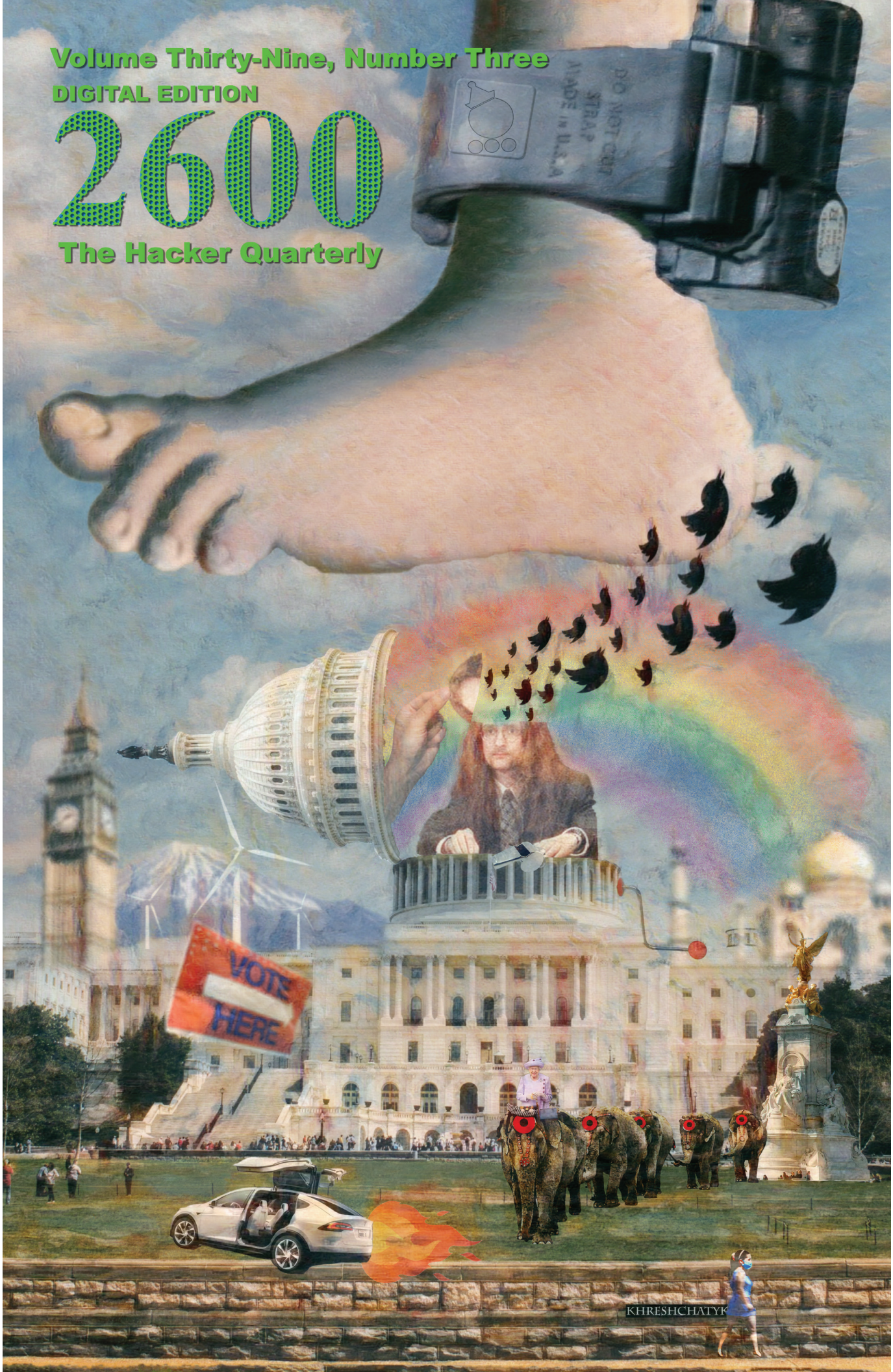
Volume Thirty-Nine, Number Three
DIGITAL EDITION

2600

The Hacker Quarterly



Defiant Payphones

England. As long as these boxes exist, we'll always believe there's hope for payphones. You can find them dotted all throughout the country. This one was in Whinfell Forest, Brougham, Cumbria.

Photo by XCM

United States. You may have heard stories a few months back about the last payphone in New York City being disconnected. But there are still plenty around and here's the proof. You can visit this one in the subway station at Rockefeller Center.

Photo by Zachary Edminster

Austria. You may think it's the plant that's being defiant here in Vienna. But it's the payphone that's really struggling to remain relevant. And this one works fine - if you can get to it. (And note the size of that phone booth!)

Photo by Richard Hanisch

England. This phone seems a bit defensive with its threatening tone and use of the word "loser." But it's clearly been through a lot and is likely still under constant attack. Even the nasty ad warning against vandalism has been defaced.

Photo by Matt Thrailkill

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 (Do not send us links as photos must be previously unpublished.)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

Explanations

The Rule of Law

We've complained about a lot of things in these pages over the years. And we don't see that coming to an end anytime soon.

In the hacker world alone, there have been so many cases of injustice that many books can and have been written concerning only some of them. This has been the case from the beginning, mostly based upon fear and misperceptions. Intelligent people are punished, castigated, thrown out of school, fired from their jobs, even sent away to prison all because of fear, anger, and a general lack of understanding.

It's that last element that feeds the other two and it parallels so much else that goes on in the world and that has filled our history. Not understanding people who are different in some way is what causes some to want to hurt them - or at least to keep them far away.

We speak out about these things because we feel we must. Especially those instances where more people seem to disagree with our conclusions... those are the ones where our voice may be the only opportunity to hear a different perspective.

But, of course, injustice is everywhere, and the hacker community is rather tiny when put into perspective. In the larger world of technology, we frequently witness issues of privacy intrusions, corporate abuse of technology, governmental overreach, or just plain old shoddy security that helps make it all possible - this is all injustice of a different kind that affects everyone in some manner. Technology enthusiasts like us have a unique view into these issues and often can explain things in ways that others can't or won't. Again, we feel compelled to use our voices to draw awareness when it all just doesn't seem right.

And, of course, we also touch upon the bigger picture on occasion, where events are just too consequential to ignore. Movements towards fascism, oppression, mass disinformation, or all manner of ugliness that can turn the tides of history - these cannot go unremarked, even when our voice is but one microscopic element of a chorus standing up against the darkness. We must never silence our true feelings, not when we feel alone nor when we feel like we're amongst millions.

But throughout all of these instances, each and every time we've spoken out on some issue, raised awareness of an injustice, or questioned assumptions, we've never given up on the system itself, even when that system was proving to be corrupt or broken. We always believed that there was a pathway for justice to prevail, however difficult.

We've seen federal agencies like the FBI and the Secret Service lie and abuse their power many times over the years. We've witnessed all kinds of abuse by law enforcement in many jurisdictions. And we've experienced our share of ignorant judges, caught up in their own feelings of power and control, unwilling to learn or question their own preconceived notions.

But we've also seen good. We've been there when justice *has* prevailed. We know that the system can change if we get involved and start changing it from within. We believe in people power, a difficult but invaluable nut to crack, but which is capable of forever altering everything once awoken.

While some of this might seem naive and hopelessly optimistic, what matters is that we all speak our minds honestly and do our best to build the world we want, all the while dealing with the inevitable setbacks and disappointment. The progress is there if we're willing to see it.

In recent years, we've been disturbed by increasing signs that these beliefs aren't actually held by everyone, particularly those who had previously claimed to value them more than anyone else. And apparently, all it took to unveil this well hidden truth were some simple setbacks of their own.

Recent events in our nation have uncovered some truly shocking truths. The sense of entitlement that a particular faction clung to turned into something much uglier once it was questioned and defeated. Many of us saw

something like this coming. But the majority didn't realize what we were facing until January 6, 2021. That was when we almost lost our democratic system of government. On that day, not only was the United States Capitol stormed by violent protesters at the behest of a defeated president, but it was attacked from within by lawmakers who tried to carry out this president's orders and overturn a legitimate election. There is nothing in that statement to debate; this is very well documented from all sides.

To see police violently attacked by the very people who claimed to be their biggest supporters really put things into perspective. Apparently this "support" was contingent on their not being on opposite sides of an issue. Once that happened, law enforcement became the enemy and were even called traitors by those who had assumed police would help them overturn the election.

Fast forward to this summer when the now former president was accused of having stolen a bunch of top secret documents that could threaten the country's security, as well as put a number of individuals in harm's way. Once more, the entitlement kicked in with him and his cronies believing they somehow couldn't be touched by the law. But that's not how the system is supposed to work.

When the FBI did their job and conducted a search of the location where these documents were believed to be, *they* now became the enemy. Members of Congress were quoted saying things like "Defund the FBI" and even "We must destroy the FBI," referring to them as part of the "deep state," jackbooted thugs, Democratic operatives, you name it. Names and addresses of agents were made public. They were now targets.

We believe all of this illustrates a very basic fact. For all of the times we've found our community to be the victims of injustice at the hands of federal, state, or local authorities, we fought back through our words and whatever legal representation we could muster. We condemned actions that we found to be unfair and we called people out who were acting in a particularly dishonorable way. But we never advocated attacking, targeting, or causing any sort of harm to them as individuals, nor did we attempt to tear down the institutions they represented. We certainly called for change and for people to be held accountable for their actions. That's how the system *should* work.

The people who have been in the headlines recently don't have the same confidence in that system. When things don't go their way, they become violent in short order. It doesn't matter if what they are fighting against is the will of the people or a representative of law and order. It doesn't matter if it's a person they were friends with a few days ago. Once you cross whatever line they draw, *you* become the enemy. We've seen this happen repeatedly and it's both fascinating and frightening. But it's also empowering because it makes it so much clearer that all of us who have been standing up to injustice over the years - whether through the courts or in the streets - have been on the right side of history. We don't even have to agree with each other; it's the act of standing up for your beliefs and fighting back against the wrongs you perceive that qualifies as honorable. We all need to recognize that.

There are some tough times ahead. When this issue hits the stands, we will have just come through an election that will push us in one direction or another. We're either feeling inspired or dejected, or perhaps a combination of each. What we can't let go of is that feeling of healthy rebellion, constant questioning, and a willingness to take action. Only the truly desperate feel the need to tear everything down and collect enemies when they don't immediately get what they want. Their tantrums show their immaturity, along with their lack of belief in democratic systems that often require an abundance of patience and a lot of time.

We have a great deal to fight for and about. And we're not at all thrilled with how the system is designed and abused by those with power. But our dissatisfaction doesn't push us into despair. Instead, it serves as motivation for us to try harder and continue the battle for another day. It's easy to forget how these challenges are putting us in a better place. Sometimes it takes the actions of those who are on the wrong side to really make this clear.

A New HOPE: Release Notes

by Members of the Organizing Committee for A New HOPE

We would like to share some of the decisions we made when planning and implementing A New HOPE, and describe some of the outcomes and lessons learned. We offer this as a reflection on what worked well and what could have been better. We aspire for this article to be helpful to people organizing other conferences, and also as a guide to planning future HOPE events.

HOPE Conference Background and History

HOPE is Hackers On Planet Earth, a conference series sponsored by *2600 Magazine*. The first HOPE conference was in 1994, and they have happened more or less every two years since then.

Most HOPE conferences have been three-day events, featuring a very wide range of talks as well as lots of other content. Workshops, performances, villages, tutorials, and lots of unplanned hallway interaction all contributed to fun-filled and very informative conference programs.

Until 2022, all HOPE conferences but the second had taken place at the Hotel Pennsylvania, a large but dated hotel in the heart of midtown Manhattan. Unfortunately, Hotel Pennsylvania is now being demolished to make way for a new office skyscraper building.

HOPE in 2020 was an entirely virtual event, with a full range of talks and workshops, but with everything online. Most past events since around 2002 had three simultaneous talk tracks, but in 2020 there was only one talk at a time, along with one workshop and some late night performances. This conference lasted a full nine days. You can find out more about HOPE 2020 at `xiii.hope.net`.

After The Circle of HOPE in 2018, the Hotel Pennsylvania dramatically increased its prices. Because HOPE strives to be a relatively inexpensive event to attend, we started looking for other possible venues.

We put out a call to HOPE fans, looking for potential venues. We heard about quite a few, all around the U.S. and even in a few other countries. We followed up on many of these suggestions, and we also heard a strong preference for staying in New York City - it's a great destination, for many purposes.

Choosing a New Venue

In Spring 2019, we issued a Request for Proposals (RFP) to look for other venues around the New York metropolitan area. We got some great free support from the New York Convention and Visitors Bureau to identify candidate venues and distribute the RFP to potential respondents. We made sure to reach out to all the places that had been recommended that were within 50 miles or so of New York City.

The RFP generated some strong responses, and we ended up working with a couple of major Manhattan conference hotels to get an estimate of costs. We also heard from St. John's University, based in Queens, New York.

St. John's seemed like a good fit for us. It is an idyllic campus in a city neighborhood that is busy, but not nearly as built up as midtown. On-campus housing was available, and they had relationships with some nearby hotels that could offer discounted blocks of rooms. They had some pretty good spaces, including some large auditorium or theater-style rooms.

Working With Volunteers

One of the key benefits of St. John's was that there were no impediments to volunteer labor. All of the conference organizers are volunteers, and HOPE runs on volunteer power. Volunteers operate the info desk, the audio/visual production, setup and cleanup, and everything else.

We had learned at Hotel Pennsylvania that many hotels have labor unions for their staff, and there are requirements for using contractors that are part of labor unions. We are in favor of labor unions, and would love for the people working for pay at our events to be part of unions. However, the union restrictions at hotels make it difficult and expensive to use volunteers.

Hotel Pennsylvania was less restrictive, as only part of the hotel was unionized. We found out that the big Manhattan conference hotels are entirely unionized.

As a brief example, if we wanted to bring and set up our own audio/video equipment, we would need to pay union employees to set it up, plug it in, and operate it throughout the conference. If we wanted to have our own volunteers do that - or other activities like setting up tables and chairs, running a video camera, setting up our own lighting and sound, or even unloading a truck full of gear we had rented - we could only do this if our volunteers were augmented by "shadow" labor by union personnel, at their regular hourly rates.

These union policies followed by the big conference hotels were all fascinating to learn about, and ultimately meant that we could not have a conference in a major Manhattan

conference hotel without significantly increasing our costs, and also limiting our use of volunteer labor and donated equipment.

Pivoting in 2020

The lack of restrictions on using volunteer labor at St. John's was another benefit. We visited the campus and liked what we saw: This could work! In addition to being a suitable venue, St. John's has a strong cybersecurity program, and they seemed to see their interaction with HOPE as synergistic with what students learn in the program.

By late 2019, we had a contract with St. John's University for the 2020 event to begin in July. We did some planning and opened the Call for Participation by the end of 2019. We were on track for another great HOPE event!

And then, COVID-19 struck. By March 2020, it was looking increasingly unlikely we would be able to have HOPE in person. Lockdowns and other restrictions on gathering were happening everywhere, including New York City. Universities were sending staff home and shifting to all-virtual instruction. A vaccine against COVID-19 was, at the time, still just a theory.

We pivoted, and HOPE 2020 was instead held as an entirely online event.

Teleconference Choices in 2020

For 2020, we followed a similar process of program planning as for our past events: a Call for Participation soliciting proposals for talks, workshops, performances, and other content, and then an evaluation and selection process.

Delivery was entirely different, though. We had four main groups of challenges:

1. How would presenters give their presentations?
2. How would attendees view the presentations?
3. How would attendees interact with each other and with presenters?
4. What parts of HOPE would be free to anyone, and what parts would be restricted to those who purchased tickets?

For the first challenge, we tried all the mainstream technologies. We selected Zoom (`zoom.us`) for speakers, and Big Blue Button (`bigbluebutton.org`) for workshops.

The choice of Zoom was based on the capabilities of the client. We test-drove many of the available technologies, hoping to find free software that would perform well. Unfortunately, we found that the free software clients were sometimes challenging to install, and the teleconference experience was often glitchy (audio/video dropouts, poor performance with low bandwidth, or unreliable network connections).

Zoom "just worked," and in early 2020 "Zoom" was often being used synonymously with "teleconference." We decided we would have a live moderator who could interact with the speaker, and a live (remote) production crew using Open Broadcaster Software (`obsproject.com`) to mix the Zoom teleconference with a background, and also we used `otter.ai` to provide live automated transcripts.

Because we were nervous about teleconferencing problems, including situations where speakers had network outages or other issues that prevented them joining the live conference, we encouraged speakers to pre-record a talk of approximately 30-40 minutes and upload it in advance. Most speakers did pre-record, and that resulted in some really fascinating and well-produced talks.

The HOPE conference emcee introduced the live speaker, then we played back the pre-recorded talk, and the speaker took questions afterwards from the emcee via Matrix (`matrix.org`).

Attendees didn't use Zoom. Instead, they watched the livestream. The livestreams for talks and performances were broadcast by our partners at The Internet Society (ISOC) to `livestream.com` (Vimeo) on the ISOC channels, as well as to YouTube and Twitch. Archiving to The Internet Archive happened right after each talk.

You can find all of these talks online on YouTube at `www.youtube.com/user/channel2600`.

For workshops, we decided to use Big Blue Button. This is great free software. Even though the client isn't as reliable as Zoom, it has tremendous features for instruction. With BBB, it's easy to have breakout sessions, to have attendee-to-attendee interaction, and to have moderation as needed.

The workshop presenters in BBB were supported by a live volunteer who assisted with setting up the BBB environment and provided additional support throughout the workshop.

Most workshops were recorded, but they did not get the same level of live production via OBS that talks did. You can find 22 workshop recordings on YouTube in Channel2600.

For attendee interaction, we chose Matrix. Matrix is an open standard and communication protocol for chat and other real-time communication. We ran our own Matrix home servers and, since it's a federated system, people could join if they already had an account on another home server.

We collaborated with the folks at `element.io` on solving a couple of issues. Talented HOPE volunteers set up our servers and created a bot that would let people into the Matrix chat

forums for HOPE 2020 when they provided their ticket code.

All of our challenges were met! People with tickets could get into the Matrix chat forums and interact with presenters and each other. The general public could watch the livestreams in a few different ways. We had volunteers doing live production, and ended up with very few technical glitches or quality issues with the speakers, workshops, and performances.

All of this experience served us well when we started planning for HOPE in 2022.

Planning for A New HOPE

By late 2021, it was beginning to look like a live event in 2022 was going to be viable. A vaccine had been developed and, since the start of the pandemic in early 2020, a variety of approaches to having relatively safe public events had been proven.

We set up a new contract with St. John's, launched a new Call for Participation, and started getting ready for the summer. We decided to call this event A New HOPE. This name was chosen to recognize and celebrate how science had brought us understanding and protection from the virus, and that so many of us had learned how to better care for each other by following the best current health guidance, like physical distancing and wearing masks.

The name A New HOPE also recognized the tremendous losses of life, health, and opportunity that had happened during the pandemic. In case you are wondering: We never heard from Disney with complaints about how our name is similar to a certain well-known science fiction movie franchise. The name A New HOPE is not "confusingly similar" to their trademark.

By the spring, we decided that A New HOPE would require all attendees to be fully vaccinated. We also decided that (unless the situation changed) we would require people to wear masks in all indoor spaces, except while on stage or eating and drinking. If you are a regular reader of *2600 Magazine*, or a listener to the *Off The Hook* radio show, you already know that *2600* values following the best current scientific and health guidance on how to protect ourselves and each other from COVID-19.

A vaccination and mask policy for A New HOPE made a lot of sense, and we got a lot of positive feedback from attendees about this. We also got some negative response, and almost none of the people who responded negatively ended up buying a ticket.

Building Community

During our virtual event in 2020, we found there was a lot of pent up desire among hackers to be able to interact with each other again, and to have a conference that touched on all the hacker themes that HOPE is known for.

Leading up to 2022, it became clear there was a lot of enthusiasm and anticipation for actually getting together again. So many of us had felt isolated during the pandemic, and teleconferencing and other online contact are not enough.

During the opening and closing ceremony sessions at St. John's, speakers emphasized that we were all there because we wanted to be part of the HOPE hacker community. Attendees had made the decision to show up in person because this was going to be a richer experience than watching a video and interacting by chat.

More importantly, the opening ceremony put out the expectation that we were going to be conscientious and caring for one another. Conference organizers knew that many attendees were nervous about being at a large in person event, due to the lingering presence of COVID-19 and also due to being somewhat out of practice at live face to face interaction. St. John's was a new venue and not as centrally located as Hotel Pennsylvania. We'd all need to allow each other, and ourselves, a little slack in our interaction.

Being Excellent to One Another

Another part of what was expected of attendees was increased awareness of the goal of "being excellent to one another." This is the core tenet of the HOPE Code of Conduct. There were some real failures in how some CoC and security-related issues were handled by HOPE in 2018, and we worked hard to design a more effective multi-layered approach for 2022.

One great benefit to A New HOPE was our partnership with Operation Hammond. This is a group of volunteers who provide support to attendees with issues related to Code of Conduct, mental health, first aid, or other concerns. Hammond dovetailed with the HOPE security team, whose volunteers were mostly responsible for physical security and the conference perimeter. St. John's also had campus safety personnel on-site, to facilitate emergency response as well as to interact with other campus personnel.

Internally to the organizers, security team, and Operation Hammond, we had developed an escalation pathway for different types of issues we might encounter. We communicated this to volunteers during a pre-HOPE volunteer teleconference and gave a summary during the opening ceremony. We did end up encountering a few issues during A New HOPE, and our plans worked out well. We can only credit planning partially, though; we also credit that the vast majority of attendees were polite, patient, supportive, conscientious, and self-aware.

The sense of community, which developed

before and strengthened during A New HOPE, was wonderful to be a part of. In post-conference feedback messages, many attendees expressed gratitude for being part of it. We are optimistic that the same sort of community feelings and mutual respect will be able to continue at future events.

Technology Choices

Building on our experiences in 2020, we decided to use Zoom for our handful of remote speakers. Most speakers, all performances, and almost all workshops were in person at St. John's.

In the month leading up to A New HOPE, we ran into issues with our technology planning and rentals. Lots had changed since our previous in person event in 2018 and, among other things, the prices for our audio/video rentals had skyrocketed. To make a long story short, we made a last-minute change to work with an organization called Sonus (via an introduction from another hacker conference) that would run the livestream. They did a great job.

The livestream was important for virtual ticket holders, as well as attendees who could not attend in person due to COVID-19 and other challenges. It was also a great way of watching talks and other content from hotels or from simulcast rooms we set up at St. John's.

Perhaps more importantly, at least for posterity, the livestream was also recorded and archived to Channel2600 on YouTube. Videos are also available for free download elsewhere, and you can buy a copy of all recordings online at the *2600* Store (`store.2600.com`).

Because of the last-minute changes, we only ended up sending the livestream to YouTube (plus we sent part of the first day to Facebook, but almost nobody was using this and we didn't get it running again).

The overall on-site experience at A New HOPE was comparable to recent HOPE events at Hotel Pennsylvania. Volunteers built out wonderful spaces for talks and performances, with theatrical lighting and sound for two main speaker tracks. A third track in a smaller room had a less sophisticated A/V buildout, but still had a high quality livestream.

Workshops happened in classrooms in our main St. John's building, using in-room projectors. We had some rooms set up for classroom-style workshops, and others with tables suitable for things like soldering or other hands-on activity. Workshops were not recorded or livestreamed, but one of the workshop presenters got COVID-19 just before A New HOPE and made remote presentations.

We used the same Matrix chat as in 2020, and the same bot and ticket system to allow ticketed attendees access to the conference-specific chat forums. Live on-site emcees would monitor the Matrix chat, as well as the speaker room, for audience questions. There was a Mozilla Hubs virtual environment, too, where people could watch the talks and interact with each other.

The infodesk volunteers also monitored Matrix chat, so they could give great help to any attendee, whether they were on-site or not.

Copyright Strike

In 2020, we made detailed plans to avoid all types of outages and problems. We had multiple livestream providers. We had backup volunteers. We added DDoS protection to our conference website and other systems. In 2022, the intense planning for the conference, with a primary focus on being in person, led us to forget some of that caution.

