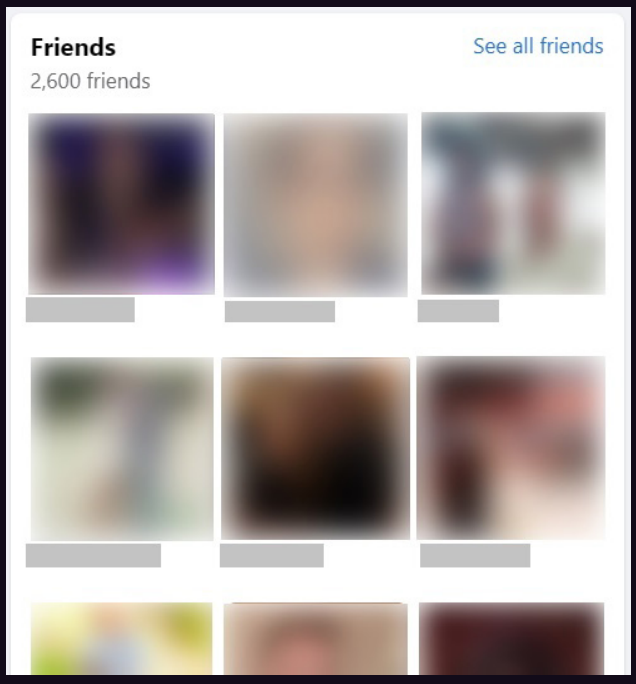
United States. Maybe it's the landscape or the way the colors really seem to go well with each other, but we found this non-working, lonely phone to be a thing of beauty. Seen in Julesburg, Colorado along the South Platte River Trail Scenic Byway.

Photo by Screaming Yellow Fish

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

The Back Cover Photos

We had quite a reaction to the picture of the typewriter repair shop we printed a year ago. **Dan Grebb** found *another* one, also in Pennsylvania! This one is in Lansdale and has been around since 1945 - and hopefully will be much longer. Having "1337" as an address just adds to the magic.



So this is an accomplishment to be proud of: hitting the 2600 mark in Facebook friends. While **dsttyy** considers most of these people to be acquaintances and not actual friends, it's really all about the number for us. And they swear this wasn't Photoshopped. (And obviously, there's no reason for anyone to ever send us another picture when this exact scenario happens to them.)

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.