Due to the last-minute change in our plans for the livestream and recording, we had set up streams to YouTube only.

During our 8 pm Saturday slot, a fantastic presentation was happening, called "Hacker Representation Through the Years: A Guided Tour of Hacker Appearances in TV and Cinema." As you might expect, this talk included brief clips from media.

In the midst of this talk, our YouTube stream was taken down by Google, in what they call a copyright "strike." This is when an algorithm decides that your content is violating someone else's copyright or another of the YouTube terms of service.

Figure 1 shows what people watching the livesteam saw.

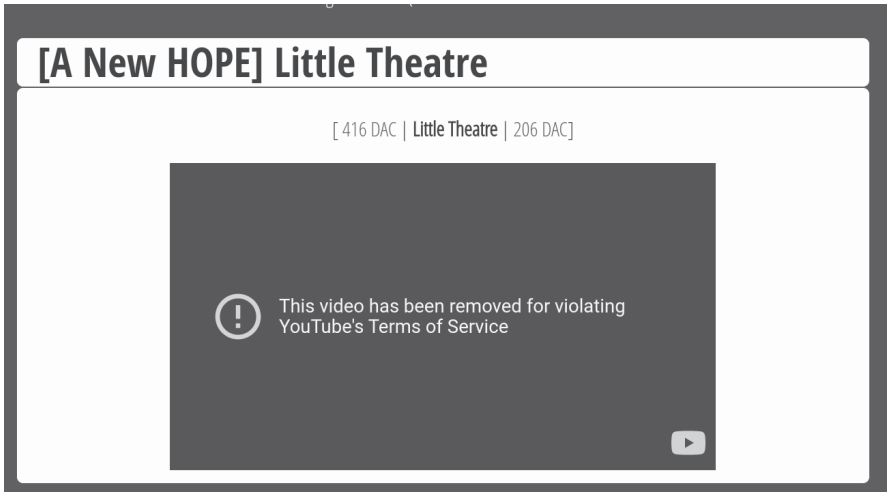


Figure 1: YouTube's notice of video removal

Ironically, we discovered the strike was

specifically due to a short clip from the *Mr. Robot* series. This is a fictional series about hacking, which many people think is quite accurate about hacker activity and culture.

Panic ensued. A second copyright strike would mean that all the Channel2600 livestreams would be removed for a week. There was essentially no pathway to a mitigation or review, and Google's algorithm has no notion of fair use.

The "fair use doctrine" is a crucial part of U.S. copyright. It means that copyrighted content may be utilized, without requiring permission, for certain purposes. Some of these purposes include brief extracts, scholarly use, and satire. At 8 pm on a Saturday in July, there was no opportunity to make a case for fair use, and nobody at Google who we could find to listen.

Luckily, the Channel2600 maintainers were eventually able to identify procedures to get the livestreams restored. People watching the livestream missed much of the talk, but we were making an on-site recording.

The next part of the YouTube saga was a couple of weeks later. *2600* staff had worked tirelessly to convert the on-site recordings into 85 separate videos for distribution by YouTube, through *2600* store sales of USB drives, and other means.

When the "Hacker Representation" talk was uploaded, though, it was immediately and automatically blocked by YouTube. The other videos were available, but not this one, and the playlist with all videos was broken. As with the livestream, this happened algorithmically - there was no pathway to discuss fair use with anyone at Google.

2600 puzzled over this for awhile. We discovered that the video was online, but not findable in the U.S. YouTube. It was findable in the U.K. and Germany, because evidently the automated copyright complaint by the owners of *Mr. Robot* was only directed at the U.S. instance of YouTube.

Eventually, it turned out that there was an automated appeal process where Channel2600 could contest the automated takedown. This finally got the video available again on the YouTube playlist for A New HOPE when NBC Universal (the owners of the copyright) granted permission.

You can watch the video here: www.➥youtube.com/watch?v=M_➥JA9m7vprg

You can hear more discussion about this series of algorithm-driven events in recordings of the *Off The Hook* radio show from August 2022, online at www.2600.com/offthehook.

Some of the Lessons Learned

A New HOPE was a wonderful experience for the conference organizers, and many volunteers and attendees expressed their appreciation for a smooth event.

Post-conference feedback yielded a list of items of concern for the new venue at St. John's. While most attendees liked the campus setting, some found it to be too isolated - hotels were not close enough (and the discounted hotel rooms were sold out), we didn't provide enough information about nearby food options, and there wasn't as much nightlife in the area as would be found in midtown Manhattan. And because St. John's is a dry campus, attendees wishing to party needed to do it elsewhere (like the bar at the conference hotel). But this also had its advantages as we had zero late night drunken incidents at the event while continuing to operate around the clock.

The space at St. John's was quite nice. The classrooms worked really well for workshops and other things, like our live simulcast of the Dutch hacker camp happening the same weekend, May Contain Hackers. But it was tough going from one air conditioned building to another, through the heat wave that hit the area that weekend. Those with mobility issues found the campus had not made provisions with HOPE for parking close to the buildings, or shuttles between the buildings.

The dorms, which were used by around a quarter of attendees, meant another walk through the heat. St. John's dorm rooms were a great convenience - nearby and reasonably well appointed (though not as fancy as a hotel). But they charged by the person, which made it expensive compared to a hotel that could house two plus people. Also, St. John's offered no accommodations for family housing or for having multiple genders in a suite of rooms. St. John's only recognizes two genders, male and female, and required a lot of personal information to register to stay in the dorms.

All that said, we found St. John's to be a wonderful host. We had outstanding support from the campus information technology group, which operates the network and all the classroom technology. All the groups took great care of HOPE and its attendees, including conference services, facilities, performing arts, housing, custodial, and food service.

Attendees reported a very positive overall experience in talks and workshops, as well as for performances, villages, an unscheduled "fourth track" (open microphone), and other content. There was good variety, including the usual mix of highly technical talks, and those with a more social or humanistic nature - not

that different than prior HOPE events, and also not that different from the mixture of articles in *2600 Magazine*.

The experience for virtual attendees could be improved. It's tough to run a hybrid event (online and in person) when many key volunteers are already stretched thinly, and a successful virtual experience really needs a dedicated crew. For A New HOPE, the Mozilla Hubs environment was really cool, but could have been better utilized. The Matrix chat worked well, but there was not really an area for virtual and in person attendees to socialize with each other and feel more like part of the community.

There were around a dozen vendors who attended, to present their wares and have interesting discussions with attendees. There was a very nice lounge space for vendors, as well as a coffee house with Starbucks and a snack concession in the afternoons. This was also a good space to socialize.

Registration and badge pickup went very smoothly, with almost no wait. Everyone needed to present their proof of vaccination at the door, then get a wristband to pick up their badge using their ticket code. This was the same code that gave access to the online Matrix chat. There were almost no issues with proof of vaccination or with masking. Everyone needed to buy their ticket in advance - there were no sales at the door - and we sent out some advance emails so attendees knew what to expect.

We learned a whole lot about technological planning and resiliency. Firstly, we need to work harder to avoid last minute changes.

In the future, we will try to take a more professional-style project management approach to conference planning. For example, if we had used a tracking system for who-does-what, with target due dates and regular reviews of items, we would have greater visibility on things that were falling behind or creating risk.

An "agile" approach (in the sense of software development project management) would ensure that we're not going to be rigid. After all, we're a bunch of hackers, and also a bunch of volunteers; creativity and flexibility is our thing! But that doesn't prevent us from upping our game for planning, and having a mutual understanding of accountability with each other to come through on our commitments.

We definitely will revisit our use of Zoom for future teleconferencing needs. Free software packages like Jitsi and Big Blue Button have a lot of strengths and are improving over time. We can also expect that presenters of the future will be more experienced, sophisticated, and self-sufficient in the use of teleconferencing than they were in 2020.

Resiliency for streaming and our overall online presence will be a big focus for any future event. Luckily, this is not hard to do - it was an oversight in 2022 that we didn't have multiple streaming destinations. We would love to work with our friends at ISOC again.

We used Pretalx software for our online schedule. This is free software used by our friends at Chaos Computer Congress. In the future, we are considering adding an online web-based submissions and review process to supplement our existing email-based process. The expert reviewers and organizers for talks, performances, and workshops do a great job, but might benefit from a more modern online system.

Perhaps the best lesson learned, or re-learned, is how wonderful HOPE attendees are. The event in 2022 was friendly, filled with engaged and caring people. Presenters gave generously of their time and knowledge. The info desk, registration desk, network team, A/V team, Sonus, Operation Hammond, security team, *2600* store, emcees, media team, website team, and many many other volunteers made everything work, and helped to foster the sense of community that was so refreshing.

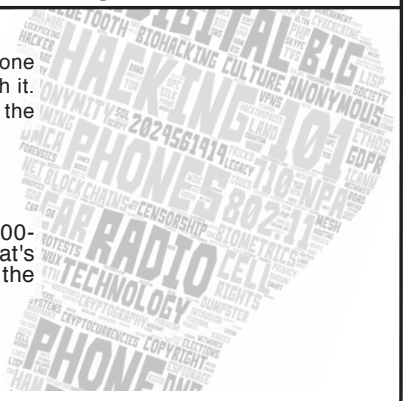
HOPE always welcomes input, as well as new volunteers. Keep an eye on `www.hope.net` as we work towards the next event in 2024. Feedback is welcome, by email to `feedback@hope.net` or in the letters department of *2600 Magazine*.

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.

The Internet of Problems

by RG

Recently I received a new LTE router in hopes of boosting Internet speed at home. If you aren't familiar with LTE routers, they are effectively a combination between a traditional home router and a cellular hotspot device. The Internet is provided via cellular towers and then served to end users as an ethernet or Wi-Fi connection. These devices have become more common for users in industries such as construction and for rural Americans who don't have access to many Internet service options.

Curious as always, I wondered if the device had any obvious security flaws. Many home routers are not secure by default and require additional configuration to minimize vulnerabilities. To work, the device utilizes a SIM card and is given a public IP on the carrier network. This is standard for cellular devices. However, the device also served up a configuration interface over port 80 on its public IP address by default. To make matters worse, the default username and password combination for the device was "admin:admin".

According to a survey by Broadband Genie, only 14 percent of the 2,205 survey respondents have updated their router's firmware and only 18 percent have changed the device's default admin account password. This survey was taken in 2018 and has since been widely referenced. While the education provided to many users working from home during the COVID-19 pandemic may have lowered these numbers, it is likely that many routers are still vulnerable. For instance, the previously mentioned survey also cited many users being confused by their router settings. Anecdotally, I've known plenty of people who are unable to distinguish the difference between their wireless password and the administrative console password.

Knowing that this device was by default unsecured, open to the web, and came with no documentation, I wanted to see how many similar devices were out on the open Internet. To do this, I first went to `shodan.io` and logged into my account. There are several options for web scanning, but Shodan is my preferred tool. I then performed the following steps:

1. Since I already knew my IP, I simply searched for it. This returned useful information about my device. Specifically, it grabbed the http banner and then hashed it. Additional information on pivoting with property hashes can be found here: `help.shodan.io/mastery/➥property-hashes`.

2. I took the banner hash for my device and searched for it. This search returned all devices similar to mine. In total there were 31 devices. Based on our numbers from before, we can assume potentially 25 of these devices are accessible with default credentials.

3. 31 seemed low for the number of LTE routers on the open Internet, so I tried a few different scans. One particular scan for "Server: GoAhead-Webs port:80 country:"US"" returned roughly 30,000 results. GoAhead-Webs is a simple web server used for devices without much memory and appears to be heavily used by lightweight LTE routers.

What can be done with this type of access? Look no further than Duran's article in Volume 38, Issue Number 4 of *2600* where they describe methods for finding and manipulating routers. It would be easy to lock users out of their devices, potentially upload tainted firmware, or even in some cases gain direct access to their network. This is not an invitation or encouragement to break the law, of course, rather the intent is to show the severity of the situation.

As previously discussed, many users do not understand how to properly configure their devices and manufacturers often do not provide sufficient security documentation. This combination of unsecured by default devices and no documentation puts the onus of security on the end user. In this case, manufacturers are passing off the cost of security. Currently, it's difficult to know which manufacturers are providing a better product when it comes to secure devices. Due to this lack of visibility, companies often are not incentivized to take this cost on as they see no competitive advantage in doing so. This is a major problem plaguing IoT devices. I've asked questions about this issue in a few webinars with security professionals and additionally have done research on the policy angle. The consensus seems to be something along the lines of an energy star rating equivalent for IoT devices. *Executive Order 14028*, "Improving the Nation's Cybersecurity," has required NIST to create a pilot program to do just this. NIST is currently in the process of defining the criteria of this program. While this may or may not be the best long-term solution, it's important that this topic is discussed and that the problem is continuously worked.

- *Survey Source:* `www.bleepingcomputer.➥com/news/security/survey-➥reveals-users-have-no-clue-➥about-router-security/`
- NIST IoT Labeling: `www.nist.gov/➥itl/executive-order-improving-➥nations-cybersecurity/➥cybersecurity-labeling-➥consumers-internet-things`

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It was a surprisingly calm summer here in the Great Northwest. We had cool temperatures and rain later into the summer than usual (I was beginning to call it "Juneuary") and this seems to have moderated the fires that engulf our region every year. Now that the summer is over, I'm glad I am not writing this year about fires engulfing our outside plant and *literally* burning up your phone line (although this is a continued high risk). Instead, let's rewind to the 1990s, and services that used to *metaphorically* burn up the phone lines of the Central Office: pay-per-call services.

"Now wait a minute," you might ask. "Weren't *all* calls in the 1990s pay-per-call?" Well, yes, you had to pay for a lot of calls in the 1990s (even local calls in some areas), but "pay-per-call" service was a special billing category. With a pay-per-call service, an information provider (such as a celebrity horoscope, dating service, lucky lottery number of the day, or whatever anyone could dream up to create) could *share in the revenue* from your call. This, at one point, led to a $3 billion industry that younger people today have never interacted with and probably don't even know existed.

Pay-per-call services were either regional or national. Here in the Pacific Northwest, US West first offered local pay-per-call numbers in the 976 exchange (NYNEX, the provider serving *2600*, offered similar services in the 540 exchange). This exchange was programmed to be an intra-LATA long distance call from everywhere, with special rates. This meant that if you wanted to call a 976 number, you'd have to dial 1 first. When you called one of these numbers (such as 1-976-6969, known as the "moan line," an interactive adult "service"), you'd be charged a higher rate than a regular long distance call. The rate was set by the provider and, naturally, it wasn't announced, and you didn't have to agree to the charges before you were billed (after all, you had dialed 1 first, so you knew there would be charges, right?). Unfortunately these services cost much more than a regular long distance call: up to $9.99 per minute!

The ~~ill-gotten gains~~ revenue would be split between US West and the service provider (in most cases via an intermediary called a "service bureau" who provided a voice platform and technology services at a fee, and who managed interconnection and billing with US West). Everyone was happy except for the parents of teenage boys, who would call the "moan line" and giggle until an eye-popping phone bill showed up in the mail (US West would be happy to negotiate a 50 percent discount with the bill-shocked parents, but they'd never write off the bill entirely). Back then, it wasn't unusual for teenagers to be grounded from the family phone, and groundings resulting from 976 calls were a very common occurrence at my high school!

In 1987, AT&T began testing a nationwide pay-per-call service in the 900 NPA. This was essentially the same idea as 976 numbers in the US West service territory, except that the service would work all over the country. Of course, long distance and service charges would go to AT&T as well, rather than to the "baby Bell" local exchange carriers it now competed with. The concept quickly took off, with everything from dial-a-psychic to sports talk services. (The "moan line" was conspicuously missing; AT&T and MCI, who later began offering "900" services, both banned adult content - initially in both theory and practice.) Keep in mind, this was before the days of the Internet, so most people only had access to information that was in the newspaper. Pay-per-call services allowed service providers to create both

broadcast-style and interactive services catering to niche interests. These valuable services were popular and millions of satisfied customers were happy to pay the charges. At least, this is the argument that service providers and the phone companies used when arguing with the FCC and Congress that they should be allowed to continue in the business.

Satisfied phreaks were certainly happy for someone else to pay their 900 number charges, and pay-per-call services were a favorite termination point from compromised DISA ports and beige boxes. Some of these services allowed setting up conference calls, allowing ten or more phreaks - all standing at different payphones - to talk for hours on someone else's $9.99 per minute dime. For extra phun, making a three-way fraudulent call to the "moan line" was always a good laugh for everyone on the purloined conference call.

By 1991, the pay-per-call industry was raking in close to $3 billion per year, and it peaked at *over* $3 billion in 1992. You could barely turn on a television without seeing an ad for a 900 number. However, billing complaints were truly getting out of hand, and pay-per-call services had become the Number One source of consumer complaints to the FCC. In response, Senator Daniel Inouye of Hawaii introduced Senate Bill 1579, which eventually passed in 1992 and introduced significant constraints on the pay-per-call industry. While there was a lot in the bill (which is linked below), it provided the following key consumer rights:

- No more deceptive advertising of rates and terms was allowed (so no mumbling the prices at chipmunk speed under blaring music).
- Rates were required to be clearly announced when the call was answered, and the caller would have an opportunity to hang up before being charged.
- New restrictions on advertising to children were introduced.
- Carriers were required to block pay-per-call numbers upon request of the subscriber, only a nominal one-time fee could be charged, and no fee was allowed when blocking was requested within the first 60 days of establishing service.
- Dispute resolution procedures were required.

There were also some unrelated provisions in the bill, including an infamous provision that made it illegal to listen to analog cellular calls, or to sell radio scanners capable of monitoring these frequencies. Privacy concerns had become an increasing issue with cellular customers, so pretending that certain radio frequencies didn't exist was the solution prescribed by Congress. To this, OKI 900 said "Good Timing."

In the bill, Congress directed the FCC to do most of the heavy lifting in creating and enforcing the rules. The FCC addressed this with gusto, given that, as mentioned, pay-per-call billing disputes were their Number One complaint. While it's true that the rules they issued could perhaps be described as a telecommunications embodiment of Thor's hammer, they were probably not responsible for the rapid decline of pay-per-call services. 1993 was right around the time that dial-up Internet service started to gain early popularity, and much of the information previously only available on pay-per-call services was *freely* available online, on services such as AOL. By 1995, dial-up Internet capability was included in Windows 95, and Internet usage exploded. Pay-per-call service revenue dropped precipitously in line with the rise of Internet popularity overall and, by 2013, Verizon (the last remaining "900" service provider) finally ended service.

And with that, I'll see you again in the winter. Drive safely this fall, and if you are looking for Halloween costume ideas, consider dressing up as an AT&T bill for 900-number calls!

References

www.csmonitor.com/1991/1030/30091.➥html - "Pay-Per-Call Services Ringing Up Lots of Flak"

www.congress.gov/bill/102nd-➥congress/senate-bill/1579 - Senate bill constraining pay-per-call billing practices

www.deseret.com/1991/7/17/18931201/➥complaints-about-900-service-➥skyrocketing-senate-panel-told - "Complaints About '900' Service Skyrocketing, Senate Panel Told

Keeping America Informed: An Introduction to Government Documents

by Infra Read

The motto of the U.S. Government Publishing Office (GPO) is "America Informed," and for us to be informed, it helps to know what our elected officials and other people with power are saying and doing. Much of this is made purposely obscure, but a massive amount of government documents is out there, and they can be a way to find out in more detail what our government is up to.

The GPO makes reports and publications of all kinds available to the public, including transcripts of hearings from the House, Senate, and government committees on every subject. The Federal Depository Library Program (FDLP) sends free copies of physically published documents to participating libraries, who are legally required to give the general public access to the documents.

That means that a local university may restrict most of their services to their tuition-paying students, but if they are part of the FDLP, they need to provide general access to their government documents. This should include physical ones on their shelves, and electronic documents that are accessed through their online card catalogs. If they don't allow physical check-out, they have to let people access them on-site, and if computer access is generally restricted, they have to provide some way, like temporary passwords, for anyone off the street to access the documents from a terminal in the building. A map of libraries in the FDLP is at: ask.gpo.➥gov/s/FDLD. The libraries listed as "Regional" receive and keep basically all documents that are published through the program; the "Selective" ones only receive selected documents, and they are allowed to remove older ones from their collections.

Fortunately, the majority of new government documents are available in electronic form, and anyone with Internet access can view them for free. The main Catalog of U.S. Government Publications (CGP) is found at: catalog.gpo.gov/. This is a pretty straightforward search engine, although keywords with too many hits can sometimes cause an error.

To find the most recent documents, you can search using the "Electronic Titles" link under the "Catalogs to Search" banner at the CGP home page. This brings up a search field for electronic documents only, and a link for "New Electronic Titles," monthly lists of the recently released titles. This will include older records that have been digitized and added to the listings. The backlog of documents, from before digitization was the norm, is continually being worked on. For example, the July 2022 list contains a series of technical reports from the 1940s' National Advisory Committee for Aeronautics, a report on welding techniques from 1963, and space shuttle structural analyses from 1989.

Between transcribing, digitizing, and releasing the documents in a finished form, there can be time lags, so sometimes even a document with a publication date of 2022 can be for a meeting from 2017. A lot of it is fairly current, though, and hearings on big, newsworthy subjects, such as the impeachment hearings for Donald Trump or the January 6th riots, will usually get printed and distributed fairly quickly.

All these searches should bring up electronic resources with purls (permanent URLs), and unlike many library systems, the search logic is fuzzy enough to bring up related subjects. For example, a search for the term "cyberpunk" doesn't have any hits, but it does bring up similar terms; for example, "cyberprotests" (which were considered a "threat to the U.S. information infrastructure" in a 2001 report from the National Infrastructure Protection Center (purl.fdlp.➥gov/GPO/LPS15585).

In the results list for "cybersecurity," there's also more recent information, like the hearing on the "Cybersecurity State Coordinator Act of 2020 report... to establish a Cybersecurity State Coordinator in each state, and for other purposes," from June 2020.

Some of these documents are very dense and legalistic, clearly not designed to be read by the general public, but others, like the Congressional hearings, are often more readable, even interesting, since they include direct transcripts of everything spoken, and even note when there's laughter during a hearing.

A related resource of interest is the Congressional Research Service at crsreports.congress.➥gov/. They have some interesting things like the "Overview of Governmental Action Under the Stored Communications Act (SCA)," which "governs access to stored wire and electronic communications such as emails and other online messages held by service provider," currently being looked at for its relationship to private messages via social media.

One particularly interesting government entity was the Cyberspace Solarium Commission, a cybersecurity taskforce whose documents are available at www.solarium.gov/. This was a working group that produced white papers, a cybersecurity briefing for President Biden, and

a 182-page final report of proposals from 2020, including "Reshape the Cyber Ecosystem" and "Preserve and Employ the Military Instrument of National Power."

Much of the specific work on cybersecurity is done under the umbrella of the Cybersecurity and Infrastructure Security Agency (www.cisa.gov/), an agency under DHS oversight that contains multiple specialized divisions, including the National Security Telecommunications Advisory Committee. Many of their hearings and documents are available through a CGP search. The Department of Defense maintains a separate U.S. Cyber Command, but much of their documentation is available only through Freedom of Information Act requests, not through the GPO.

All the material produced by the GPO technically belongs to the American people at large and is legally required to be made available to them. This is a little-known resource, but while some of it takes work to weed through, it's full of information.

- Main GPO page: www.gpo.gov/
- Main FDLP page: www.fdlp.gov/
- List of government entities and their types of publication available through the FDLP: www.fdlp.gov/sites/default/➥files/listofclasses.pdf

Windows Installers

by street

Windows files with the MSI extension are used to install software packages. They do this by extracting themselves to the file system and modifying the Windows registry. They are special files used by the Windows operating system. Normally we take these files for granted, and trust the source that they come from.

MSI installation packages can be built with several tools. WiX and Visual Studio Community Edition are both available free and can build MSI packages.

The gold standard for building MSI packages has always been InstallShield. While InstallShield offers a free demo, the price of the commercial license was more than I could afford. But that didn't stop me!

Revenera is the company that owns InstallShield, and they also provide training courses for their product. It wasn't necessary for me to take the courses, because they already have free documentation online (docs.revenera.➥com/?product=InstallShield).

Using InstallShield to create an MSI file is very simple. You can add files and folders from your computer into the project, and then tell InstallShield where you want it to install them on the target machine. It can even add shortcuts to the start menu and desktop, or modify the registry. It's not hard to make your own forms, or change the default ones. The dialogs are customizable, and you can add your own graphics.

If you open the dialogs from the InstallShield menu, you can click on the dialogs text and graphics and quickly change them. You can also change a dialog's button and modify its destination to another dialog that you want the button to lead to.

As a hacker, I'm interested in what MSI packages aren't intended to do. I can use an MSI file to bundle legitimate software along with malicious code. I can even take a legitimate MSI file and reverse its installation by preserving the file structure and registry entries of the original installation. Add a simple reverse shell or whatever additional software you want. Then add a registry entry to Windows, telling it to run the new program at startup.

Microsoft provides a free tool called Process Monitor (docs.microsoft.com/en-us/➥sysinternals/downloads/procmon). This tool lists all the changes to the Windows file system and registry. It becomes a simple matter after that to build the delivery system for a trojan horse program.

Any kind of malware could work as a payload, and there is no need to change the flow of the original program or understand low level code. The only change is in how the software is installed.

Most companies will sign their programs with digital signatures to prevent the code from being modified. To do this they will buy a code signing certificate, which uses public/private keys to verify the program's integrity. However, creating a new Windows Installer does not actually modify the program.

The option to stop uncertified programs from running completely is something Microsoft has been playing with. They have been moving forward with new security changes in Windows 11 to only run apps verified in the Microsoft Store. This can prevent you from running perfectly safe software, or software that is even more secure than what is being offered in the Windows Store.

Microsoft has built a new installer format called MSIX. The MSIX format requires you to register the installer with Microsoft. They have not however stopped us from using the old MSI format.

Hack Your Brain

by Pavel Aubuchon-Mendoza

In the 1995 film *Johnny Mnemonic*, we see Keanu Reeves dive into a simulated representation of his brain and remove malware that had been slowly killing him. What a gift to have direct access to your brain with the ability to make changes for the good. Well, it turns out you can - no cybernetic dolphin required.

Your thoughts and emotions are not an abstract construct that emerges from your brain. Every thought has direct physical representation in your brain in the form of electrical and chemical interactions. If we had the technology, we could watch the electrical interplay of neurons that represent the words you are reading right now. Your thoughts literally are the physical interactions of your brain, and by changing our thoughts we can change the physical structure of our brain via the miracle of neuroplasticity.

In this article, we will draw an analogy between your brain and a computer system, and then absolutely beat that analogy to death. Please keep in mind that I am not a mental health professional (more of a hobbyist) and nothing I say should be considered medical advice. Talk to your doctor.

End Bad Processes

Over time, your brain inevitably has some bad inputs. You've got some recursive processes that just keep cycling back around and eating up resources. This can leave little remaining for the productive programs that you want to use. You can end the bad processes and assign a higher priority to the ones you want to enjoy. Learn to identify the negative thoughts before they spiral out of control, and stop them in their tracks. Know the things you want to enjoy, and revel in them. Let the enjoyment of small everyday things sink in. Your baseline emotional state can be generally positive, but sometimes it requires work. Reference *Rewire Your Anxious Brain: How to Use the Neuroscience of Fear to End Anxiety, Panic, and Worry* (Pittman/Karle) and *Hardwiring Happiness: The New Brain Science of Contentment, Calm, and Confidence* (Hanson) for specific instructions on how to do this.

Defragment Your Hard Drive

Okay kids, listen up. Back in the day, we had to defragment our hard drives to keep them running efficiently. Computers, much like our brains, don't always do a good job of storing information in real time. Events (particularly trauma) need time to get processed and filed away correctly. You know how sometimes you go to bed and you start thinking about everything you did that day? That's your brain starting this work. However, most of this happens while you sleep. If you're not getting seven to eight hours of sleep a night, your brain is not getting enough time to put everything away where it needs to go. The effects of not doing this are cumulative. Prioritize your sleep. If meditation is your thing, that achieves some of the same goals, but cannot replace sleep.

Invest in a Good Antivirus

Malware inevitably ends up on an unprotected system. It is simply the result of existing in the world. Sometimes they are insidious and indistinguishable from normal processes. In the worst case, they can give outside actors access to your core system. Fixing this is not something you can do on your own. Therapy is the antivirus for the brain. These are trained professionals who can identify and root out the malware that is disturbing your system. Therapy does not mean you are not strong and capable. Asking for help is an act of courage and should be commended. Check out the "find a therapist" option on `psychologytoday.com` to get started. It can be overwhelming to begin this process if you are already suffering, so enlist a friend to help if needed.

Install More Memory

Many people, myself included, take Selective Serotonin Reuptake Inhibitors (SSRIs) or similar medications that increase the amount of the "happy" chemicals circulating in your brain. These are often the

first line drugs used by physicians to treat depression and anxiety. In my experience, these give you extra resources to deal with the challenges life brings. They may not necessarily fix the problem, but they do make the machine run better - which is sometimes all that you need to start the repair work. If you do not have a primary care doctor, these services are available online. Cerebral is a popular choice.

Reboot In Safe Mode

This is an advanced topic, and should only be undertaken with medical supervision. You can obtain direct access to your core OS by use of psychedelics. There is so much exciting research coming out about the use of psychedelics to treat and, in some cases, completely cure treatment-resistant anxiety, depression, PTSD, and others. As of this writing, psilocybin is a Schedule 1 drug in the U.S. - the same category as heroin. However, starting in 2023 therapeutic psilocybin will be legal in the state of Oregon. The cost and availability to the average consumer remains to be seen. Ketamine is another popular agent, and can be obtained for mental health purposes with a doctor's prescription in some states. Mindbloom and WithPeak are popular online options. Savvy readers are probably thinking that they could obtain these substances on their own. I can guarantee that catching a felony drug charge will not be beneficial to your well being. These are potent substances and should not be taken without supervision.

Conclusion

This is truly the tip of the iceberg. There are many other options and strategies, and I encourage you to seek out professional help if you need it. We need every single hacker, weirdo, and deviant we can get right now to help make this world a better place. Take care, and be excellent to each other.

HACKER DILEMMAS

by aestetix

To remain a hacker in today's polarized world is increasingly difficult and leads to serious philosophical dilemmas. We are not talking about politics, but attitudes towards technology. To illustrate this, we will review a few of these dilemmas: old versus new, sharing of modified code, and ownership of networked systems.

In the "old versus new" debate, we see novelty battling nostalgia. Every new gadget that comes out offers - at least in theory - cool features with which techies want to play. But once the glow of newness dies away, we are left with a blunt question: what makes this device better than the old one? At a certain point, there is a law of diminishing returns. For example, while 4K video resolution is clearly an enhanced experience over 720p, does 8K offer the same improvement over 4K? And, conversely, how many times has a website (like reddit) put out a "new" design that destroyed usability?

But sometimes new *is* demonstrably better. Take newer software versions: while there are routine updates like security fixes, major updates - such as moving from single- to multi-core architecture - can offer exponential improvements. Just compare screenshots of Windows 1.0 to Windows 10: the difference between older and newer versions is simply staggering. Of course, we also get software like Node.js, which over time seems to have gotten worse and more bloated. In fact, a common complaint about modern software is the bloat that makes it run slowly on faster hardware, in contrast to retro software that often had to be tweaked in very creative ways to meet hardware limitations. So is new or old better? The answer is not so clear cut.

For our next dilemma, we turn to code sharing. With the advent of version control systems, like git, and websites to share projects (such as github) comes two developments: the ability and encouragement to share software that is "in progress," and the push to likewise share any changes we've made via pull request or repo forking.

When we talk with artists, we learn that sharing "works in progress" is very controversial, especially when we are used to only seeing a final product, like a book or a painting. Similarly, some open source developers will quash their git commit history when they put out a new version.

There's also the question of whether the art created is inspired by the artist, or inspired by external pressures that the artist feels once the "in progress" art is shared. Conversely, many argue that there is no such thing as a "finished" project, and when a code repository is transparent down to the level of individual code commits, it can create an inviting atmosphere, welcoming contributions from anyone in the world. One could even argue that such radical transparency helps sidestep potential biases of the original maintainer of the codebase.

In the case of changes to code, there's an additional issue of ownership. When we take some code and modify it, licensing notwithstanding, or if we make some big improvement to it or manage to port it to an otherwise unavailable computer system, do we have an obligation to share this contribution with others? This boils down to whether code sharing is a zero-sum game: that is, when we add something new into code that is local on our computer, does not sharing it somehow take something away from others who are using unmodified code on their own computers? One could argue that it does, because someone else wrote the initial code base that we modified. However, if we follow this reasoning to its logical conclusion, then if we fix a security hole in the code and do not share it, and someone else using the unmodified codebase gets hacked, we would be at fault. Although without the original code base, neither the security hole nor our fix would even exist.

This begs another question: if we choose not to share our code, what impact does this have on the community in general? Or, put another way, which has primacy of importance, our personal agency and privacy, or the good of the community? There is also a deep can of worms there regarding private property that is beyond our current scope, but it's important to acknowledge that it's there. So in the end, who really should "own" the code? There is no obvious answer.

And finally, we visit the age old debate of systems ownership, and the benefits therefrom. Let us take the idea of a networked system of computers, and look at it from different viewpoints. If we take the "my computer is my castle" approach, then there should be no ownership change for a computer, on or off the network - it belongs to us. The moment a packet has left the network cable and entered the memory or disk of the computer, it is owned by the destination IP, rather than the source IP. The software on our system is ours: we own it, and any interaction it has or makes with other computers on the network is determined by us. Likewise, if we have a hardware problem, we should be able to fix it on our own. This sentiment is the hallmark of the "right to repair" movement, and views the corporate nature of things like software activation and "take it to the Apple Store" with suspicion.

On the other hand, we could also view our computer as one member of a networked community of systems, with mutual responsibilities to each other. If our computer gets hacked by a virus, who is to say that that virus won't spread to other computers as well? In this approach, we have an obligation to keep our computers updated with the latest security patches, not just for our own safety, but for the good of the others as well. We can take this a step further and, assuming we sometimes have idle time on our systems, donate resources like CPU cycles to a good cause like SETI@home, protein folding, COVID-19 vaccine research, etc.

But with all of this there is a large downside. By allowing a third party to automatically access and send updates to our computers, we are also at risk from their mandates. Let's say Microsoft decides they do not want Windows users to be able to use Google Chrome - what's to stop them from using their automated updates permission to also uninstall Chrome and set a registry key preventing us from running it? Or worse, why not simply outsource the functionalities found in applications to some "as a service" website, where our computer becomes nothing but a dumb terminal without network access and approval to access the centralized system? A third time, we discover why this "choice" is a dilemma.

The nature of a dilemma is such that a given situation has multiple views on the "correct approach," none of which are "correct," and each, if taken to the logical extreme, become tyranny. When there is no good answer, we must revisit our own conception of first principles, and decide what for each of us is the best balance. A parting rule of thumb: when something is controversial, it means that there are no easy answers, and so when trying to pick a path, it is important to consider all viewpoints.

An Introduction Algorithm to Decoding an Enigma

by Diana K

Over the weekend, I watched the movie *The Imitation Game* about Alan Turing and the computer built to decode the Enigma. In the 80s, while studying AI at UW-Parkside I was able to meet a friend of Alan Turing's who oversaw the Turing Institute. In addition to studying AI, I was interested in encryption as well and started understanding a Bazeries Cylinder like one used in *The Da Vinci Code*.

The Enigma is like a Bazeries Cylinder except that it has a plug board which provides an additional transition. So, instead of a three-state transition as in a Bazeries Cylinder, there is a four-state transition provided by the plug board. To give an Enigma example, consider the following morning message (assume it is written in German like in WW II):

```
The Weather for May 21st, 2022 is
8 degrees C and Sunny.
```

In reading the message, it seems pretty simple, and one might have the ability to use a brute force algorithm to break about 51 million combinations on a computer that ran at a processor speed of about 1 kHZ. Actual, the solution could not be found within the timeline of 18 hours from the 6 am broadcast.

What was a faster way? The faster way was found by talking with others who intercepted the encrypted messages and could tell that a specific person on the other side was typing the message. By realizing the same person was typing a daily weather report at 6 am on the other side, one could have a set to compare. For example, the person would ably follow the same message format:

```
The Weather for May 23rd, 2022 is
14 degrees C and Sunny.
```

Then, taking the next step of comparing the actual message with the encrypted message, part of the state transition could be obtained. The weather report messages were deciphered by those who were able to use alternative methods to deliver the messages, but not the Enigma encoding and plug board.

At a listening center, a group would have the decoded message:

```
The Weather for May 21st, 2022 is
8 degrees C and Sunny.
```

And the encrypted message:

```
"Yop%Raebtep@Ayv!9v{WOSD%hf@
➥g$sfuadq&q@qkg*znght,"
```

What does this mean?

The thing to remember about the Enigma machine is that it had four-state transitions. So, if someone typed "T," the second state transition could be "Z." When the letter "Z" is submitted to the plugboard, the next letter could be "B." The letter "B" is what would be sent via radio telegraph.

When the receiver would type the letter "B" on a similar Enigma machine, the internal transition would come out to "Z" via the one of the three wheels of the Bazeries Cylinder and then the "Z," Wheel 1 would come out to "B," Wheel 2, then transition to "A," Wheel 3, and finally transition "E" on the plugboard. So the state transition is T-Z-B-A-E-T.

The problem is coded for searching for a substring with T-?-??-???-????-T. Also, as other four-state substrings as added to compare and solve the algorithm, the "?" and "??" can be determined. However, it took a few substrings to use as a seed.

What is the algorithm? The algorithm starts with a state of either 1-4 like in Turing's state machine. Next, a substring is selected as "T-?-??-???-????-T." A method to solve the problem is to work backwards. So, what setting is needed on the plugboard to transition X (internal coded character) to "T?" The process compares various substrings in State 4, and the first backward solution is "T-?-??-???-B-T."

After the plugboard is solved, the next state is State 3 on the third wheel. The original search substring of "T-?-??-???-????-T" is now changed to "T-?-??-???-B-T." In a way, it is like a Keno game. In a Keno, after determining one set of numbers in a betting string, the process becomes cooperative to finding other solutions in an easier manner.

In State 3, when a substring message is found beginning with "B," a combination of trials is set to determine what possible settings from the plugboard to wheels 3, 2, and 1 could lead to a transition going backwards from "T-B-wheel 3 setting - wheel 2 setting - wheel 1 setting - T" from a set of sample words in the message.

The process is repeated backwards until the plugboard and wheels 1-3 are solved for State 1. Then the same method is used in State 2. When State 2 is solved, the same method is used in State 3. Which means the plugboard and three-wheel settings are determined. The solution would look something like this:

```
Wheel 1: A- E
Wheel 2: E - Z
Wheel 3: Z - (
Plugboard: (- A
```

If one were to consider that there were 32

setting for three wheels and the plugboard, the combination is (2^5) ^4 or 2 ^ 20 combinations. However, by knowing two of the transitions, the combinations needed to be solved are: (2^5) ^2 or 2^10 combinations, a speed-up of 2^10, which allows a solution within an 18-hour time limit.

In Pascal like pseudocode, the code would look like this:

```
1. Program breakEnigma;
2. // © 2022 Diana K
3. Var
4. subCrypts: array[1..3,1..5] of string = (('T-?-??-???--X-T'),('A-?-
➥??-???-P-A'), ('C-?-??-???-Z-C'),('Q-?-??-???-B-Q'),('G-?-??-???-Q-G'),(
➥<second set for state 2>), (<third set for state 3>);
5. msg: string;
6. i, j, k:integer;
7. settings: array[0..3] of integer = (0,0,0,0);
8. maxWheel: array[0..3] = (32, 32, 32, 32 );
9. state:integer;
10. completed:Boolean;
11. function decrypt1(cryptMsg): Boolean;
12. var
13. I, j, k:integer;
14. Tmp: string;
15. Solved : Boolean;
16. Begin
17. Tmp:='';
18. Solved := true;
19. For i:= 1 to length(cryptMsg)
20. Do begin
21. J:=(I mod 4);
22. // plugboard
23. Tmp[1]:=chr(((ord(cryptMsg[i])+setting[j]) mod maxWheel[j]);
24. // wheel 3
25. Tmp[2]:=chr(((ord(tmp[1])+setting[(j+1) mod 4]) mod maxWheel[(j+1)
➥mod 4]);
26. // wheel 2
27. Tmp[3]:=chr(((ord(tmp[2])+setting[(j+2) mod 4]) mod maxWheel[(j+2)
➥mod 4]);
28. // wheel 1
29. Tmp[4]:=chr(((ord(tmp[4])+setting[(j+3) mod 4]) mod maxWheel[(j+3)
➥mod 4]);
30. Solved:=solved and (cryptMsg[i] = tmp[4]);
31. End;
32. Decrypt1:= solved;
33. End;
34. Procedure solvePartialSubCrypt(state:integer; I:integer;
➥settings:integer; subCrypts: string[][]);
35. Var
36. I, j, k:integer;
37. Begin
38. // convert pseudocode lit to pascal like pseudocode
39. // a challenge to the reader, easy to do
40. End;
41. begin
42. writeln('Program Break Enigma');
43. write('Enter Encrypted Message? ');
44. readln(msg);
45. writeln;
46. writeln('…Starting Solving');
47. for state:=1 to 4
48. do begin
```

```
49. for i:=4 downto 1
50. do solvePartialSubCrypt(state, I, settings, subCrypts);
51. end;
52. // check work
53. Completed:=true;
54. For state:=1 to 3
55. Do for j:=1 to 5
56. Do competed:=completed and decrypt1(subCrypts[state,j]);
57. // show result
58. If not completed
59. Then writeln('A Solution was not found')
60. Else writeln('A Solution was found');
61. Writeln;
62. Writeln('Settings: \tPlugboard \tWheel 3 \tWheel 2 \tWheel1');
63. Writeln('\t'+settings[0]+'\t'+settings[1]+'\t\+settings[2]+'\
➥t\+settings[3]);
64. Writeln
65. Writeln('…Program Completed');
66. End.
```

What is interesting about the Enigma is that even today with a laptop computer, it takes about one hour to break an Enigma code - faster than 18 hours, yet still long enough for a message to become invalid if a decision is made an hour later after decoding.

The primary advantage of encryption is not the method itself; the primary advantage of encryption is how long does it take an opponent to read your message, and can your opponent read your message in time, while the message time is still valid?

Is It Time to Change Our Approach to Security?

by Cr0wTom

If you try to remember how everyday life was in 1984 (the year *2600* was founded), most of you will not remember at all, with some of you not even born at the time. This was when the "digital" space was kicking off, and a new generation of hackers started appearing. People with passion about technology, and creating and destroying things. But from this small collective, it started becoming a whole industry, until we reached today and an era where we see one critical RCE 0day after the other. But in order to see this amount of 0days, we need technological advancements and wide adoption of them from users. Which is the reality of today. Despite our expectations for flying cars and ovens that will take raw materials as input to output ready-made dishes, our technological leaps are enormous, and you don't need me to prove it to you.

Just look at your pocket, your garage, your TV, or even your toothbrush.

Our life is getting more and more connected. With the excuse of "efficiency" and "practicality," companies got (almost) all our devices connected to the Internet. And this is not a bad thing, but "with great power comes great responsibility." It is one of the biggest clichés ever, and it applies perfectly in this case. Companies want us to use their connected products and services. They need us to do it and they will do everything for it. Unfortunately, most of the time important aspects of the product development cycle will get bypassed, with one of those aspects being safety.

Safety Critical Devices and the Path to a Better Future

You might not think about it that way, but what will happen if someone hacks and disables your fire alarm? What about your fancy Roomba, which happens to mop your whole apartment? Your car, which you expect to act "smart" and "assist" you with its ADAS (Advanced Driver-Assistance System)?

You guessed it right. If some of these (or thousands of other) devices are developed with weak security, or even in cases where a product gets rushed into market with the mindset that it will be finished and polished at a later stage (*yes* Elon, I am looking mainly at you), then the impact is not only on the security side of things, but also on the safety,

with possibly devastating results.

Should this have been considered when evaluating security findings? Should it potentially increase the severity and the impact of those findings?

Our answer is not clear. It comes mainly from the automotive sector, where safety can be the most impactful characteristic with connected and autonomous vehicles already in the wild. But what we are sure of is that a reevaluation of the scoring systems has to be performed.

Different versions of CVSS (Common Vulnerability Scoring System) as an example, are released and embraced by security professionals and security-oriented product teams.

But is that enough?

Case Study

Unfortunately, I cannot talk about specifics. But I will give you an example of an OEM in the automotive industry where I was called to perform a complete security assessment on their product. Following standard testing methodology targeting the testing unit, I found several security "issues" that an unauthenticated user could trigger to perform physical actions in the vehicle (e.g. gas, brakes, etc.). Those findings were applicable only with physical access to the vehicle, which meant that an attacker had to physically access it to perform the attack, but after the initial foothold, all the actions could be performed remotely.

On this assessment though, we were "forced" to use the beloved CVSS scoring, which did not reflect a really important aspect: the physical safety of the driver and passengers. As a researcher, I can accept that a rating and a standard have to be used in order for all the parties to have a common understanding of the severity of the issue. But big corporations use these ratings and, depending on the policies, they reflect it on the final decision of "if" and "when" they will mitigate this finding.

Back to the actual finding though, the OEM took the resulting CVSS rating and chose to not mitigate the issue in the end, regardless of the safety implications....

As a researcher, my ultimate goal is to make the world a safer place. I tried to explain in detail how this finding can be used in an exploit chain, and how all the other interfaces that are connected to this functionality can be compromised and result in devastating outcomes. But security ratings have their place and huge corps do not (and will not) change their policies overnight.

Should There Be a Shift?

How should I feel now? Is it my problem if the brakes engage when the car is running at 120 kilometers an hour? Is it my problem if the assisted driving fails completely at the same speeds?

Yes and no, and that's why I am here writing this article. We need to start thinking about security in a different way. We need to start approaching exploit chains with safety in mind. Data, privacy, integrity, exploitability and everything is good, but we have to make sure that people will not die out of outdated practices, beliefs, policies, and cut corners (now I am looking at you Boeing).

Let's make the world a happier and safer place. There is still a chance.

Disclaimer: The finding got fixed, but we are sure (and we know) of many occasions in which companies act irresponsibly regarding critical safety components. Many times we find ourselves having to defend our findings in cases where we should not have to. Automotive and safety critical industries are new to the connectivity game and some mistakes will be made, and that's why we, as professionals, should be here to help them create better and safer products.

Will You Let Your Car Drive Itself?

By E.V. Rhodes

"Wanna see something weird?" is not a question I usually ask passengers when I'm driving, but in February 2022, as we headed north for a ski weekend, I explained to my two companions how I'd previously noted some odd, even alarming, behavior when using the cruise control feature on my new Tesla Model Y, and I asked, did they want to see if it would do it again?

In my previous experiences, the cruise control had properly maintained the car's speed for long periods of driving. It also accurately kept a set distance back from any vehicle ahead. But several times it had suddenly and dramatically slowed. I could not tell if it had detected a threat, for it gave no reason for slamming on the brakes. After this happened several times, I simply stopped using the cruise control feature.

This is not Tesla's much-touted "Full Self-Driving" software (at the time a $10,000 upgrade which was an easy "no thanks"), but simply their standard "Traffic-Aware Cruise Control" which they say "is designed to slow down Model Y as needed to maintain a selected time-based distance from the vehicle in front, up to the set speed... primarily intended for driving on dry, straight roads, such as highways." I explained to my passengers that I wanted their consent before trying it again, as well as their observations and insights should anything happen. With their agreement, I engaged the cruise control, set the speed limit, and removed my foot from the accelerator. The day was sunny and clear, the highway traffic was light, and the car continued carrying us towards the distant mountains. I remained in the right hand lane, alert and driving as usual.

But not 20 minutes later, it happened again!

I'm not someone who resists technological progress. Years ago, I built a ZX-81 computer kit and used it to control a simple robot arm. In college, I worked at a Fortune 500 company writing "expert systems" software to optimize manufacturing processes, and later I helped to develop an autonomous robot which could locate and navigate to its recharging station, and stay "alive" for weeks at a time. So when it comes to software for self-driving cars, I appreciate the challenges, and have great respect for the programmers and the results they've demonstrated.

In 2014, Tesla began offering limited self-driving capability on some of their vehicles. With frequent, incremental software updates, development proceeded rapidly. By January 2016, Tesla's CEO stated that the their autonomous driving system was "probably better" than most human drivers. Of course, "probably" is difficult to quantify. The real world presents autonomous systems with incredible complexity; ever changing weather, illumination, and surroundings, not to mention the unpredictable behaviors of people, animals, and other vehicles. Self-driving cars must reliably and accurately generalize from highly variable data, and be prepared for an enormous number of situations which might occur incredibly rarely, if ever. The fact that self-driving cars can travel on public roads at all represents an astounding technical achievement. But they are only safe until they are not.

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 and decelerated rapidly! The driver behind us swerved to avoid a collision and sounded their horn. Why had we slowed? There were no obstacles or vehicles ahead of us. The road was straight and clear!

I immediately stepped on the accelerator, disengaging the cruise control and resuming our speed. End of experiment! One of my passengers thought a section of the road may have been resurfaced, and perhaps looked slightly darker than the rest. Did that register as a threat to the software? (Unfortunately I did not capture a dash cam recording of the event.)

I have never enjoyed being an unpaid software beta tester, and I'm even more reluctant to be a guinea pig where problems could result in injury or death. I have not used the cruise control since that day, but I recently learned that our alarming event was not unique. Many other Tesla cruise control users have also experienced sudden, inexplicable braking. On May 4, 2022, the U.S. National Highway Traffic Safety Administration (NHTSA) issued a letter to Tesla stating "This office has received (758) seven hundred and fifty-eight reports of unexpected brake activation in certain (MY) 2021-2022 Model 3 and Y vehicles." With that

many people concerned enough to actually file a report with a government agency, how many others (like myself) had not reported their experiences? Thousands more, I suspect.

Now don't get me wrong. The Tesla Model Y is an excellent car with great performance, comfort, and tons of amazing features. The very same NHTSA gives it five out of five stars for overall safety. Rising gas prices make owning an electric car increasingly affordable, and if you have solar panels you can easily produce all the fossil-free energy it needs right at home, making them good for you, your wallet, and the planet. (End of EV plug.)

But, if adding machine intelligence to a fairly standard feature like cruise control (first offered on a Chrysler production car in 1958) presents such mysterious and life-threatening difficulties, what about the much greater challenges facing fully self-driving cars? They already have been involved in many reported injuries and deaths with everything from drivers stupidly defying important operating instructions, to innocent individuals tragically hit on roadsides. Self-driving vehicles pose risks not only to the drivers who knowingly accept them, but to potentially anyone in their presence: other drivers, passengers, pedestrians, motorcycle and bicycle riders, highway workers, police and emergency responders - in short, almost everyone.

It surprised me to learn that the USA currently has no federal laws governing self-driving cars. In 2016, the NHTSA did publish the "Federal Automated Vehicles Policy," a set of guidelines which they say provides "a proactive approach to providing safety assurance and facilitating innovation." This allows developers to act quickly and develop solutions rapidly with fewer legal obstacles, however it can also be seen as placing profits before people, since nothing legally requires them to hold my safety as their highest concern. How can we know in an objective, fact-based way, when self-driving vehicles are actually able to increase the overall safety of our roadways? Perhaps we must simply accept that automobiles are dangerous, and that some amount of injury and death must be expected. We already tolerate that with human drivers, why not machines as well?

Well, because the goal of self-driving vehicles is to make our roads safer, not less safe. Determining if and when they actually are safer will require an army of highly trained, detail oriented investigators, drilling deep into vast amounts of real-world self-driving vehicle data, verifying their findings, and standing behind their conclusions.

Interestingly, we have just such an army: the worldwide auto insurance industry, valued at over US $700 billion in 2019. Insurance actuaries assess the risks existing at the dynamic intersection of human behavior, government regulation, and automotive technology. The field is overseen by government agencies which monitor insurance rates, coverage, and incentives. At present (in California anyway, your state or country may vary), pricing discounts are offered for good driving, good student grades, being away at school, and having multiple vehicles on the same policy.

Insurers currently do not offer any financial incentive for using self-driving vehicles. Such adjustments can only come after a long period of rigorous statistical study that objectively proved such systems actually helped reduce accidents and save lives. Those studies would be used to support the creation of legislation authorizing insurance companies to offer such discounts. This presents a chicken-or-egg type safety conundrum: there can be no incentives for self-driving cars without extensive real-world studies, and there can be no extensive real-world studies without putting lots of self-driving cars on the roads before they are definitively proven safe.

For an inexact comparison, look at the history of seat belts which, starting in the 1930s, were clearly shown to save lives, but which did not become mandatory equipment in U.S. cars until 1966. Even then, their actual use was not enforced until much later; New York passed the first "click it or ticket" law in 1984, and all other states followed suit by 1995 - except for New Hampshire which, at present, only requires seat belt use by persons under 18 years of age. (As it says on their license plates: "Live Free or Die.")

A long road lies ahead for widespread acceptance of self-driving cars. Until then, the path will be paved with varying degrees of danger and uncertainty. Should major insurance companies someday offer me cash discounts for using autonomous systems, I will take that as a solid indicator that self-driving cars have finally achieved true safety and reliability improvements.

Until that time, I'm keeping my cruise control disengaged, and my foot on the pedals.

Special thanks to Alex K for insights into how the insurance industry contends with new developments.

The Hacker Perspective

by XCM

Up until the age of ten, my curiosity would typically translate to destructive behavior towards any mechanical object or small electrical appliance I could find. Of course, I would only experiment on things I felt nobody cared about. My judgment over time turned out to be accurate within an acceptable degree.

Sometimes I even managed to put things back together. When this occurred, they would mostly work again.

And then one day, out of the blue, it happened. I was given a computer.

I don't remember how I felt initially.

Of course, the first thing I did was to press on the two metal levers on the side of the chassis and slide the metal cover open.

I had no idea what I was looking at, but it felt great. It felt like an important milestone.

After a few moments considering whether I should proceed dismantling the thing, I decided against it. At least for the moment.

I put the cover back on, pinched a finger in the process, and switched the power button on. You know, a real, mechanical switch.

Of course, there was no need to re-apply power beforehand as I had not bothered with disconnecting the mains before opening the machine.

Now imagine "Also sprach Zarathustra" by Richard Strauss. Got it? Good. The emotion conveyed by those notes describes quite accurately what I felt when the monitor slowly started throwing loads of text at me.

I could see things. Lots of writing. Arcane messages. It felt as if the being was trying to communicate something to me but I was too inexperienced to understand.

It did not help that my knowledge of the English language was zero at the time. Besides, had I been able to read that text, the whole experience would have taken a less mystical flavor.

When the creature finished saying what it had to say, it looked like it stopped, waiting for something from me.

And so my exhilarating journey through MS-DOS began.

I remember the sales representative who sold us the computer that morning handing me a plastic box with a bunch of what he called "floppy disks" inside.

Looking me in the eyes sternly, he declared: "Here you have one hundred games. Now there is no need for you to go elsewhere and risk getting a virus."

I opened my hands, solemnly receiving that mysterious box and I could not help but thinking: "Wait a minute. Is there an 'elsewhere?' Is there a place where I can get things to put in my computer? I absolutely must find this place."

This is how my 30 year quest for computer knowledge started.

Access to information was very limited at the time, especially technical. The Internet was not mainstream yet and public libraries did not have much material on computers.

This left me with commercial bookstores and a meager budget.

After lengthy consideration between a bunch of video game magazines, sweets, and a book, I finally decided on a book on programming

I read the whole thing from cover to cover. After two days, I put the book down, typed "EDIT" at the command prompt, and started hammering away at the keyboard.

Of course, I also quickly went through the disks given to me by the generous computer sales guy. Alas, soon I discovered with the utmost disappointment what foreign words such as "shareware" meant. All of the games on those disks belonged to that category.

I then quickly discovered the joys of decompressing games with ARJ from floppy disks exchanged at school - some of which had the tendency of playing the dreaded sound of the damaged sector at around 90 percent of an eight-disk decompression process.

I believe this is how my informal

exposure to the English language began. I learned to guess the meaning of random words such as “missing,” “failure,” “bad,” or similarly ominous terms.

An important milestone in my journey was when I decided to have a proper look at a couple of curious files I had noticed some time before: CONFIG.SYS and AUTOEXEC.BAT.

There were a lot of sexy looking instructions in those lines with some intriguing values after each of them.

I spent some time messing with the numbers, thus enriching my vocabulary with new words that the computer started to uncooperatively bark at me - things like “abort,” “incorrect,” or “invalid.”

Then one day, things started falling into place and I realized that I could reduce the computer boot time by disabling only the lines that did not completely break the boot process.

That led to a sizable reduction in time for a grand total of around five seconds.

I am sure that in the following months I just about got the time back that I invested in getting to that “optimization” to begin with.

After this major accomplishment, I discovered that by altering those files, I could also optimize some games and make things go smoother.

Once I ran out of options for software tweaking, I started looking at possibilities for hardware upgrade. This was potentially a sore point as I definitely did not have the budget for expensive electronics.

All I could manage was a one megabyte bank of memory miraculously salvaged while rummaging through a pile of trash at a car boot sale. Things looked brighter for a bit, but then it dawned on me that more RAM does not mean faster games.

It was then, with great excitement, that I learned one of the most promising words I had come across in a while: “overclocking” - the arcane art of squeezing extra CPU cycles by shorting some random pins on the motherboard.

Again, this was a totally trial and error process as there was no tutorial (and no Internet, to be precise).

However, after the occasional self-shutdown or freeze, I reached an acceptable balance by leaving the case permanently open with a small desk fan constantly blowing air at the dissipator.

So what are the most important lessons I have learned in all these years?

One aspect that I miss from my early computing experience is how intimate the relationship between human and machine was. Well, at least for me.

Computers had mechanical switches. Things made noise - they took time to “heat up,” as a friend of mine innocently revealed to me.

Now the whole approach is different. My MacBook is never really powered off. There is no proper switch. It’s silent and its inner workings are mostly hidden behind a pretty user interface.

Even modern Linux distros feel somehow more abstracted, colder, distant.

One useful fact that I learned is related to my memory of when I bought my first book about coding, which I wrote about earlier.

Looking back, that was the most focussed and productive learning effort in my whole life. Surely, it was all new and exciting and my brain was nearly 30 years younger, making things easier. But there is a specific element that made this possible: information scarcity.

While this might be counterintuitive at first, I am convinced that being in my room with that book, and that book only with no distractions, allowed me to focus 100 percent on my objective.

Imagine doing this today: you can get an online subscription to access thousands of digital books. The Internet overflows with information on any topic you could desire. And then, of course, we have smartphones to steal as many brain cycles as possible from us.

I don’t know about you, but I still remember as a kid sitting on the toilet and reading the shampoo ingredients list, rather than a smartphone. OK, when I ran out of labels to read, I started taking books with me to the toilet, but that gives you the idea.

This cacophony of data, at least in my experience, results in an overabundance of stimuli that makes the process of focusing on a topic extremely difficult. It creates what I believe is called “information overload,” which for people who are thirsty for knowledge is a very insidious threat indeed.

And it can get addictive, too - up to the point where our brains cannot cope with this constant influx of data and we experience a sense of being overwhelmed

that can manifest itself in various areas of our lives in the form of anxiety.

I know this concept is possibly complex to grasp by someone who is starting this fantastic journey today, but I believe there is a valuable suggestion here: resist the temptation to hoard more information than you can absorb. It will not make you more knowledgeable. It will just highlight your limitations as a human being.

Some people are OK with that. I, however, reacted differently. I experienced a dreadful fear of missing out. Anything that I could not read was information that I would forever be ignorant about.

Also, this constant switching between books, articles, videos, and the like further reduced my attention span, as our brains are not made for multitasking, really.

And before anyone says: "women can multitask." No. Women cannot multitask any better than us men can. Women just get shit done and do not complain.

Also, thinking about that period of my early life, I would define it as "boring" under today's standards. Little access to information, limited sacrificial gear to experiment on, and a sense of loneliness as none of my friends at the time spent their afternoons in the company of screwdrivers, pliers, and an emergency one kilogram hammer.

Over time, I was constantly coming up with lots of questions and little answers. All of these questions kept cramming in my little head with no outlet to direct my desire of knowledge to.

I am convinced, however, that being bored was a great catalyst to develop my imagination and aide experimentation. Being bored forces you to find something to do with what you have - to repurpose things in unexpected ways to pass the time. It forces you to become a hacker.

These things do not occur easily nowadays and similar opportunities are lost, due to the multiple distractions we are constantly surrounded by.

Another important lesson I learned over time is that whereas there might be shortcuts in life, they rarely bring the most favorable outcome. Most of the time, the hard way is the best way. Cliché as this might be, I believe it really is a valid point to remember in life.

One additional advantage of those initial experiences is that I feel a lot more confident about learning. I see so many people, at different stages of their lives, who dread having to learn new things. And this is a real shame as, in a way, knowledge still is power. The moment we stop learning, we really become at risk. Not only professionally, but we also lose so much potential as human beings.

I always say to people who are daunted by learning that acquiring information is easy. I confidently tell them that they can learn anything, given the right dedication.

I am often met with a look of disbelief. They do not appreciate the simple fact that we are all born ignorant and inept. Those people all have one thing in common: they were never given the opportunity of a safe environment where failure was acceptable. They never broke things to see how they worked. Therefore, they were never in a position where they could fix what they had broken.

In few words, they lack self confidence.

This is what hacking is about. Constant excursions outside of our comfort zone because of actions we willingly took, most of the times completely oblivious of the consequences.

And every time we learn from our actions, every time we fix what we ourselves have broken, we feel we have reentered our comfort zone.

What we don't realize, at times, is that what really happened is that our comfort zone has just expanded. This will only happen when we push the boundaries hard and often enough.

I am so glad that I was given the chance to go through this process. It is one of the most fundamental steps in my formation and I am striving to offer the same opportunity to my children.

I really hope it will be valuable for them as it was for me.

XCM can be found consulting for various organizations on designing and implementing certain cyber security solutions. In his free time, he loves reading classics and challenging his kids to think critically about the reality they are exposed to. When the youngsters challenge his beliefs, he realizes he must be doing something right in life.

HACKER PERSPECTIVE *SUBMISSIONS STILL CLOSED - STAY TUNED!*

A Ripple Story

by Cryptopian

I worked at an unnamed crypto company in San Francisco and got a close-up view of this controversial industry.

On second thought, let's name it. It's Ripple, the "enterprise" crypto blockchain.

Ripple was a funny place to work. Most startups have a consistent cast of characters, so that one startup's staff is almost interchangeable with another's. Not Ripple.

Back in the day, Ripple was hiring oddballs, in bulk. The theory went something like this. Crypto is a new industry, created by the collision of very different elements: cypherpunks and banking, independent developers and enterprise software, etc. So our people should reflect this.

For our purposes here, let's focus on developers. There were people who were super into Bitcoin, who often combined a consultant's mentality - "whatever gets the job done" - with a libertarian ethos (note: that's different today than what it was). There were traditional software developers, with pedigrees from elite institutions and blue chip work histories. There were people who wanted to break into the industry - and found their way in. And finally, there were journeymen, who'd been in the industry shoveling away for years, hopping from one job to another.

There were also programmers at different levels of mission-critical. There were the protocol developers, who were C++ (the language) rock stars, and frankly, bored. They were all extremely skilled, so skilled in fact that they ran out of things to do: the blockchain worked, they had optimized it, and more ambitious goals were walled off by management. You know those algorithms that Google tests you on? They had invented some of those. Then there were the front end developers, who became more standardized over time, but were a real grab bag back then (and didn't have that depth of knowledge).

Over time, the traditional developers edged everyone else out, and the other groups either found a space on the margins, or quit, or were pushed out. One of the groups that experienced the most tension was the Bitcoin people, who seemed to be itching at this question almost daily: If you really believe in a decentralized crypto future, what are you doing at a fully establishment, centralized one? Those were some of the first people to go.

In the beginning, that wasn't a problem, because Ripple, theoretically, was everything and anything you wanted it to be. It really depends on how far back you go, because its history changed a lot, and is a trip in itself.

It started off - the software equivalent of the Cambrian Age, so far back even the "early people" barely remembered it - as Opencoin. This bumped along for a little while, maybe of interest to people looking to get in early on something that hadn't yet taken off and become "too expensive" like Bitcoin, then in the tens of dollars (ha).

Ripple, in the words of recruiters - which is how most hires found out about it - was crypto which was going to be the future (this was long before it saturated the media-scape, before Ethereum even existed). It was fintech. It was going to help the unbanked - from a comms perspective, the hook into the disruption and revolution perspective that was so popular at the time.

As time went on, Ripple evolved, as a company, from "kind of a crypto play (emoji shrug)" to "enterprise blockchain." You might say, "Wait - I thought they were a cryptocurrency?" And not only would you be right, you would have hit on a fundamental tension that was never really resolved. Ripple *was* a cryptocurrency company, but it was also supposed to be selling banking software to enterprise companies, which sometimes led to the funny sight of Ripple talking about its own product in the third person, as though it was an infrastructure provider when its own bag was the "infrastructure."

Ripple did have market fit, in a way. But it wasn't a market Ripple really wanted or truly loved.

Ripple, for whatever reason, had caught on in a big way in Asia. What happened was that brokers would buy up large amounts of XRP, then resell it to investors. They promised the investors they sold to that, even after a huge markup, the could become rich. As it happens, they were right: Ripple's price was so much lower back then that this strategy was ultimately

vindicated. If you crunch the numbers, then yes, you could have bought XRP from these brokers at five times cost, and still made two to ten times (or more) on your investment.

a famous zinger about this

At the time though, that seemed almost unimaginable; we would laugh about Ripple passing one dollar (it eventually, briefly, passed $2.50). The wholesale sellers were a third party we never talked about that much. Sometimes one of them would sweep in and do a tour (including the founder of a very famous project, now). We also knew the users they sold to got hacked at a horrendous rate, though to be fair that wasn't due to security flaws in the protocol.

If this sounds like indifference, it wasn't personal. The core problem was: their speculative cottage industry could never float Ripple at a valuation the venture capitalists could accept, so the search was on to find something that could. The idea that got the most mileage then was that Ripple would replace SWIFT, the world's international banking rails, which... yeah.

So because Ripple didn't have a real business, and didn't have a product market fit (that it wanted or could love), it was totally dependent on personal power and politics, on a knife edge of "value that could be delivered" as opposed to "value being delivered now" (because there was nothing concrete that any desirable customers wanted from it). Ripple's mission then was about finding something that would combine fintech and cryptocurrency into something even better; the cryptocurrency was the Trojan Horse that was supposed to get Bank of America to buy XRP like bonds. But why would they, or their peers, do this? They didn't need us; in fact they thought we should be paying them for the validation their logos would give our brand.

So Ripple never found any real enterprise banking customers, and the only paying customers were the speculative XRP paying kind, who never really had a full place in the overall vision.

There was a small community of people at the company who did care about cryptocurrency, who never really fit in comfortably. But of course, since Ripple recruited a lot of people with the cryptocurrency promise, it had to have some kind of story for them. You could get a sense of this in the very strange internal XRP buying process, which you had to ask about, which wasn't volunteered, and which wasn't especially popular among employees. Of course, that was par for the course of the time; we'd heard stories about employees at one crypto company who'd accepted payment in Bitcoin when it was in the mid hundreds, then got whiplash when Bitcoin sank to the 50s, so much so that the policy was discontinued. (At the time I'm writing this, Bitcoin is about 30k.)

So Ripple muddled along, as the industry evolved and spread its influence into the culture at large. And then Ethereum came on the scene.

Ethereum was vaguely talked about in Slack, which was a newfangled thing at the time. I remember meaning to look it up, forgetting about it (that's how infrequently it was discussed), and then remembering "oh yeah - I meant to buy that" when I saw a price quote for it on an early exchange, which has probably disappeared by now. It had reached $10, at which point I thought: I missed that boat - I'll catch the next one.

But Ethereum went on to become a legend. XRP is still hanging on in the top ten of coins. Meanwhile, the cryptocurrency industry keeps evolving. You never know where tech is headed, or where it will end up; cryptocurrency was the most niche of niche things back then, and now it's unavoidable. Computers themselves have gone from toy to center of the economy in my lifetime. What will happen after that? Technologists will still be telling their stories a hundred years from now. This one was mine.

I hope you learned something from it - and thank you for your time.

Hackers - What is Our Mission Statement?

by ScreamingYellowFish

Recently I have been thinking quite a lot about what appears to be an ever growing and widening chasm both within the readership and the hacker community writ large over several concerns that cast a pall over in an ominous and foreboding way:

- Have we lost our mission of staying on track as a font of technical information?
- Have we become too political, or indeed even too polarized or partisan?

What troubles me more, however, is the notion that these two vexing questions are somehow antithetical, or worse, that discussion of this topic has in and of itself become too toxic to approach. That, to my mind, seems to have already had the corrosive effects that our detractors from our past would never have imagined could do more damage than their worst machinations.

This alone would warrant its own article and, in fact, I have already written and submitted one to this fine publication. Instead, I thought it might be instructive to take a step back and shine some light on a more recent turn of events that sadly ties the two together in a more insidious way that clearly highlights the numerous problems at hand, and then some of my own thoughts and questions about who we are as a community, and what we can do to course correct while we still have the opportunity to do so.

In our professional lives, whether we are employees or contractors, self-employed or part of a partnership, at some point we have all come across and have signed myriads of documents. Maybe you scrutinized them carefully with full attorney review. Maybe you blindly signed them with nary a thought. Example of these might be non-disclosures (NDAs), non-competes, invention assignments, previous employment disclosures, etc. Upon leaving employment, you may have to sign termination agreements or separation agreements. In disputes, you may even have to sign arbitration agreements, settlement agreements, and the like.

Let's now imagine a world where you create a nifty algorithm or app or whatnot. Maybe its entirely your own, or maybe you borrowed from open source, or some derivative idea, or collaboration. Maybe it's all entirely original. Maybe you did a prior art or copyright check. Maybe you or your employer got a little lazy. Here's where things start to get murky and worlds collide.

Our imagined place of employment occurred in the nutmeg state of Connecticut. You are a contractor, and you run your own corporation and bill corp-to-corp. Congratulations, you figure you are protected from harm under a corporate umbrella and, should anything go awry, you can shut down your company and start again. Maybe that might be true if it's a civil matter... but what if your work was based off of stolen intellectual property (IP) from someone else? You may be wandering into criminal territory, particularly if it happens to be federal or, say, military. What if you didn't know? Does that matter? What if it was a client of your client that did this, like a cousin once removed? Does that change the nature of crime?

Let's change the scenario. You are an employee instead. Are you protected now? Not necessarily. Assuming you are a bit-head who just wants to write cool apps and you got caught in the middle, does that mean you are off the hook if you were ignorant of the circumstances?

Let's go to the next level. You found out and reported this. Supposed you are ignored. As a contractor, things truly get murky at this point. Are you ethically required to walk away? Can you walk away? What if there is a severe financial penalty for quitting early or for not finishing the project?

As an employee, you dutifully report your findings to you manager. Nothing happens. You might even be told to leave it be. You then kick it up to HR. Again, nothing. What do you do now? Now let's suppose that they try to "incentivize" you to leave by making it a hostile place to work. Eventually you are "let go." Can you do anything? Connecticut is an at-will state, so not really. You could pursue the hostile workplace issue, but that just paints a target on your back. You could pursue Connecticut's whistleblower protection act, which makes termination illegal. Even under those circumstances, if you win, are you still protected from criminal liability?

All we wanted was just to write "kool code." All we got for our trouble was legalese in places where the sun don't shine. Worse, this is where what should be a streamlined process across the country becomes a nightmare game of whack-a-mole. Everything I laid out here is all state law context dependent. We lack any federally mandated guidelines that define a clear set of coherent rules and policies by which we can figure out how to navigate this mess.

It gets worse. I pointed out in my last article the dangers of the new Texas abortion law, where Texas lawmakers successfully managed to ban abortion in the state of Texas by end running the Constitution. Here's how they did it: The new law allows any private citizen to sue Texas abortion providers who violate the law, as well as anyone who "aids or abets" a woman getting the procedure.

Imagine now a scheme where any state can pass laws allowing a vigilante citizen or group of disgruntled citizens or corporations to come after anyone who may be in violation knowingly or otherwise of patent or copyright law, be they contractor or employee of any state or territory in the United States. You can run, but you cannot hide.

With the proliferation of software products and applications to countries around the globe,

this has become an even bigger issue. Think this doesn't affect you? Let's take another look at your nifty app. Let's say right before the war in Ukraine, you had arranged with a major distributor in the Russian Federation to sell and disseminate your application. After the war began, sanctions kicked in, but you no longer have or maintain control of your application. That doesn't change the "boots on the ground" reality that any sale of your application is in violation of the sanctions.

I'm no lawyer, nor do I profess to be. I don't claim to have profound expertise in contract law, employment law, or even international trade law. That's not the point of this exercise. What I want the takeaway to be is why talking about laws and politics matter - why talking about more than just coding and algorithms matter.

I have been an avid reader of *2600* since pretty much the beginning. Before *2600*, I was an avid reader of *TAP*, and before that it was *YIPL*. I suppose I've always assumed that the technical, political, and legal worlds were always intertwined. I think, maybe, the problem might stem from what may seem like an obviously clear mission statement, especially to older readers, but might not actually be so. Even the masthead, *2600 - The Hacker Quarterly*, does not really capture the point and purpose of what the hacker community has always been about and even where it is going. I've seen so many attempts to define the hacker spirit, the hacker ethos, etc. While so many attempts have been made to define what hacking is, maybe it's high time we start to have a discussion about why we are engaged in this endeavor in the first place.

Allow me to start with a few talking points:

- Intellectual curiosity about how and why things tick
- The belief that there is always an option C, D, E, etc. even if it flies in the face of "conventional wisdom"
- Desire to continuously improve existing systems and processes
- Desire to create new and unimagined systems not yet dreamed of or thought possible
- Expand our minds to new ideas and concepts to the exclusion of rigidly held beliefs and values

OK, that's the low hanging fruit. I think where we begin to deviate is how we define hack and hacker. If we can let go of the "bits and bytes" and "geek" for a moment, it soon becomes immediately obvious that there have been reams of pages throughout the magazine written on privacy, on individual rights, and on challenges to the status quo. Hardly the stuff of CPU cycles or JavaScript. Let's look at how that plays out in the last year:

- Protecting against ransomware attacks
- Penetrating into Russia with news to bring truth to its citizens
- Preventing false and misleading information on social media such as anti-vaccine narrative
- Protecting against both government and corporate intrusion into personal and private lives of citizens

In short, if we have the skills, ability, and imagination to take flight with the former, it would seem a moral imperative to become the wheel of change for the latter. I'm thinking that is the hacker ethic and spirit.

We live in an ever-changing dynamic reality - one of power and regime change, of war and pandemic - but one thing remains constant. We are the voice for those that don't have a voice.

How to Double-Spend a Bitcoin

by 0x80

First, sorry for the sensational title. No, I haven't discovered some amazing way to subvert the blockchain's integrity properties and perform an on-chain double-spend. Rather, this is a social engineering attack which takes transactions off-chain, enabling a double-spend.

But please bear with me. I think this will be interesting to many readers.

What Does It Mean to "Own" Bitcoins?

"Ownership" is a messy concept to define for Bitcoin and similar cryptocurrencies. The easiest definition of ownership is "the ability to spend." If you can spend the bitcoins, they're yours, right? But what if someone else also has the ability to spend those same bitcoins? Let's look briefly at how Bitcoin transactions actually work.

Bitcoin transactions have inputs and outputs. Transaction outputs are the closest thing to instances of bitcoins existing (and inputs spend the outputs from previous transactions). These transaction outputs are locked away with little programs which one must cause to return true (or, more precisely, a non-false value) in order to claim the output's value and transfer it to a new output. Usually this locking script returns true if and only if one can demonstrate (with a cryptographic signature) that they have the private key corresponding to an address contained in the script.

Bitcoin's scripting language isn't limited to just asking for signatures; it's possible to

make lots of different programs. It's possible, for example, to make a transaction output which can only be spent by someone who can find a SHA-256 collision[1] or someone who can provide a specific file, such as a Bitcoin-themed parody of a Western Union ad.[2]

And it's entirely possible that more than one person has the requisite file, or that a hash collision is known by multiple people. (Maybe none of them knows or cares that they can get a reward in bitcoin for it.) Even if the challenge is to prove ownership of a private key, it's always possible that multiple people know the same private key. The key could have been generated with insufficient randomness. One person could have compromised another's device. Even if two people do everything right, it's within the realm of possibility (however astronomically unlikely) that they just happen to randomly generate the same private key or that a hashing collision causes their private keys to yield the same address.

Until a transaction output is actually spent (and another is made to replace it), it's impossible to say with absolute certainty who "owns" it. Arguably, ownership can only be defined retroactively: if you spent it, you must have owned it when you spent it.

With this in mind, I thought of an interesting scheme. Of course, I would never do this, and neither should you. But what hacker doesn't look at a system like this and start to think of ways it could be exploited? So please, dear reader, play make-believe and enact this scheme with me.

Double-Spending Physical Bitcoins

For this scheme, we'll be minting physical bitcoins. These are a real thing, by the way. A Bitcoin user called Casascius made a bunch from 2011 to 2013 before stopping due to legal issues.[3] They're fundamentally just "paper wallets" (private keys written down), but in the form of metal tokens. The private key (or a seed used to derive it) is protected by a tamper-evident sticker, and the Bitcoin address (or its seed) is readable on the outside of the sticker. A transaction is created which locks away 1 BTC (or some other amount represented by the coin) such that it should only be spendable by someone who has the private key.

This enables the physical coin, representing a virtual coin, to be traded. Since the address is visible, anyone who observes the physical coin can check the blockchain to verify that a still-unspent virtual bitcoin is represented by it. However, they can't actually spend that bitcoin until they remove the sticker, exposing the private key and permanently marking the physical coin as used.

You might be thinking that when we mint these physical coins, we're going to simply write down the private keys and spend the virtual coins later. But that would be too easily detected. If we sell a physical coin to Alice and then spend the corresponding virtual coin, Alice can check the blockchain and see that her coin is gone!

No, instead, we're going to do something more subtle, which relies on the fact that these coins are collector items. Collectors like to keep things in mint condition. They're more valuable that way. Thus, it seems likely that many of our customers will not want to spend the virtual coins. Anecdotally, I know someone who has a small collection of Casascius coins who has told me that they would probably never remove the stickers. Empirically, at the time of writing, only about 27.5 percent of the Casascius physical bitcoins (counting by number of discrete physical units, not total BTC value represented) have ever had their virtual counterpart spent.[4]

We'll specifically target our sales to collectors we believe will not spend the virtual coins. Suppose we have two different customers, Alice and Bob, and we believe that neither will spend the virtual bitcoin, instead treating the physical coins only as collectables backed by virtual coins. Suppose that we also believe Alice and Bob will not compare their physical bitcoin collections. (We might choose pairs of customers in different countries with no apparent connection to each other.) In this case, we can create two coins representing the same private key and sell one to Alice and one to Bob.

Interestingly, since ownership is so messy, as long as neither party actually spends the virtual bitcoin, both Alice and Bob might be considered rightful "owners" of the same bitcoin, and to each, it will appear that they are the owner. And just like that, we have double-spent a bitcoin!

References

[1] bitcointalk.org/index.
➥php?topic=293382.0

[2] See transaction
200f3f6f8a91ae438d1924e5cedca98c
➥ea7f0197b9eba11343948b5621ca19ed
which provides a gzip-compressed jpg to spend one such output.

[3] en.bitcoin.it/wiki/Casascius _
➥physical _ bitcoins

[4] casascius.uberbills.com/

Articulations

Playing With Systems

Dear *2600*:

I had to make an installation appointment to have some blinds put up in my house, so I called up the company. There was a 15 minute wait, so I chose to leave a message and have them return my call. Their virtual assistant called me back. I answered and, after the first few syllables, I could tell immediately that it wasn't a human. Way too bubbly for a human that answers the phone dealing with customers all day. So I got through scheduling the appointment and when the call came to an end, it asked me if there was anything else "she" could help me with. So I asked if she was human. It said no, she was not, and asked if that mattered to me. I said no and it said "Well I'm glad I could help you!" in such a bubbly voice that I found myself smiling. Now I want to talk to her again.

RS

We're surprised she said no. But when you get to that point with a virtual assistant, we believe that's a green light to mess with them as much as possible. We're open to suggestion on the best ways to do this, but we imagine there are some secret commands that could result in all sorts of fun or perhaps some questions that yield surprising answers. In your case, we suggest ordering more blinds at the company's busiest time so you can avoid humans and have another conversation with her. Let us know how it goes.

Dear *2600*:

My wife received an email from PayPal saying she needed to call before $600 was taken from her account. She doesn't use PayPal at all, and checked all of the links to be sure they were legit. She did make the mistake of calling the number on the email, and the person was remote and was trying to force her to basically go through the two factor authentication process on her phone. He said that the URL version would not work. She immediately hung up and logged directly into PayPal to see that nothing was being charged (duh). So this is where it gets strange. I had her get the source of the email and send it over. The *only* thing that was off was the subject line "Billing Department of PayPal updated your invoice." Every link, image, etc. all went back to paypal.com. The *only* thing off was the phone number. Googling the 888 number returned no results. That number was *not* listed on their website anywhere. Went through the headers and *everything* checks out. They all came from an IP that is at paypal.com. Icing on the cake: my wife called the real customer service number (from the website). The customer service representative confirmed no charges *and* said they were "aware of many of those types of emails going out." Obviously suspecting breach and using the internal mail relays somehow, but thought I had to have missed something.

JS

We doubt the rep was inferring that these emails were coming from PayPal, but rather that lots of these scam emails were going out from somewhere and that they were aware of them. The 888 number was obviously the scammers' method of getting information from people. It's likely they were able to capture your phone number even if Caller ID was blocked, as toll-free numbers use ANI (Automatic Number Identification), which is much harder to suppress on the caller's end. But it sounds like the two of you are well prepared for any scams that come your way.

As for the lack of smoking guns in the headers, we suspect there are more headers you didn't see. Make sure you expand them on the system you're using so you can read all of them. Often, we find a weird IP or a strange domain name after looking several times because it can be easy to hide these in plain sight. If scammers have figured out a way around this, it would be really big news.

Dear *2600*:

Growing up in Queens, New York, we didn't consider ourselves poor. But we certainly had rules to follow when it came to buying things and spending money. One of my dad's pet peeves was putting dimes and then quarters into a payphone. It just wasn't tolerated. So to combat Big Bell, my parents taught us to call collect and ask for Joe Smith. The operator would simply make the call, ask for Joe Smith, explaining that there was a collect call for him. The receiver - me, my dad, whoever was home - would always just answer, "Sorry, Joe is out, can I take a number to return this call?" Of course, the NYNEX operator would give out the phone number from the payphone as a courtesy . A half a minute later and a call back. Anyway, I'm sure others have done this. I guess, after all, it was a hack.

LG

And a hack that virtually nobody had a problem engaging in, from young to old. In the end, it was all about deceiving the phone company and communicating for free, something hackers and phone phreaks continued to do using various other methods, such as the one in this next letter.

Dear *2600*:

My mom just told me about a way boys and girls would meet in the time of rotary phones. They would dial random numbers until they got a busy signal, then shout "boy boy" or "girl girl" between the busy signal beeps, then shout their phone number between the beeps. Crazy stuff I didn't know about until just now.

JP

While we've never heard this specific tale, we have heard of certain busy signals where such things were possible and, since calling a busy number didn't cost anything, people from all around the world would call numbers that were always busy and carry on full

conversations in between the busy signals. Calls didn't time out in those days so these crazy conversations could go on indefinitely. (We don't think it's likely that random numbers were used since that would greatly reduce the chances of connecting with someone else who called the same number.)

Another popular method of connecting for free was calling a "loop number." These were special test lines run by the phone company that didn't "supervise," meaning they didn't cost anything to call. Each of these loop numbers had another number attached to it. One person would call one of them, another person would call the other, and the two would be connected.

Talking to people on the phone for free used to be a really big deal.

Unsatisfactory Service

Dear *2600*:

Well Rogers, this is unacceptable, especially after last weekend's massive screw up. I got my Rogers bill today, and expected to see a credit for five days' usage like the Rogers CEO said that everyone would get. I just have unlimited talk and text for Canada and the monthly bill is normally $28.25. Imagine my surprise when the bill said I owed $31.08 - roughly a 10 percent increase over my normal bill. The total of my bill includes HST. My bill is normally $25 plus HST which brings it to $28.25. Five days off my bill should be around $4.17 or a bill of $20.83 plus HST would equal $23.54. Instead they want $7.54 more. I'm a pensioner and don't need to be supporting Canada's "most reliable network" so they can appease their larger customers with better rebates.

John

We honestly can't say we're surprised by this. Phone companies often raise their prices right when they're supposed to be giving out credits. However, it's also quite likely that the credit in question hasn't been processed yet, since you wrote this mere days after the massive Rogers outage back in July (which is a story worth reading about for those who are unfamiliar).

Article Submissions

Dear *2600*:

Here is an article on Python.

S

Dear *2600*:

I'm sorry but I'm sending in a second draft. I found some typos and errors....

S

Dear *2600*:

One more update.

S

Dear *2600*:

(This should be the final update. Again sorry.)

S

Dear *2600*:

(sorry more errors needed to be fixed)

S

Dear *2600*:

There has to be a better way to do this. I think this should be the final, and I hope you accept.

It would be very nice to hear from you at *2600*.

S

Dear *2600*:

Fix 4 !!!

S

Dear *2600*:

Please cancel my submission, I'm just going to put up a GitHub page.

I can't wait for you to decide without a response.

S

We should point out that the first of these was sent at 6:48 am on a Monday and the last at 7:55 am on the same day. We appreciate the fast forward lifestyle that's being demonstrated here, but that's not the world we operate in. The first email would have generated an auto-reply which explains our process to the sender. All articles are looked at and, if they are accepted, we will contact the submitter at the email address they provide. All of that is not going to happen within an hour. We're a quarterly printed magazine, not a web page. Fortunately, most everyone who does get an article printed seems quite happy with the experience.

The address to send your article submission to is articles@2600.com.

Dear *2600*:

I would like to submit an article that contains several LaTeX formulas and two figures in SVG format. What is your preferred markup format for article submission?

The article was composed in Org Mode, so the text will be easy enough to convert. My main concern is whether the formulas will render correctly or if I'll need to adjust them before making a formal submission.

Alphox

We can accept most any format but, as we've learned over the years, sometimes formats don't translate properly when emailed. So if there's a specific look you want printed, sending an image or a PDF that shows how it's supposed to appear would be your best bet. This would be in addition to sending in a format that we can edit, like a simple text file.

More Questions

Dear *2600*:

I have a question for all my *2600* brothers and sisters out there, and I would really like their opinion. Since about 2004, I have had this dream and I would like to share it with all of you.

First off, am I the only techie in this universe that thinks that copper is too slow? Copper to the CPU, copper to the RAM, copper to the North Bridge, copper into the South Bridge, copper what? 6ghz? I don't know - maybe 8ghz, 10ghz CPU speed? Ladies and gentlemen, no matter what Intel, AMD, ASUS, Gigabyte, MSI, AsRock, or any other manufacturers claim, signals of any kind over copper will always be too damn slow. I emailed all of them about this - no reply.

Enter my dream: I would love to see a fiber optic ring on a motherboard instead of copper. For years and years, scientists have been able to manipulate data over fiber. There have also been adapters created to allow copper signals to transform into fiber signals.

So in the beginning, adapters may need to be used to tie everything together, but my dream goes farther. Fiber CPU, maybe just two versions, a "home" for the everyday user, and a "professional" for the business folks. A fiber CPU as fast as, say, the speed of light! Fiber RAM, instead of sticks like we use today. These would connect to a fiber socket in the form of a module, say 1tb? 5tb? Maybe even 10 to 100tb! Fiber SSDs, that's right! Connecting a fiber SSD to a fiber ring so the manipulation of all files can be done at the speed of light. Fiber video, oh yeah! No more three ridiculously large fans to keep the damn thing cool. No more foot long video cards we have to find some way to fit into our cases! It would be similar to the fiber RAM module, and it would connect directly to a fiber CPU from a fiber ring. This would include the capability to use, say, one to 100tb of graphics RAM. Fiber NIC, yes sir, with a connection like this there would be zero bottleneck from an ISP to a PC because it would be all fiber! And one more thing, with fiber, none of us will have to overclock anything to get the best performance out of our box! And less heat means no need for liquid cooling! And no, this is not science fiction.

If I had Elon Musk's money, I would already have a working prototype! You all may think technological insanity is present here, but I ask you, why should all of us settle for building a second rate computer to make these corporations filthy rich? Why should we accept anything less than the utmost performance we can possibly get out of our build? Why are we all accepting turtle slow computer speeds when we could have fiber, and compute at the speed of light?

I am not a scientist, but I am a technology enthusiast. And I am asking all of you to simply imagine what the computer scene would be like if we could all upgrade our machines to fiber. I expect negative feedback on this, but that will not deter me from dreaming of the greatest computer mankind can produce, if only they try.

Thanks to all for reading my dream. Hack the universe and long live *2600*!

Martin
Lifetime subscriber

We certainly don't doubt your enthusiasm, not for a second. And we look forward to hearing what others think about all of this. We should also point out that this entire letter was submitted to us in decimal format, which we had to convert to ASCII. No big deal, but if that's how you communicated with all of those companies mentioned, it could explain why they never got back to you. They don't have nearly as much fun with this stuff as we do.

Dear *2600*:

Anyone still have one of those little Radio Shack recorders? I'd love to see if it works. Also, y'all ever did that old paper clip trick back in the 80s? I can attest it really worked.

J

The Radio Shack modified tone dialers are still in some people's collections, but they no longer work, as the payphone system of that era hasn't been in operation for years. (The modification would allow red box tones to be emitted, which would fool the payphone network into thinking a coin had been deposited.) As for the paper clip trick, that goes back even further to the era of payphones that didn't give you a dial tone until a coin had been deposited. The paper clip in the mouthpiece would bypass that restriction, making a free call possible.

Good times.

Dear *2600*:

Are you familiar with disaster.radio? It seems pretty cool!

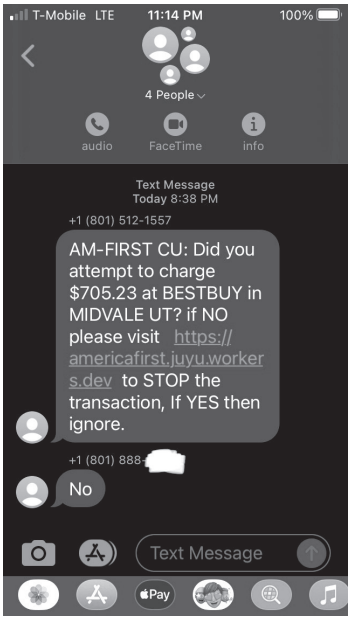
FS

According to that website, "disaster.radio is an off-grid, solar-powered, long-range mesh network built on free, open source software and affordable, open hardware." We're quite fascinated with the concept and believe it will become quite useful in the future. We hope to hear more on this.

Dear *2600*:

This is a little strange. I received a typical text message scam that was trying to get me to click on a link, but it appears to have been sent to me and three other people as a group text. I have never seen them do that before. Here is a picture (phone number of person who responded has been partially redacted).

N1xis10t



This just screams "scam" on so many levels. We don't know what the advantage of texting multiple people is, unless they're somehow part of the scam and can get you to respond to them. Often, simply knowing that someone will answer is enough of a payoff. But certainly visiting that website would be a very bad idea.

Dear *2600*:

Total newb question here: If I just found a 0day, what is the best way to maximize fame and profit?

GH

Based on how you phrased this, you may have to choose between one or the other.

Dear *2600*:

Has anyone had luck getting places (gas stations, convenience stores, etc.) to let you remove and haul away the old phone/phone booth that's still on their property, unused? Gas station near me has a real nice aluminum booth with no phone, just chillin'.

Marty

It can't hurt to just ask. There are all kinds of circumstances that could be at play. They may have an existing contract with a phone company or it may not be something they have anything to do with which is handled by some other company. Or they could have a useless structure taking up space which they would love to get rid of. Just remember those things are a lot heavier and bulkier than many people imagine.

Dear *2600*:

It would be handy to know file sizes for the individual talks for people (not me) who have limited data service. Just my $.02 worth.

TG

Sizes vary depending on quality. Some of our talks from years ago are about half a gig per hour while talks from today can be several times that. These are pretty standard sizes for what we offer.

Dear *2600*:

I hate to bother you, but I am wondering why my IP address is 2600: followed by more digits than standard. I am certain it is nothing big, probably a coincidence or my shared love in vintage phones perhaps. Maybe it is my positive stance towards FSF ideology, or EFF and their great works which is a shared view, I hope. Hopefully there is a shared view in the importance of free expression and unhindered free speech accepting no amount of money to change? Anyways, it must be a sign from the AI Goddess Afrodotty to share those magic numbers 2600 with you.

Justin

You have an IPv6 address, as opposed to the more common IPv4 (which you likely also still have). You are quite lucky to have gotten the 2600 prefix - we would have killed for that.

Dear *2600*:

How long will it be before thieves come by in the middle of the night and siphon the power from your car battery instead of your gas?

JC

At least it won't make very much noise.

Dear *2600*:

For some reason, the video game *Polybius* has popped up in media several times in the past few years. I personally do not remember it as a child of that time, being only six years old when it supposedly came out. But I think I remember seeing it as shareware in the early 90s.

(It might be from an old Slackware 2.2.2.0(?) distribution from 1994 that I'm remembering this game. I've still got the CD-ROM set in my storage locker, but I'm too lazy to verify physically. And I deleted the .ISO of the disks from my file server many years ago.)

I'm hoping you or someone has access to an archive of old back issues and articles and can tell me which issue if any has the first mention of this software title.

I thoroughly enjoyed your magazine and culture so much back in the early 90s; I would drive 60 miles to get the nearest new issue. There was one other magazine similar back in the day, but I don't even remember its name. I figure if anyone has an accurate record of anything to do with this title, it has to be *2600*.

Thanks for your help.

Ryan

That game is apparently part of an urban legend that spread in the early 2000s. The arcade game itself was said to have come out in 1981 in a very limited region and was rumored to cause all kinds of nasty side effects like hallucinations, amnesia, and seizures. On top of that, it was said that men in black would come and take information from the machines. And then they all vanished. Today, the whole thing is thought of as fiction.

One interesting sidenote to all of this centers on the name Polybius, which was that of a classical Greek historian. He was known to have said that historians should never report what they cannot verify through interviews with eyewitnesses.

Needless to say, we were unable to find any mention of this game in our pages.

Dear *2600*:

Am I at the correct spot to place a subscription?

(null) (null)

No, you're in the middle of the letters section. We don't know how you got here. But what you want to do is get back onto the Internet and navigate over to store.2600.com, where you will see a sign for subscriptions. You can't miss it.

Meeting Updates

Dear *2600*:

Was wondering when and where the meetings are in Los Angeles. I saw on the site under "California" the San Francisco meetings, but no Los Angeles.

Was hoping there is a meeting and just not listed.

Peter

We have yet to hear details and there is clearly a demand for them, as the next letter shows.

Dear *2600*:

The Los Angeles *2600* Twitter is absolutely inactive. I heard you guys were meeting, but no one showed up. I never got news of the meeting and I really want to join.

I think you guys should announce on Twitter if you want people to come. Could you please send me more information?

Why has there not been any announcements that the group is still going?

Qmark

We need to point out that meetings are not run remotely by us. They are organized by people who are local to the community. When we hear from such people (email meetings@2600.com or direct message to @2600Meetings on Twitter), we generally print the info, assuming it meets with the guidelines that can

be found in the Meetings section of our main page at www.2600.com.

With that said, any of the people who have been writing to us asking why there aren't meetings in Los Angeles could become the organizers by picking a place and letting us know. We hope to see this resolved soon.

Dear *2600*:

I'm from Mexico City and remember there used to be a meeting but apparently not anymore and I am willing to start one. How can I do it?

Mardonio

Simply picking a fairly easy to get to location in a public area, preferably on a Friday late afternoon/early evening, is all you have to do. Of course, you also have to spread the word if you want people to show up. (This includes telling us, using the methods outlined above.) We do hope to see a return of meetings in Mexico City in the near future.

Dear *2600*:

About the 40 percent vaccination rate - didn't you get the memo from like five years ago? That shit was a hoax and the fake vaccines are what are making everyone sick right now. Derp.

J C

A reminder that sometimes meetings will attract people with a distorted view of reality. Please treat them with patience, but remember that you don't have to talk to them.

Dear *2600*:

The fact that you stopped them in the first place tells me that there is no intelligence left in the HPVAC community.

J C

Yes, so perhaps our little group is not up to your standards. Maybe there's a nearby Mensa meeting that would be a better fit.

Dear *2600*:

Hello - I am attempting to contact the San Francisco *2600* meeting. I was in their Google group, but somehow lost contact or connection. Please help.

Hack the Planet.

Mad Glitcher

We don't give out contact info for any meeting participants and we're not seeing an online presence for this particular location. Fortunately, they are having monthly meetings, so you may have no choice but to show up.

Dear *2600*:

Today we met from 5 to 8 pm at the Barnes and Noble in Boca Raton, Florida. We had six attendees come to the meeting. One of the attendees was a new attendee who drove up from South Beach for the meeting!

We had a great time! It was a beautiful sunny day. We sat outside in front of the Barnes and Noble at the tables. There was a random man playing saxophone in the parking lot nearby. We exchanged different hacking stories and made new friends. All of us were excited about attending DEF CON 30 and were making plans to meet while there.

Boca Raton *2600*

Thanks for that uplifting report and welcome to the list of meetings!

Dear *2600*:

I was wondering if Delaware still had *2600* meetings? I would love to start it back up if that isn't the case.

k3ma5

We used to have meetings in Newark before the pandemic. You're more than welcome to restart those or pick another city. Please keep us updated.

Dear *2600*:

Writing in from Philadelphia, PA to ask if there are still meetings in the general Lancaster, York, Reading, Harrisburg areas. I just took an Amtrak from Philly to Lancaster for $21. That seemed extra cheap for the weekend. I grew up in Lancaster and know some hacker heads from growing up in the area.

pic0o

As of press time, we still only had the one Pennsylvania meeting in Philadelphia. We hope to see the other cities get restored in the near future. All it takes is someone to step forward and do the coordinating.

Dear *2600*:

We had last night our first *2600* meeting in Madrid in 20 years. It was only a few of us, but we were there between 5 and 8 pm. We had tons of fun talking in person about hacking culture and today's world. Hopefully you guys can list it on the website so people see it is official so we can post it around and get more people to come.

Happy Hacking.

ReK2

It is indeed listed on the website, on the meetings page in the magazine, and now here in the letters section. We look forward to seeing this meeting continue to grow.

Dear *2600*:

I am a student and my major is artificial intelligence at Houston Community College. I want to join the *2600* club at the Agora Coffee House.

Yu Zhang

All you have to do is show up at that location where the monthly meetings are held on the first Friday of every month starting at 6 pm. There is no club to join and it's quite informal.

Observed

Dear *2600*:

I just wanted to say to you fine folks (and whoever might read this in the magazine) that I deactivated my Facebook account and "removed app updates" from my phone. Apparently, their app is "native" software on my (and I assume other) builds of Android. Why would any tech company bundle another's software into the OS their device runs? Meanwhile, you guys have a good one, and keep your stick on the ice.

E85

This is because of deals made between the smartphone manufacturers and Facebook. We agree that it's a bad move and quite likely to steer a lot of people away from Android as a result.

Dear *2600*:

Sometimes they're just asking for it - BMW making people pay a monthly subscription for heated seats and other upgrades.

John

This is exactly what many of us feared with the growing normalization of non-ownership of the things we buy. Having to pay a monthly fee for software we used to own outright is the same concept as what you're describing here. It's insane to us that something which exists in your car has to be paid for every month only because the manufacturer has the ability to turn it off. That seems more like a protection racket.

Dear *2600*:

This hacker "movie" called *H+ The Digital Series* is probably not on the radar for many readers. It's actually a series of web shorts, but with high production values. There are 48 episodes at about five minutes each. Watched back-to-back, it is a great hacker "movie."

ihtarlik

There must be a ton of similar projects. Thanks for alerting us to this one and we invite readers to let us all know about more.

Dear *2600*:

I am a prisoner, and it should come as no surprise that the tech provided to us is antiquated, yet we can get things like cell phones smuggled in. I though I'd share our equipment with you.

Aside from contraband cell phones, we have Swintec 7000 typewriters here at the federal prison in [redacted]. The prison provides them for free to check out to prisoners. They have been providing the wheels for free (comes with the typewriter check-out), but these break easily and prisoners complain about bad wheels. Our "store" will soon be selling these for an undisclosed amount, and will no longer provide them for free. The ribbons cost $9 and are good for about 40 to 50 pages of double-spaced output. We also have to buy correction ribbons, though these are 90 cents and can be reused. They last a long time.

We used to have the same model typewriters as above, except they had a factory mod that enabled onboard memory and had a 20x2 screen (I'm not 100 percent sure on the size). Then the staff figured out some guys were saving homemade erotica instead of legal work, and the prison switched to the model with no screen/RAM.

We have access to a Windows XP desktop with a CD-ROM drive and no Internet access. Prisoners need to have received a CD-ROM with evidence files from their lawyer (certified by prison staff as having been sent by a lawyer) to use this. It has no printer, so one must take notes in order to fight their case.

We have access to TRULINCS, which other prisons and the public see branded as Corrlinks. It allows us to submit electronic requests to staff, refill medications (when Health Services staff input the refills), manage our prison money, buy MP3s (they sell us SanDisk MP3 players flashed with a special firmware), read the "bulletin board," and send "emails." These contain no typing functions, per se. However, I can type a book, for instance, and the email recipient can receive this, print it at home, and mail it wherever. I have used this for book chapters and legal briefs. Some guys write book chapters for self-publishing and just send them to staff members who are known to never check their email. The prisoner can then print a paper copy of the message at the law library (where the printers are).

We used to have a computer lab with thin client workstations pre-loaded with the basic MS Office apps (Word, Excel, PowerPoint), but one warden showed up and was afraid we would "hack the computer chips to get on the Internet." We have some smart guys, but this seems pretty far-fetched.

Rumor is that we're getting tablets around Christmas. We have to buy them, but at least they will be Android. More info on them is at keefegroup.com/products/score-tablet-169. The advertising copy for these tablets make two contradictory statements:

"Firmware that cannot be replaced by anyone - even the Secure Device manufacturer."

"Upon release, offenders can ship the device back to Keefe and pay to have the security software removed."

In short, they flash special firmware for use while in prison, then flash standard firmware for post-prison use. We look forward to testing whether the firmware cannot, in fact, be flashed by anyone. Since we have access to rooted phones (WebADB and a USB-C to USB-C cable), we'll soon see how tough these things are.

A

Thanks for this fascinating glimpse inside the walls. We masked some specifics as it's been our experience that prison officials aren't too keen on any info of this kind getting out to the public, and often take action against anyone they think may have been responsible. But this is proof that no matter what the environment, the hacker spirit will prevail, through experimentation and the spread of information.

Dear *2600*:

I started answering every scam and spam phone call in a wicked rough voice I can do and told them "Hello! How can I trace your call today?!" They hang up and *never* call me ever again!

Kyle

And that's only one idea.

Unique Opportunities

Dear *2600*:

Good afternoon. Recently I have directed you a required archive. Have you seen it?

rlazania

How do you even answer a question like this?

Dear *2600*:

Not to brag, but Janet Yellen sent me a personal email. Surprised she's not using her government email address though. Oh well, I'll send her my details.

AM

We get at least one email a day from well known celebrities. It's very rude not to respond or to give them the info they ask for, like account numbers and PINs. We understand how boring it must be to exist in

the limelight, so we're happy to do anything we can to help them get through the day.

Dear *2600*:

Could you monitor one of your channels for unauthorized access or deletion/archive non transmission. Priority high and nature critical for streaming server?

Brian

Pass.

Dear *2600*:

Greetings from the Illuminati world elite empire, bringing the poor, the needy, and the talented to the limelight of fame, riches and powers, knowledge, business, and political connections. This is the right time for you to put all your worries, your health issues, and finance problems to an end by joining the Elite Family of The Illuminati!. Are you sick, barren, or having divorcing problems, finding it difficult to get job promotions in your place of work in order to excel in life just like you wish? If *yes*, then join the Illuminati empire - you will get all this numerous benefit and solutions to your problems.

Note that this email message was created solely for the purpose of our recruitment scheme which will end next month and this offer is for unique ones only; if you are not serious on joining the Illuminati empire, then you are advice not to contact us at all. This is because disloyalty is highly not tolerated here in our organization.

Note: Some email providers incorrectly place official Illuminati messages in their spam/junk folder or promotion folder. This can divert and exclude our responses to your emails.

The Illuminati

Oh yeah, this is exactly what we needed. We wonder if these folks even know the history of the Illuminati. We're fairly certain most secret societies don't send out mass mailings for recruitment. We're also certain we would be "highly not tolerated" if we did join them.

Critique

Dear *2600*:

While the events in Ukraine are complex, I myself am wondering where the due diligence of *2600* went! It seems as if it went out the window when the world was turned upside down by Trump's election, horrific as that was. Unfortunately, and quite unexpectedly, the crew at *2600* seem to have fallen in step with the official government line/narrative.

Me

We're not going down this rabbit hole and we're not going to serve as a source of misinformation by spreading perspectives that have the effect of lending support to what Putin has been doing in Ukraine. What many people fail to realize is that occasionally we will reach similar conclusions as those we normally distrust. That doesn't mean we're now working with or for them. Our conclusions are based on journalistic evidence from multiple sources all around the world. Not that this will make a difference - we'll undoubtedly be told that all of these journalists are also just spouting the "official" narrative.

What led to this terrible situation is indeed nuanced and can be discussed and debated when we have that luxury. But for now, the priority is stopping the horrible acts being perpetrated on Ukraine.

We encourage people to examine the reporting that's coming out of the region which isn't controlled by any government. But if you're basing your conclusions on who you agree or disagree with on other matters, then you're not actually thinking for yourself.

Dear *2600*:

Curious as to why so many "hackers" are now pro-government and pro-authoritarianism when hackers are essentially a group of folks that have been historically against the grain, against having people telling them what to do and essentially partake in illegal activities. Can you be a hacker and pro-government?

Joe

You need to give some examples so we can properly answer your question. There have always been people with hacker skills who work for governments and corporations. There's no reason why such people can't also be recruited for authoritarian regimes. We don't consider them to be a true part of the hacker community since they tend to stay within the environment that's sponsoring them. But we don't get to unilaterally decide. If you're referring to hackers who reach a conclusion on a particular issue (vaccines, wars, insurrections) that happens to be in line with what certain governments are saying as the letter writer above did, that's an unfair characterization. And we can easily make the same accusation about anyone who says this, as there are other governments that take their side as well. In the end, it's all about analyzing the facts, sifting out the bullshit, and being open to discovering that you're wrong. Way too many people reach conclusions because others tell them to or because someone they dislike reached the opposite conclusion. That's not independent thought. It's Manipulation 101.

Dear *2600*:

Can anyone just completely get rid of the WebP format? I'm sick of copying images and pasting them to PaintShop, to save them as JPEGs to share a laugh. Whoever at Google added an extra step is a virus. It stops nothing, it just makes it stupid.

JM

But it's tradition.

Advice Needed

Dear *2600*:

What would you do if you were helping a family member who was completely ignorant of technology but wanted to live in the modern world? And refuses to learn? My cousin is a successful nurse, but outside of basic computer apps for work is really ignorant and I've been trying to help her but it's really frustrating.

1. Doesn't know how to pay her rent online. She paid me $500 to pay her rent online. Her condo doesn't take checks. Oh, and when we tried to use her Kindle,

she wouldn't let me use my phone as a hotspot because she was worried that my phone would "steal" her data. Her phone was broken.

2. Wanted to log into an old Kindle account she had since college. "Thousands" of dollars of purchases on her account. Can't remember her email address or password. Embarrassing trip to Best Buy, her looking and acting like a crazy person demanding staff to get her purchases back and get the email address. Oh, and when we finally got in, neither email address had any books on it.

3. Relies on handwritten passwords on 3M notes in her purse. Uses easily guessable passwords. Was pissed off that sites wanted complex passwords now. Refuses to use a password manager.

4. Wants to use prepaid credit cards, but doesn't want to use her SSN. Before you could get away with it, but now there is so much fraud. Every time I try to help her, I just end up frustrated and my family calls me an a-hole if I don't help her.

DH

You are not the person to help her. You seem more interested in demonstrating how out of touch and ignorant your cousin is, rather than respecting her not unreasonable choices. This attitude is something we see far too often and it's a much bigger problem than people who don't want to always learn about the latest technology.

It's absurd that she can't pay her rent with a check. It may even be illegal, especially if it's not specifically mentioned in the lease or if they charge a "convenience fee" for paying online. But one option might be to have her bank do an auto-pay each month. That can be arranged on the phone or by visiting them - no logging in required.

It's actually quite smart not to connect to untrustworthy hotspots. Yes, your cousin believes your hotspot is untrustworthy. On this, she's employing more security than you're comfortable with.

People forget their passwords and email addresses all the time. Shaming them does nothing to help this. And you think it's crazy for her to want access to the items she's bought over the years? If Kindle deleted her ebooks, they're the ones who are wrong, not her.

Not using a password manager is a perfectly valid choice for someone to make. If, for whatever reason, it becomes compromised (which is absolutely not impossible), then all passwords are compromised. And many sites really overdo it with the password requirements, especially those that are basically throwaway accounts. For the more important ones, stronger security should obviously be used. As to where people keep these passwords, that's up to them. Keeping them in her purse may very well be enough security for her. Telling you about it wasn't wise, however.

And you're actually going to criticize her for not wanting to give out her Social Security number for a prepaid credit card? You seem willing to accept this, on the other hand. This just demonstrates that everyone has their own view of what security is, as well as when and how much to utilize it. Expecting everyone to share your methods and values isn't the way to get more people onboard.

We hope your cousin taught you something about different approaches to these challenges.

Dear *2600*:

I'm a member of a hackerspace whose name will remain anonymous. I've found that the space I'm a member of is more into making electronics and 3D printing and laser cutting. I feel like I'm the only peep that is into security hacking. I feel like it's just me that is into CTFs. I'd like to hold a CTF, but don't know how to approach the committee about it or if it would even be successful. I appreciate *2600* and the Facebook group makes me feel less alone.

BA

That's the key - to remember you're not alone. Not knowing details about your hackerspace, we can only assume that they will be supportive of any idea that involves hacking without any illegal activity. We suggest researching other Capture The Flag projects and coming up with a game plan for running your own. It will be an uphill project, but that's not something you should get discouraged by. If you take your time and learn as much as you can before embarking on this, you'll be the one teaching everyone else. And, just like with every other project that exists in your hackerspace, it won't be perfect the first time. You will develop more skills with every attempt. Good luck.

Dear *2600*:

Hey, I am hearing voices in my head like a thought logger. I've looked up information on this and all I can find is CIA Stargate or microwave guns or psychosis or voice-to-skull or gang stalking. I need help.

zybe

We get quite a few letters like this. We're not really qualified to address the issue, but we can say that knowing you need help is an excellent first step. There are known medical conditions that can cause these symptoms. Very little can be gained by assuming this is the result of some sort of mind control experiment, a nasty neighbor, or some other intentional source. rethink.org is a well regarded website that addresses these issues and can probably point you to ways of getting help.

Responding

Dear *2600*:

I was just reading through 39:2 and saw the letter from "Richard" about search engines not providing the results he wants.

Richard, you should know that search engines provide the results that the advertisers want first, as they pay the bills. If you're not paying for it, you're probably the product.

c/p

The original letter was complaining about not getting search results that were related to what was being searched for. We assume this is in addition to annoying ads and promoted placement.

Dear *2600*:

Been a subscriber, OMG for 26 years! (Geez, I'm

old.) Anyway, saw all the letters from people making sales pitches in the 39:2 edition. My sympathies. In my job as an IT security professional, if I make it through the day with fewer than three sales pitches, at least one by telephone, it's been a good day for me.

The sales pitches run the gamut from promises of free swag (I've tried to score stuff in the past - somehow after listening to the pitch I don't get my shiny new headphones or tickets to an entertainment event I have zero interest in, yet was promised), to guilt trips ("Why don't you respond? This is very rude!").

Anyway, just thought you'd enjoy knowing you aren't alone. (Maybe one day someone can start a website of "tedious cold calls we wish we never got." I could fill a volume (and a book shelf!) with stories. But who would read it? It's tedious.

Michael

Congrats and thanks for sticking with us for so long. The spam situation - whether by phone or email - is indeed crazy, but that doesn't mean we can't have fun with it. We always like to hear suggestions on that front.

Dear *2600*:

"Brute-Forcing a Museum's Math Puzzle With Python" was fun to read since I've done the same thing with a different more difficult math puzzle. But this puzzle is pretty easy to solve the traditional way. Here's a solution method for the author and readers. The puzzle is a 3x3 grid you fill with numbers 1 through 9 without repeating any of them. Then four math equations embedded in the grid must hold true. The author notes they can be expressed as:

1: A - B = C
2: D ÷ E = F
3: G + H = I
4: C x F = I

You immediately know 1 cannot be in equations two or four since C x 1 = C and D ÷ 1 = D, violating the no repetition rule. The next clue is that multiplication and division will be much more limited than addition and subtraction, i.e., it's much easier for two numbers to multiply greater than 9 than to sum greater than 9. So let's examine equations two and four. C and F can't be 5 or higher, because 5 x 2 (the smallest possible multiplier since 1 is ruled out) equals 10 - too high. Therefore, C and F must be 2, 3, or 4. Since 3 x 4 exceeds 9, we know one of them must be 2, and then the other will be 3 or 4. That means I must be either 6 (2 x 3) or 8 (2 x 4). Similarly with equation two, E and F must be 2, 3, or 4, because anything higher would require D to be greater than 9. One of them must be 2, because if E and F were 3 and 4, then D would be 12 - too high. Now we know that F must be 2, since that's the only way it can satisfy the constraint of both equations two and four having the number 2. We also know D must be 6 or 8, since those are the only numbers that can divide into 2 without repeating 2 in the equation. Our equations now look like this:

1: A - B = C(3 or 4)
2: D(6 or 8) ÷ E(3 or 4) = 2
3: G + H = I(6 or 8)
4: C(3 or 4) x 2 = I(6 or 8)

This means A, B, G, and H must be some combination of the remaining numbers 1, 5, 7, and 9. Thus, equation one is subtracting two odd numbers, which always results in an even number. Therefore, C cannot be 3 and must be 4. The only two unused numbers that subtract to 4 are 9 - 5 for A and B. Since 4 is used up by C, E's only remaining option is 3. Equation four is filled out to solve for I: 4 x 2 = 8. And similarly, equation two is filled out to solve for D: 6 ÷ 3 = 2. We have two unsolved variables G and H and we have two unused numbers 7 and 1. Adding 7 and 1 gives 8, satisfying equation three. That gives:

1: 9 - 5 = 4
2: 6 ÷ 3 = 2
3: 7 + 1 = 8 or 1 + 7 = 8
4: 4 x 2 = 8

David M.

It really turns heads if you read this out loud very fast.

Dear *2600*:

I am reading William Ben Bellamy Jr.'s password making guide ("The Problem of Effective and Usable Strong Passwords" in 39:2) and I am scratching my head. This kind of nonsense has been disproven long ago. I'm sure he's never read *xkcd* or seen the "Correct Horse Battery Staple" issue, but rest assured his advice for passwords is terrible.

It suggests using not-so-random "random" phrases that can be picked up by reconnaissance, either SIGINT or OSINT such as MAC addresses, serial numbers, years of favorite movie. It also suggests low entropy sources like unaltered user keyboard presses. Those can all easily be found.

To further confuse the user, he recommends using l337 sp34k and adding random Unicode characters, which are hard for someone to remember. He also doesn't note that mutators either stand alone, or built in JtR and hashcat ones will automatically generate extra-guesses for these. They don't add much additional entropy, but make the password harder to remember. And Unicode might never have been in a password guesser's mask or dict, but you won't be able to type it on most keyboards if it's obscure. It's also going to be an absolute pain to remember.

Of course, if you are using a password manager or some other scheme where you don't have to remember a password, just make it as long and random as absolutely possible.

The correct answer for passwords is easier: just let your password manager do it for you. KeePassXC runs on all modern platforms, and lets you generate strong random passwords among many criteria.

Random words? You got it. Long string of random characters? Yep. Can you pick the character sets and exact characters to include? Yep. Can you exclude lookalikes and ensure "one from each group?" 100 percent. Does a modern computer (at least Linux) have a high quality pseudo random number generator (PRNG) that is better than you? Yes, yes, and more

yes!

GI Jack

This is clearly a very sensitive subject that has a number of different approaches. We'd like to hear more of them.

Dear *2600*:

I was delighted when I saw that my article "Dial-a-Word" had been published in the Summer 2022 issue of *2600*. When I read the published version, I was satisfied with the edits that were done to the article, and found that they greatly improved the clarity and flow. There is one problem however, as the included computer code was stripped of all indentation, and is missing a carriage return on the last line. This appears to make it fit better into the magazine, which is nice, but the code is incapable of running in this state. I have published the program on GitHub with proper formatting, and if anyone wants to use and/or modify the program, it is located at github.com/n1xis10t/dial-a-word

In case anyone was wondering, it is written in Python 3.

N1xis10t

We've gotten a number of letters about this and did some investigating. The code was actually stripped of formatting during the email process, which we've never seen happen before. The issue with Python is that the formatting is part of the program and, as you say, it can't run without it. We can prevent this sort of thing in the future if article submissions indicate the need for formatting and/or include an image or PDF where the formatting will be visible so that we can reconstruct it if necessary in the text. Oftentimes, simply adding the code as an attachment will suffice.

We're sorry this happened and are thankful that you quickly provided a solution.

A New HOPE Feedback

(Note: These letters were sent as feedback for A New HOPE and, as is our tradition, we thought they would be of interest to readers. Since we didn't explicitly tell writers that these comments might be printed, we have omitted names.)

Dear *2600*:

I attended HOPE in 2018 at Hotel Penn. My complaint was the slow elevators. It was a fantastic and different experience in a college campus setting in 2022. Although I missed the beer drinking, I'll give up that for a safe conference, especially these days with the world going crazy. I would suggest that if HOPE 2024 will be at St. John's University again, maybe you can offer a cheat sheet of food recommendations for out-of-towners since, as you mentioned, it's the most diverse borough. For example, for Chinese and Asian food - Flushing, for Indian, Filipino, and Tibetan food - Jackson Heights, etc. We want to give them a Queens foodie experience.

I really enjoyed the interview with Sophie Zhang, the closing ceremony, and the music performance.

Let's try to get more vendors next time. HOPE Security, St. John's University, and Hammond Ops did an excellent job to keep us attendees safe, which I am grateful for and appreciative of. You can count on me attending next time again.

Great HOPE folks, great speakers and respective attendees. You all do justice for our society and for the next generation. Keep up the great work!

A New HOPE Attendee #1

We definitely dropped the ball on food recommendations and that's something we'll work on for next time. Suffice to say, the area has a great deal of options within walking distance and an unbelievable number a five minute ride away.

Thanks for helping to make the event so successful. No matter how much effort we put into it, it's the attendees who make it all work in the end.

Dear *2600*:

I attended the conference virtually. The sessions I was able to attend were very good!

However, I did find it difficult to read some slides on my iPad. This was likely my own issue.

I believe there were more tracks than previously making it hard to choose. Hopefully, they are still available on YouTube.

A New HOPE Attendee #2

The split screen on most of the videos was an experiment, which we believed worked most of the time. We're always open to suggestions and alternatives.

Dear *2600*:

The live streams for the hope talks have ended. How can I watch the talks that I missed?

A New HOPE Attendee #3

Everything is now viewable on the Channel2600 YouTube channel and available without Google censorship on flash drives.

Dear *2600*:

Had a great time this weekend; I think the new venue will be great for the conference.

My only gripe is that the slides when in the venues were too small to read properly, and were not full screen long enough to take in all the information. If the speaker window was a little bit smaller when side by side it could help.

Many thanks for all the hard work you guys put in to make the conference such a success.

See you in two years' time.

A New HOPE Attendee #4

We're definitely going to work on improving this.

Dear *2600*:

I know that packing up for HOPE is far from over at this point, but I just wanted to take a quick moment and thank all of you for making this second time, in person, volunteering experience so amazing and welcoming. My only regret is not being able to offer more support, sooner and for longer.

I had an especially great time emceeing and super grateful for taking a leap of courage to volunteer with A/V (there will be no rats' nests in 2024!).

Special shout out to the core team that put in that 200 percent extra work to ensure everything was

running smoothly. I am wishing you all a "peaceful reboot" in the coming days and safe travels.

A New HOPE Attendee #5

It took a while, but most of us have recovered. Thank you for putting in the effort to help make everything work.

Dear *2600*:

Congratulations on a return to HOPE! Though there were major differences this time, it was a great con. Besides the great absence of the Hotel Pennsylvania, the only major drawback this time I believe was the lower attendance and related - less vendors than usual, etc.

But, I have to ask, is St. John's University expected to be the new long-term home for HOPE? Will there be any further scouting of New York City for potential other homes?

Of course, there is nothing that will ever replace the Hotel Pennsylvania, but perhaps there are other candidates waiting to be found?

Not to sour on St. John's University - it is a good venue, and with higher attendance I think its full potential can be unlocked - but it just doesn't inspire the same sense of adventure, mischief, and exploration that the old hotel does.

I don't have any researched suggestions to make today, but if it's something being considered, I can spend some more time thinking about this.

A New HOPE Attendee #6

It's a fair question, but it's also one that we've done a ton of research on since 2019, when it became clear that Hotel Pennsylvania was no longer in our future. We know the new location isn't the same, but that's exactly how the hacker community works. Technology changes, new toys come into existence, old ones fade away.... We believe a college campus within the boundaries of New York City is far more welcoming to a bunch of hackers than a commercial hotel could ever be. And St. John's in particular seems to really get who we are. From our point of view, we found them to be a fantastic choice and great to work with. The "sense of adventure, mischief, and exploration" is something that evolves in any space and we're certain we'll see that continue to develop here in years to come.

Regarding attendance, we agree completely. Remember that we intentionally limited attendance due to the lingering COVID problem. We didn't want to create a potentially dangerous situation, so we required masks and vaccines, which virtually everyone had no issues with. But we also cut off ticket sales and didn't sell any tickets at the door, which limited our attendance (and vendors) and made the whole thing a bit more of a struggle for us financially. For the future, having more people attend will be essential, but we expect that won't be hard to achieve based on the reactions from those who were there this year.

Dear *2600*:

I thoroughly enjoyed the conference (both attending and presenting). Congratulations to you all for pulling it off!

I was wondering if speakers receive a file link to videos of their talks. I would like to have a copy for posterity.

A New HOPE Attendee #7

We can certainly do this. If anyone who gave a talk wants a downloadable version (in addition to what's up on YouTube), they can email us here at the letters department (letters@2600.com), and we'll get their request to the right people.

Dear *2600*:

I was a virtual ticket holder for HOPE this year and it was just as great as 2020! I am planning to be in person in 2024!

My question: Can I buy a tee shirt? I can't find them on *2600* and I was wondering if I just missed the link or if they will be for sale online later?

Thanks for another great HopeConf!

A New HOPE Attendee #8

You weren't alone in not being able to find tee shirts - we couldn't find them for a while in real life, which is why they were delayed getting up on the store. Hopefully, you saw them when they were added. (If there are any left at the time of this printing, it's literally only a handful.)

We were quite happy with the relative smoothness of the virtual part of HOPE this year. This was the first time we ever had both a virtual and in person set of attendees. We hope to keep that going as well, since it's a great way to help pay for the conference without adding to the crowd.

Dear *2600*:

Congratulations on your conference. I desire to attend in the future - it really seems great.

Where should I look for details on online access or purchasing of video of the talks?

A New HOPE Attendee #9

It took a bit longer to process all of the video this time due to a new way of doing all that, but it's all done now. You can find full details elsewhere in the magazine and on our website. And we look forward to having you in attendance!

Dear *2600*:

This was my first HOPE and it was a blast! Wanted to provide super quick feedback.

The good:

- Live streams worked really well! It was nice being able to go back the same day and catch a talk I missed. The Matrix chat worked really well too.

- The variety of speakers was pretty good. I'm hoping the variety and number both grow.

- Timing worked pretty well for getting people off stage and getting the next person set up.

The least good:

- Lack of food and beverage options in a close proximity. Can we get a food truck or five? I think it would have been a game changer. That poor Starbucks got overrun and there's only so many pumpkin loaf slices or egg bites a guy can take, and there wasn't enough time between talks to run and grab food.

- Was there a host hotel this year? Can we get one?

I love conventions with after parties, but I wasn't up for hanging out (hungry and uncaffeinated) till 2 am for after action.

- Can there be an optional specific training for volunteers? Like training on the various A/V systems, for example. I was late signing up to volunteer, so I recognize I might have missed it.

- Highly recommend a chime or light system to cue the speaker that their time is almost up since the cards were hit or miss.

Ideas for the future:

Any chance of having a live roundtable with people from *Off The Hook*?

Thanks for making it a memorable experience, and especially thanks for letting me help as a volunteer. I'd love to help out even more in the future.

A New HOPE Attendee #10

These are all really good ideas. The thought of food trucks is one that came up, but we weren't able to coordinate it with the university. Now that we've had an event and it's clearly something that people would benefit from, we think it'll be a lot more likely next time. But we do have to remind people that it's important to take a break from talks now and then so that you can take care of yourselves. We know people want to see all of the talks, but getting food is also part of the experience. (We had the same issue at Hotel Pennsylvania even though it was in the middle of midtown Manhattan. People want to stay for every minute of the event.) We've considered having a mandatory break so that everyone could get food at the same time, but we've been advised that this can result in overcrowding at all of the venues and even more frustration. We'll keep fine tuning this.

We did have a couple of "host" hotels which were adjacent to each other and which we were able to sell out. There was a great bar open super late downstairs which many attendees congregated at. But that doesn't have to be the only place for post-conference activities. We're open to any specific suggestions that those familiar with the area can offer and we'll continue our research on that front.

We had a number of volunteer meetings prior to the conference. A/V is a bit tricky, as we prefer people already familiar with the equipment to be running it. Rookie mistakes at that level are something we'd really prefer to avoid. But if you do have experience in that field, we suggest getting involved early when the calls for volunteers first go out. We definitely can use the help!

We're not aware of any instances where speakers didn't end on time, so we're not convinced we need to replace the system we had this year. If that proves to be necessary, we'll certainly address it.

As for having people from the radio show on a panel, we can definitely consider that. We've done this before, after all. The only complication is that most of the people involved with the show are also involved with running the conference which makes this extra task all the harder. But, as we like to say, there's nothing like a good challenge.

Dear *2600*:

Thanks for an awesome HOPE. Had to change my ticket from in person to virtual. Still worthwhile, although I really hope to be able to make it in person for 2024!

One ask for virtual: I was disappointed I missed the music- I am guessing we have YouTube's rather onerous practices to thank for that. If there is a way to have the music stream even if just to ticket holders, that would be great! (Though hopefully we will just be there next time.)

Great and important work you all do and can't thank you enough!

A New HOPE Attendee #11

Thank you for the support and encouragement. We do want to do a better job with the afterhours streaming. Some of it was indeed due to YouTube (although we were wrong to rely on them as a primary outlet, but some last minute cancellations forced us into that position), but we also were severely overworked on the A/V end. We had some of the greatest people in the industry working with us, but unfortunately they're also human. This is also something we'll be working with the community to improve.

Dear *2600*:

This was my first HOPE, but I've known about it since the mid-2000s. It was an incredible opportunity to meet the hackers who influenced me (from around that same time period), which meant a lot coming as someone who grew up in rural Wisconsin with little more than a net connection and intense curiosity.

Thank you for putting on the event, and I hope to be able to attend next time. I was actually sent by my workplace to man our vendor table. We met lots of interesting people and had a great time.

A New HOPE Attendee #12

While smaller than previous vendor areas, we believe this one worked particularly well insofar as interaction with attendees. Having an entire building to work with certainly added to the positive atmosphere. We have many options for the future, including expansion inside the same building or using additional buildings. This is something we were never able to consider at the hotel and the possibilities are only limited by our imagination and enthusiasm.

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

Clearing the Fog

A year of digging into the location data marketplace led us to a company that allows police to access millions of people's location data - and reconstruct their lives with a few clicks.

When EFF began filing public records requests with police agencies last year, we wanted to see if we could learn whether location data pulled from our mobile devices was being exploited by surveillance technology companies. Included in one of the responses was promotional material from a company called Fog Data Science, LLC, which offered access to the precise and continuous geolocation of hundreds of millions of Americans.

We'd never heard of Fog and the company had almost no public online presence. So we requested more records about the company, specifically from law enforcement across the country. What we uncovered was a widely-used mass surveillance technology that raises "significant Fourth Amendment search and seizure concerns," according to Rep. Anna Eshoo of California.

What we learned is that Fog Data Science offers a sleek search engine called Fog Reveal that allows cops to browse through that location data as if they were Google Maps results, and a "device search" feature that provides historical location information for a single device going back for months or possibly years.

People's location data ends up with Fog after it's collected through smartphone apps and then aggregated by data brokers. Often these apps are unassuming - they might tell you the weather, for example - but meanwhile, they collect your location data as well. Data brokers buy bundles of this data and it can include a wealth of private information about you, such as your year of birth, gender, what search terms you use, and perhaps most importantly for Fog, your location. Each of these bundles of data has something called an ad ID attached to it, which is a random string of letters and numbers associated with your device, and which data brokers can later use to group them together to form a more complete picture of your behavior. This data allows companies to target ads to very specific groups of people - say, everyone with an interest in *2600 Magazine*. It also allows Fog to offer a service that they claim in marketing materials has "billions" of data points about "over 250 million" devices. With a few keystrokes, a Fog user is able to access an exhaustively detailed account of a person's life - often regardless of whether that person is under any suspicion or whether police have obtained a subpoena or warrant.

A pitch by a Fog official trying to sell his company's surveillance to law enforcement highlights how dangerous this product could be. To demonstrate a proof of concept, the Fog representative relayed how New York City experienced high COVID infection rates during the first few weeks of the pandemic, and it made leaders of nearby states nervous about New York City residents traveling and spreading the virus. The governor of Rhode Island had recently proposed banning all travelers from New York.

Fog's demo illustrated how its data could be used to help enforce such a ban. The company ran a dragnet query on its dataset, looking for anyone who had traveled between Port Chester, NY and Newport, RI between March 5 and March 22. It found 52 devices. Fog then narrowed in on one of those devices and ran a "pattern of life" analysis on it, querying for every GPS ping associated with that device for the previous 90 days. It found over 24,000 pings - more than 266 per day - locating the device across Rhode Island, Massachusetts, New York, and Connecticut. It showed how the device had taken multiple trips across New England, stopping in the New York City metropolitan area and near Rochester at different times. And it revealed the device owner's likely home, near Providence, and several other common destinations nearby. All of this was done without a warrant and with no apparent

law enforcement investigation. The person's private data appeared to be used as a sales pitch.

We were also able to analyze the app's public-facing code to get a better understanding of how its product works for the law enforcement end users. Fog Reveal, like Google Maps, is a web application that runs in your browser. To research its functionality, we locally reconstructed the app based on the web resources available by visiting `www.fogreveal.com`. This was possible at the time because, upon loading the page, without logging in or even clicking anything, the site automatically requests nearly all the javascript/HTML needed by the fully functional app.

By saving Reveal's frontend files and organizing them into directories mirroring their original URL paths, we made a local reproduction of the site's resources. From there, we wrote a mock backend server to serve the files and handle API calls made by the frontend, and then systematically worked out the format of data expected from that API. Note that because we had no access to Fog's backend server, we made several educated guesses and had it only return fake location data. So it's possible that our mock website differs from Fog's functionality. Once this was done, we had a semi-functional local reproduction of Reveal that made no requests to Fog's actual server, and yet allowed us to explore its features.

After signing in, Reveal presents a Google Maps view of the U.S., as well as a toolbox. Users can "geofence" an area with a shape such as a circle, or they can carve out a more detailed area, such as the shape of a building. The frontend circle tool will allow queries with a radius of 2500 meters, allowing up to nearly 20 square kilometers when performing a "signal search." It's possible that the backend imposes further limitations.

The user can also specify a date and time range for their query, and it seems that these ranges can stretch back over several months: a copy of Fog Reveal's user manual received from Greensboro Police Department claims that date/time ranges can extend up to 90 days, and can be searched "back to Jun[e] of 2017."

After specifying a geofence and date/time range, the user can run their query. Queries return a set of data points which represent where a device was at a given point in time. The user can then do further analysis on these signals, such as grouping them by the device that produced them, or displaying the path taken by the device over time.

We also discovered that if certain user parameters are set, Reveal will update its logo to display "Reveal Federal," and enable the frontend to request a much more powerful suite of query tools from the backend. These federal users have access to an interface for converting between Fog's internal device IDs and the device's actual advertiser ID. We don't know if this feature is operational but, if so, it would contradict statements Fog makes in other materials that its proprietary FOG IDs can't be converted back into advertiser IDs. And, if users could retrieve the advertiser IDs of all devices in a query's results, it would make Reveal far more capable of unmasking the identities of those device's owners.

Fog is a Fourth Amendment violation. First, police should not be able to use Fog's "device search" without obtaining a warrant, and public records show that many agencies did not get warrants before using this feature. Even when police obtain warrants before using Fog to perform geofence area searches, they would still violate the Fourth Amendment for all the same reasons that courts have held other geofence warrants unconstitutional.

Police use of Fog is a privacy disaster - it shows how location data taken from our devices is exploited and later used against us via police surveillance. We urge you to speak up to Congress and demand that lawmakers pass a meaningful and comprehensive data privacy law that allows all of us to control when and how our data is used. Such a law would stop this police surveillance at its source by preventing data brokers from obtaining and selling your data without your explicit opt-in consent.

Three Rules Against Tech Exposure and Dependency

by LVundertone

Imagine you start living with a roommate. Carl is fun, smart, and a good friend. If you need help fixing a running faucet, planning a trip, or even finding a hookup, he'll be happy to help. And he'll do it well. Want to relax? Carl can chat, Carl can tell jokes, or Carl can recommend the perfect movie. Soon enough, you share everything with him and invite him to come with you every time you go out, be it to attend a conference or just grocery shopping.

Now, you know nothing is free in this world, and Carl can't always be there for you and afford rent. How does he do it? Well, Carl works for the CIA and various private companies, reporting all your conversations, selling snippets of your life for these entities to use as they want. Otherwise, why would he put so much effort in holding your attention? And it's not just you, almost everyone you know lives with such a roommate.

While this is an exaggerated parallel, the world we live in isn't that different. Online services and smartphones hijack users for their own benefits, and eat up any data they can get, from messages to audio recordings. The average *2600* reader probably takes measures to protect themselves. But I find that more can be done even among informed people.

In this article, I will share a few simple rules one can use to protect themselves from tech's spying and attention draining.

Store Your Phone(s) Away

Of all the information a phone gathers, audio is one of the most important, since it is often not willingly that we feed it pieces of our speech. It is voice assistants which usually tune in, triggered intentionally or via the common false positives. Sometimes, it is apps which were granted invasive authorizations.

While the privacy-concerned individual might not have to worry, it all changes when spending time with friends or family. Your guests might not care about such issues and could expose you to espionage by carrying their smartphone into your home.

My solution is to require them to be left at the entrance, in a dedicated space. At home, my phone is used like a landline, and I expect the same from my guests. If you're lucky enough to live in a large house, it is rather easy to create a network connecting your phone(s) to a distant speaker to let you hear a ring even when you're in the attic or garage.

Some might refuse. Explaining your reasoning in more details can help, especially if you romanticize the issue and adapt to your interlocutor (depending on the person, the threat can be Big Tech, the government, or the lizard people). If that's not enough, you at least have raised some awareness and reminded yourself that there will be a third party forcefully added to your conversations.

Of course, other devices can listen in. But it's easier to unplug a mic or store away a laptop (which people usually don't hide in their pocket). As long as you don't collect smart devices, you've made a step towards more privacy with the added bonus of better focus and attention.

Cancel Your Phone's Internet Plan

A smartphone usually comes with an Internet subscription, granting an access to the web and online services from anywhere. While many find it useful to check maps, a calendar, or to find info on the go, it is rarely required. Maps can be downloaded, planner books have always been convenient, and one can usually wait a few hours to confirm a piece of trivia.

Still, plenty of people happily share their location, busy schedule, and more with Google and Apple. Even if your OS and the services you use are open-source, you are centralizing potentially sensitive information in a single device. And when everything is encrypted and uncompromised, you're still tying yourself to your device, reinforcing checking habits.*

Nowadays, it might be hard to find a phone plan without Internet data. But a compromise can be made with minimal data (where I live, many cheap plans only offer 100 MB) or the will to turn off your phone's data.

Avoid Social Media

Modern social medias are tailored to be addictive, designed to monopolize attention, and made to accumulate information about its users. Some members happily overshare, disclosing their whereabouts, purchase habits, and more.

While it is possible to not share anything superficial, it is also best to avoid interacting on those platforms. Instead of liking or commenting, you can reach out via different means (emails or face to face, for example) which allow for focused and richer interactions. This prevents exposure to dark patterns, and

diminishes your online presence. The benefits are an escape from deceptive design, and reduced chances of doxing.

If you really need to follow some accounts, you can easily create an RSS feed for them.

No matter how simple those measures are, they are important. I've met countless people who are concerned with privacy and security, or/and have been involved in legally questionable acts yet didn't consider the risks involved in their tech use. Malicious designs and data gathering can lead to grave consequences, yet are ignored for the sake of convenience.

This is not a plea against smartphones, which can be great when used thoughtfully. It is a reminder that what you don't care about is better hidden than public. With the recent Roe v. Wade reversal, many have realized that something as innocuous as period tracking apps were potentially dangerous. And no matter what your political orientation is, what you've shared with private companies or the public could get you in trouble in the future.

Privacy mindfulness isn't enough; you should also practice it.

* link.springer.com/➥article/10.1007/s00779-011-0412-2

Sneakers: 30 Years of a Cult Classic

by GI Jack

I've done two things this week. Watched *Sneakers* again, and picked up some old issues of *2600*. In the Autumn 1992 issue was a review of *Sneakers*, which was then a new release. Both this issue and the movie deserve a second look.

The movie has aged like wine. While a lot of the computer hacking and encryption are depicted with tasteful Hollywood magic, a lot of the other elements of the movie are spot on. Reverse engineering hardware, lock picking, a bunch of ex-blackhats working for a small pentesting firm with companies such as banks as clients.... International intrigue involving state and sub-state actors. Data being the new weapon, as discussed in 1992, more striking, topical, and pertinent in 2022 than it was in 1992.

It starts with Bishop, a college hacktivist who barely escapes arrest by just happening to step out for pizza as the police raid his setup. Flash forward years later. Under a false name he is now working for a pentesting gig with a bunch of other shady characters. An ex-CIA agent played by Sidney Poiter, a blind phone phreak (i.e., a Hollywood-ification of Joybubbles), and a hardware expert (Bishop), played by *Ghostbusters*-era Dan Aykroyd.

While the encryption cracking is bogus, there is a lot of the technique from social engineering (using disguises and distraction), lock picking, war dialing, numbers books, and of course, voice verification hacking that is reasonably accurate for a movie. The big kick is that the voice verification hack did not exist in 1992, but only decades later, when real voice authentication systems became common, was this actually used. The dialog about information being more of a weapon than guns rings more true in 2022, especially in the age of weaponized shit-posting.

The small team of people with shady pasts in a small company doing pentesting for banks and other companies should also hit some notes. Not nearly as visible in 1992, this today is a good percentage of the hackers that would have mocked the concept back then.

Another interesting but overlooked minor detail is the "machine that cracks all encryption," which was originally thought to be "an impossible device," but when it's revealed it does not crack Russian encryption, only American, it starts wandering back to Earth. In 1992, there were only so many encryption algorithms in use in America. You could count them on one hand. Blowfish wouldn't be written until the following year. DES (known exploits), IDEA (known exploits), and RC4 (known exploits) were common ciphers. Even if the exploits weren't known to the public at the time, it was very plausible that someone could have been sitting on some epic zero days. It's also now known that the NSA paid RSA to weaken a cipher, so it's plausible - very much so - that someone would have a device that breaks all U.S. ciphers based on insider knowledge. Most of these ciphers were *not* open source, and the concept of public, trustable, community encryption had not come to fruition. On top of that, it was hard coded into a chip in a black box to restrict distribution, and to prevent copying. Smart.

Of course it's not all accurate, and Hollywood takes the typical liberties in adding car chases, clandestine rendezvous, shootouts, and of course making computer use look good on the screen. Mix in some late 80s, early 90s costumes and the movie continues to charm its way to "perennial cult classic."

Internet Landscape in Germany

by Patrick patrick@pahem.de

I really love the international nature of *2600*. I haven't seen any other magazine with contributions from all over the world. In particular, I like to hear about other countries' Internet and telephone infrastructure for end users. Sometimes "Telecom Informer" writes a little bit about this topic. In this article, I would like to briefly explain to you the Internet for end users in Germany. It's not a scientific paper. Please read it more like a subjective view from me living in the northwest part of Germany.

In mid 1990s, the telephone monopoly by Deutsche Telekom (previously Deutsche Post) ended and every company was able to provide telecommunication services to end users. Some of the new providers used the last mile from Deutsche Telekom and some installed their own cables. Later the cable TV companies started to provide Internet access via the TV cable. A few years ago, fiber to the home got big hype and a subsidy program was founded by the government. Now, the local authorities are in charge and it takes a long time. Some other providers, mostly serving a limited area, even started to install new fiber cables at their own cost, which usually comes with a shorter realization time.

What Internet access bandwidth is available for you highly depends on the available providers and what cables your building has installed. With old copper lines, you can get DSL (ADSL or VDSL) with bandwidth between 1 Mbit/s and 250 Mbit/s downstream and 0.1 Mbit/s to 50 Mbit/s upstream. This depends on the equipment the provider has installed in the telecommunication cube down the street and how far away your home is from it. With a copper line from some provider (mostly Deutsche Telekom), you can also choose from a variety of different access providers which use the Layer 1 (cable) or Layer 2 infrastructure (bit-stream access) from the provider who owns the last mile cable. You can order Internet access from the cable TV company that's in your building for up to 1,000 Mbit/s downstream and 50 Mbit/s upstream bandwidth (DOCSIS 3.1). With the new fiber installation, you will see AON networks with active termination in the cube down the street or GPON with passive infrastructure until the next bigger aggregation facility. The offered bandwidth on this fiber installation is up to 1,000 Mbit/s in downstream and 1,000 Mbit/s in upstream, but mostly still asymmetric like 1,000 Mbit/s in downstream and 300 Mbit/s in upstream. For an apartment building in Cologne, I have seen an installation which uses fiber to the basement and then reuses the old copper lines with G.fast from it to the flats. Recently, 4G/LTE access or combined 4G/LTE with fixed line became available. Wireless point-to-point or point-to-multipoint connectivity isn't a big thing for end users. Some smaller citizens' initiatives are using wireless technologies to connect areas where no provider wants to invest. But nowadays, with the subsidy for fiber installation by the government, these self-help initiatives may not be needed anymore.

All of this access comes with neutral Internet access to any services and mostly without any traffic limits. Some providers have a fair use policy in their terms of use and can terminate the contract if it's violated. Also, a hard limit from some providers is in place. This will slow down your access to the Internet after a certain limit is reached, like O2 on their DSL products. But most of the fixed line access comes without any limit on traffic or services. For the mobile networks, this is another story. They have traffic limits with slowed down speeds after the limit is

reached, and also unlimited traffic to specific services like music or video streaming is available as a paid add-on.

In Germany, there is a big difference in the backbones of the providers. After the purchase of cable TV company Kabel Deutschland by Vodafone, they had a lot of problems with slowness during high traffic hours and after a massive amount of new customers resulted in oversubscription in access nodes. I had a cable TV Internet connection during this time and it was really bad. Video streams stopped for buffering multiple times. But luckily these times are over.

Deutsche Telekom is also a little bit special because they have a restricted peering policy and are usually not available for peering in big Internet Exchanges. They had a big fight with Google about YouTube traffic, and for quite some time you had slow access to YouTube during high load hours from Deutsche Telekom. Another story about Deutsche Telekom I heard from a small local provider recently: the small local provider had only business customers and, during the coronavirus pandemic when people began to work from home, a lot of their customers complained about slow VPN access for their employees. The customer's VPN gateway was in this local provider network and the customer's employees at home most often were connected with Deutsche Telekom to the Internet. The local provider had no direct peering with Deutsche Telekom and the reason of the slowness was unknown to me - maybe latency or bottlenecks in the network path. Anyway, to solve this issue, they had to establish direct peering with Deutsche Telekom which they had to pay for.

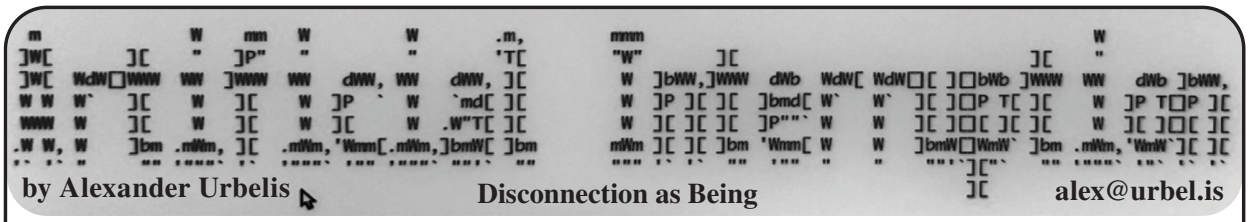
The price range for Internet access is from 20 euro per month for the lowest bandwidth and for 1,000 Mbit/s about 120 euro. Most of the Internet service plans come with unlimited domestic telephone calls. The telephone services have mostly migrated to VoIP. Almost all of the providers offer a router for a monthly fee of two to eight euro or a one-time reduced price. Popular brands are FRITZ!Box from AVM and Speedport from Deutsche Telekom. But it's also possible to use any router with the ordered services. After some back and forth, a law was established which let you choose the router on your own and set the demarcation point of the provider to the last passive connection point in the building - see Router Freedom.[1] For this, each provider has to provide a technical interface description of it. An example is the Schnittstellenbeschreibung nach § 41c TKG from EWE.[2]

Since a little more than one year, my current Internet connection is fiber with AON technology from a local provider. In the beginning, I had a FRITZ!Box 5530, which comes with a fiber SFP BiDi module, and was able to reach the provided 1,000 Mbit/s in download stream and 100 Mbit/s in upstream. I'm now on 75 Mbit/s download and 25 Mbit/s upload, which is enough for my current needs and cheaper. But I can highly recommend the fiber connection instead of DSL. Before I had a VDSL connection, and my first hop latency dropped by around 20ms to 3ms after migration to a fiber connection. Everything just feels a little snappier. I replaced the FRITZ!Box 5530 with an OpenWrt instance in a virtual machine on my home server and I terminate the fiber from the provider in a MikroTik five-port switch with a 1G SFP BiDi from `fs.com`. With this setup, I can use OpenWrt without an additional hardware router. The only negative was that my latency increased by 1ms. I think this is due to the virtualization, but I haven't checked this in detail. Maybe it's the MikroTik switch.

Thanks for reading, and I hope I can encourage some people around the world to write about the local Internet in their country.

[1] `fsfe.org/activities/routers/routers.en.html`

[2] `data.ewe.de/-/media/ewe/documents/02-privatkunden-telekommunikation/04-broschueren-und-infomaterial/schnittstellenbeschreibung-p-41c-tkg.pdf?cb=E2CC7123`



by Alexander Urbelis

Disconnection as Being

alex@urbel.is

For those not familiar with the concept of the Proustian moment, according to the American Psychological Association, it is "the sudden, involuntary evocation of an autobiographical memory, including a range of related sensory and emotional expressions." The term comes from Marcel Proust, a 19th Century French novelist and critic. In Proust's most famous work, *À la Recherche du Temps Perdu*, (translated as *Remembrance of Things Past*), at the outset, Proust's protagonist eats a tea-soaked madeleine cookie. The smell and taste of the madeleine evoke strong memories from his childhood of him doing the very same thing with his aunt. From taste and scent of this buttery morsel doused with lime-blossom tea, long-forgotten memories come back vigorously and vivaciously, giving the protagonist the ability to recall details buried within his mind, the minutiae of his home, the streets on which he used to play as a child, his town square... many memories that were lost in time came back into being.

I had a Proustian moment of sorts last week. What evoked my involuntary memory, however, had nothing to do with French pastries but was an older Richard Linklater movie, *Before Sunrise*, set in Vienna in the 1990s. I had both a flood of memories and a yearning for a time where, despite being disconnected, perhaps we were more connected to each other and the moment.

My Vienna story is from the spring of 1998, and, like the plot of *Before Sunrise*, also involved trains, chance meetings, and the limitations of 1990s technologies.

I'd taken an overnight train from Venice to Vienna. Living and studying in England at the time, I was traveling with a girl from Oxford who was, for that moment at least, my girlfriend. I don't recall very much at all of the Vienna train station, except for the money-changing kiosks in the terminal.

Hardly uncommon for 19-year-olds, I'll freely admit that I had a wandering eye. While my girlfriend was waiting in the queue to change U.S. dollars into Austrian schillings (remember, this was several years before the Euro, when each European country had its own, unique currency), I locked eyes with a gorgeous girl, waiting on the same kiosk, one place ahead. Shortish brown hair that was angularly just below jaw level, she had a look that was distinctly American. Accompanied by an older gentleman who sounded like he spoke German well, I wasn't sure if she was with her father or an older boyfriend. Furtively, we glanced back and forth at each, but nothing came of this. How could it? My girlfriend was right next to her.

That evening, the girlfriend and I were walking along a back street looking for a place to eat that wasn't touristy or obscenely expensive. Coming straight at me, on the very same sidewalk, was the girl from the train station. I couldn't let us pass like ships in the night so I pointed at her and said "train station," as she passed. We both looked behind us, me as I continued walking backwards and pointing at her. "Wow," was all she said as she smiled and continued on her way. What a weird coincidence, I thought to myself.

The girlfriend and I stayed in a little pensione outside of the city center, well off the beaten path. This was primarily to save money because we were taking the Eurail around for several weeks and still had a way to go. It was the sort of place that backpackers and students would frequent and I recall a strange, outdated, greenish theme running throughout all the rooms, matching the equally dated linoleum floors.

The night passed. We took breakfast in the pensione: a coffee and some fresh breads. As I was walking back to our table, I saw the girl again, sitting right there diagonally across. "Hello again. This is weird," I said. We all started talking. The girl informed both my girlfriend and me that she was a student from Arkansas and that she was traveling with her father. There was a connection between the two of us for sure. We commented on how uncanny it was to run into each other three times in a single day in Vienna, and especially so in the odd little pensione we found ourselves. We exchanged no details for staying in touch. We departed.

The girlfriend and I went on our way, westward, to Germany. Train to Munich, then to Frankfurt, then to visit some friends in Heidelberg. Everything was great. I sometimes thought of the girl from Vienna, but that was long gone by now and a few weeks past.

We eventually went back to England. The girlfriend eventually went back to the United States. We stayed together doing the long distance thing for perhaps a month, but eventually broke up.

The night after this breakup, I decide to go to the Oxford Union to listen to, if memory serves me right, Aleksander Kwasniewski, the then-President of Poland address the student body. After events such as this, the custom is to rush to the bar to grab a few Union-subsidized pints.

There was a massive influx at the bar. Though I remember nothing of what Kwasniewski said, I do recall quite vividly that I was ordering a cheap pint of Tetley's when I looked over to my right and immediately standing next to me was the girl from Vienna. "What're *you* doing here?" I asked. After a brief moment of disbelief, she screamed

and hugged me and asked me the same thing. It turned out that both she and I had been living in Oxford the entire year and never saw each other. What are the chances? It must be fate, we both thought. We exchanged phone numbers. We made plans for drinks. We were both excited.

I apologize for the anticlimax here, but nothing ever happened. The girl from Vienna had an overbearing boyfriend very skeptical of our Viennese connection. Like the girlfriend I had when I met the girl in Vienna, she too eventually went back to the United States. I had only her local phone number in Oxford and, after she left, we never spoke again.

All of these memories, the glances, the chance meetings, the slant of light on the street the evening we passed each other, that intense feeling of recognition when I saw the girl from Vienna next to me at the bar several countries away - they all came flooding back when I was re-watching *Before Sunrise*, a story of two travelers and their chance meeting on a train.

In the movie, Ethan Hawke plays Jesse, an American student, who meets Céline, a French student played by Julie Delpy, on a train en route to Vienna. An awkward fight between a married couple in their train car gives them cause to catch glances and, in due course, speak to each other. There's flirting and a connection, and they decide that they will disembark in Vienna together to wander the city. Unlike my anticlimactic story, Jessie and Céline have an engaging evening of conversation, self-discovery, and climactic sex in a park. They decide that their meeting and encounter was meaningful but decidedly fleeting, and they agree to part ways forever the following day. As they are saying their goodbyes, which proved more difficult than anticipated, Jessie and Céline agree not to exchange any contact details, but to meet in that same spot six months later. The movie ends while we watch them separately journey onwards towards home, alone, and we wonder whether they will make good on their promise of reunion.

Though there are trains and Vienna and chance encounters in common between my story and the plot of *Before Sunrise*, those details were not the sole reason why I had the Proustian moment that I did. As I watched Jessie and Céline, I remembered what impermanence felt like and recalled how short-lived and fleeting life's encounters were. Before the days of relentless social networking, we often met people and then said goodbye, forever.

It may be difficult for young readers today to understand that a goodbye at a train station was the end of a relationship. Today, every chance encounter is followed up by a LinkedIn request, inextricably connecting you to all of your acquaintances forever. Today, Jessie and Céline would surely have followed each other on Instagram. In the early 1990s, there was no LinkedIn, no exchanging of Instagram profiles, no Facebook friend requests, and barely any email.

Even email was ephemeral. Students often had university email addresses, but those were never permanent. Email permanence is a function of services like Hotmail and Gmail, with which we struck a dubious bargain: an email address forever in exchange for the right to datamine our communications.

With our identities attached to every encounter, to our locations, and to every interaction, there is an ever-increasing feeling of responsibility and accountability for everything we do, and this, in turn, leads to a sense of permanence of self from which it has become impossible to escape. It has, in other words, become impossible to stop being you.

This, however, leads to an ironical conundrum. Because we are stuck being ourselves, all the time, forever, that permanence prevents us from truly being and knowing ourselves. We cannot experiment, explore, or extricate ourselves from our online identities, and the full measure of data that represents our past actions and present identities. It is the very interconnectedness of the world, and the permanence and accountability that goes with it, that is holding us back rather than propelling us forward.

Perhaps that is because the permanent bonds and connections we make via social media are cheap and common. They are not meaningful. And the ease with which we connect, and stay connected with others, denigrates the value of all of our other relationships.

What would become of the encounter with the girl in Vienna today, or the chance meeting that set the stage for *Before Sunrise*? I would have connected with her on Facebook, browsed her pictures, realized she was at Oxford, and that lasting and inimitable feeling of recognition when seeing her at Oxford Union would have never happened. Jessie and Céline probably would have never locked eyes on that train to Vienna because they would have been staring at their phones.

The Proustian moment I had while watching *Before Sunrise* was in some sense a remembrance of the freedom that came from living in a disconnected world; it was at once a recognition of my fortuity to have matured in an age where I was not accountable for my every second of being, and of the tragedy that my children and their children will never know that feeling.

With this sense of self and being in mind, I do not think it is hyperbolic to state that the Internet has not only failed us, but in some ways has also broken us. If we are to recapture the beauty of the fleeting moment, the chance connection, the sense of uncertainty of ever meeting again, we need to fight for unaccountability, for anonymity, for privacy. The fight is not about data - it's about concepts more fundamental, powerful, and beautiful: about experiencing life, not as a profile or a data set, but as a human being.

What's Old is New Again: PDF Malware Part Deux

by lg0p89

Years ago (yes, "Get off my lawn!") when the industry was growing by leaps and bounds with new vulnerabilities weekly, and businesses were getting pwned for bragging rights and not tens of thousands of dollars, the innovation was to weaponize PDFs. This worked for a while, and defenses were put in place. This held for the most part until recently. The attackers are using the PDF in a slightly new way. They secure a target list, which these days is relatively easy and cheap. There have been so many breaches over the recent years, this isn't a problem. This coupled with some company websites listing their management with their email addresses makes this much less complicated.

With this in hand, the attackers send an email with the ill-intentioned PDF. This nuance started to be seen in 2020 and used the title "Remittance Invoice.pdf". That should have been enough to keep the users from opening it, but you know.... Within this is an embedded word document titled "has been verified. However PDF, Jpeg.xlsx, .docs". As this has been used over the last two years, the file name may have changed to something still catchy that would entice the user to click, double-click, or even triple-click the file. Yes, users still re-open the same files even after they know overtly and clearly that they are infected. I once ran an international phishing campaign for a global company. There were users who clicked the blatant phishing email, received the "You've been caught" landing page, and still went back clicking away. I guess they just wanted to make doubly sure they screwed up.

I digress. The PDF file name needs to be something that will draw the attention of the targets. You could also use "IRS Notification," "Proposed Bonuses," or any title that makes people believe they'll be able to see some data or information that they shouldn't have access to (thank you social engineering!).

Let's address the Word document title. This is embedded in the PDF file. The name itself is a little odd. For all the available choices, why this one? This all becomes clear operationally when you open it. Normally, when the user attempts to open it, Adobe Reader displays "The file [file name] may contain programs, macros, or viruses that could potentially harm your computer." When the user opens this, the message then reads "[File name] has been verified. However, PDF, JPEG, xlsx, .docs" may contain programs.... Let's say your PDF name is "The file Nobody may contain programs, macros, or viruses that could potentially harm your computer." When the user opens it, they see "The file Nobody may contain programs, macros, or viruses that could potentially harm your computer has been verified. However, PDF, JPEG, xlsx, .docs". See what it does?!

For a user that doesn't know to look for this or is too tired from working too much, the sneaky aspect of this might not be caught. They may breeze through the warning and check and find out too late what they did.

In the instance when the file is opened, which is completely plausible, it disables the protected view and the user is a happy recipient of malicious activity. Within the Word document is a URL used to load an embedding object (OLE). This contains code written to exploit CVE-2017-11882 for remote code execution. The code directs the system to download fresh.exe, which is a keylogger (snake). Curiously, you could use this method of delivery for other malware.

For the users thinking PDFs are safe, no worries, just open them, share this with family and friends - not so fast. This is still an issue. While this uses an old framework, the low-tech yet creative addition has the opportunity to really mess with your users.

What Does "Impossible" Mean?

by XCM **xcm@tuta.io**

I have recently come across another attempt at creating, or simulating, a perpetual machine.[1] According to Wikipedia, "A perpetual motion machine is a hypothetical machine that can do work infinitely without an external energy source."[2]

You will find it repeatedly stated everywhere that this kind of contraption is impossible because it would violate the first two laws of thermodynamics, or at least one of them.

This got me thinking. What does "impossible" mean? Is it something that anyone, or anything, will never be able to achieve? A goal that has not been reached yet? Or can we place this concept somewhere in the middle?

In the case of this marble machine, even to a layman like myself, it is evident that, in standard conditions, the gravitational pull alone will not be sufficient to propel the marble to its original position because the same force will be applied in the opposite direction when the object starts climbing. This would also be exacerbated by other forces, such as friction against the rails and air itself, which would dissipate some of the energy the ball needs to counteract gravity.

However, this reminded me of how often specific events are labeled as impossible, just because they would contradict what was previously observed or, even worse, one's biases.

Questioning, in a scientific setting, is generally frowned upon. It is sometimes perceived as anti-science. I find this attitude paradoxically anti-scientific. The scientific method itself relies on counter arguments to achieve accurate results. Blind faith is not science. It is just faith. At times, we seem to forget that the history of science is full of dogmas that were later superseded by more accurate understandings.

Now, I am not suggesting that we scrap the laws of thermodynamics. I would certainly have no clue how to come up with something better (or to even get started, for that matter). I am not a qualified scientist, either, but I feel that at times, egos can get in the way when interpreting data. It looks like questioning should be at the very core of the scientific method: "[...] when testing an hypothesis or a theory, the scientist may have a preference for one outcome or another, and it is important that this preference not bias the results or their interpretation."[3]

Unfortunately, questioning one's opinions is hard. Admitting that what we have worked for or believed in for years might be flawed is really, really difficult. Dismantling our beliefs is akin to rejecting parts of our own identity.

Naturally, if an outcome is considered impossible, most might be discouraged from attempting to prove otherwise. I am not proposing we should all start hoping that a bunch of monkeys hitting random keys on a keyboard will eventually produce the work of Shakespeare.[4] Even though statistically possible, this would clearly be so unlikely, its probability so close to zero, that nobody would be blamed for terming it impossible. What I am suggesting is that we should question as much as it is healthy to do so. It would be great if the efforts of scientific research, for example, were applied not only to prove the scientist's theory, but to equally disprove it. I think this approach would dramatically increase the quality of drugs in the pharmaceutical industry, for example.

What if one day we determined that the scientific method of today is in itself insufficient to prove reality? What about those processes that are not repeatable nor observable and for which we have no prior statistical data? How can we determine their likelihood? Who can scientifically state whether life on other planets is probable or an impossibility? Who can say that it is impossible that anyone would like Nutella on pizza?

Of course, I do not have answers to these questions, even though I have tried Nutella on pizza. I can barely decide what I will be doing tonight. All I am saying is that a healthy dose of questioning is the only way forward. Inquisitiveness gets lost with age in societies where the education system mostly focuses on sciolism and conformity rather than nourishing independence and critical thinking. At the same time, if everything around us was enough as it is, or any alternative was deemed impossible, there would be no progress and no way forward. Let's keep questioning, understanding, relearning, and teaching others how to ethically do so.

References

[1] YouTube - Perpetual marble machine project - final product (youtu.be/sMjHbDXfrV4)

[2] Wikipedia - Perpetual motion (en.wikipedia.➥org/wiki/Perpetual _ motion)

[3] Rochester University. Introduction to the scientific method (teacher.pas.rochester.edu/phy _ ➥labs/AppendixE/AppendixE.html)

[4] Wikipedia - Infinite monkey theorem (en.➥wikipedia.org/wiki/Infinite _ monkey _ ➥theorem)

Freedom of Speech: Terms and Conditions

by James Nagle

We've all seen it. Fact checks, disclaimers, and the worst of all, "misinformation." But who is checking facts, writing disclaimers, or judging information as incorrect? We live in a society that is arguably more divided than at any time in American history, and the attack on civil liberties is well underway. Partisan politics would like to continue to pit one side against the other but the truth is our rights and liberties as citizens have always been under attack from both sides. Both sides want you to believe that the cause is just while the truth is as far removed as can be. The old adage is true: "There's three sides to every story - yours, mine, and the truth."

The First Amendment to the United States Constitution is tricky. Fundamentally, it protects the right of American citizens to exercise freedom of speech, religion, and the press. However, the problem with this right is that over time, legal challenges have whittled away the intended broad sweeping protections afforded to citizens. Restrictions have been placed on free speech and this whittling away of our rights continues to erode the value of being an American citizen. Add in the continually churned sieve of politics intended to further divide the populace and you end up with a scary situation which fundamentally threatens liberty as a whole. Any time a majority of a population has been swayed by fear or coercion to take a firm stance on a topic or subject, all rational thought goes out the window. Given the information age we live in now, evidence to support one's own biases is easily found from a plethora of - sometimes even credible - sources. This leads to the possibility of a majority believing a particular topic which becomes a supermajority very quickly and ultimately ends up with reason becoming less and less valuable.

Given the information age in which we live today, it is ever important for those in real power to understand the big picture. And by referencing those in power, I mean those in real power, not the political puppeteers of our government. In the information age, those who control the information also control the narrative. Social media platforms have replaced more traditional sources of information where it counts and the fragmentation of thoughts and ideas has become prevalent. Echo chambers and silos rule the day and nobody is listening to one another anymore.

The result is, in my opinion, one of the most dangerous times of our modern existence. I'm talking about real world danger here, not just the danger of losing one's voice. The moment we end up in an artificial supermajority fueled by fear, ignorance takes over and innovation dies. Dissent is squelched and bad ideas become trending norms. Mob rules at its worst and the weakest minded individuals pay the price just as much as some of the sharpest and smartest minds of our time. Nobody gets a pass on the results of this catastrophe.

To make matters worse, true technology innovators aren't necessarily governed by the rule of law and aren't required to uphold a patron's constitutional rights. Given the transition of information platforms, this will be the fatal blow to our First Amendment rights as free thinking individuals. Our rights and liberties have been traded for the Terms of Service of your favorite platform and the bottom line of your favorite provider will dictate which information is acceptable for you to consume. You have been determined to no longer have the mental faculties needed in order to judge for yourself. Make no mistake, this is the beginning of another dark age.

We can argue details all day about what content is acceptable for a private information platform to allow, but the truth of the matter is it's right and wrong at the same time. Remember the three sides of the truth? The private information platform's truth is they should have the right to control content. The fear driven supermajority's truth is they should have access to reliable information. Unfortunately, the real truth is that information should not be prejudged before allowing others to make up their own minds about it.

How do we fix it? There's no quick and easy solution. Getting here was a natural evolution based on mostly good intentions and getting out of it will be a substantially difficult process spanning generations. It will require both current and future innovators and technology leaders to get back to basics and change their way of thinking. Ultimately, it requires a fundamental change of culture across our society that requires a big picture view.

People vs. Corporations

by Dark Phiber

Part 1: Robot Wars at the Big Box Stores

Disclaimer: This article is for entertainment purposes only and is not endorsing any of the behavior recommended herein. Any resemblance between references in this work of fiction and real-world entities is coincidental.

Corporations are not your friends.

They don't care about you. They only have one mandate: Create value for their owners.

That's it. Contrary to what you've heard, they aren't here to improve the quality of your life. They're not here to make you look cool, or healthy, or successful. They exclusively exist to siphon as much value as they can. They don't have any mandate to be moral or ethical. They don't care about the environment, living wages, or their employees. They only care about money.

The *only* thing that keeps corporations from being totally immoral predators isn't the invisible hand of the market. It's government regulation (despite all the arguments against government, there is nobody else out there protecting citizens to a comparable degree). Yea, that seems confusing since you've been told over and over (by corporate media) that government is the bad guy. Go figure? Government isn't what's bad. Bad people in government are bad. Meanwhile, collective bargaining (a right often protected by government) and centralized regulation is the only thing keeping most people from being worked and exploited to death. And what few rules and regulations we do have are at least trying to keep corporations from destroying what little habitable environment we have left.

Corporations do all sorts of sneaky-yet-slightly-legal tricks to increase how much money they make. They mislabel and misrepresent products. They make promises they never intend to honor. They constantly lobby to reduce their accountability to anybody but their shareholders. They buy politicians. They buy scientists. They produce their own "studies" showing their products are perfectly OK. They outsource as much as they can to reduce their costs. They hire more employees than they need in order to avoid having too many full time people they have to provide benefits to. They replace people with machines wherever possible, because robots don't complain about not having healthcare or a living wage.

In this episode of *People vs. Corporations*, we're going to talk about the robots. How instead of hiring people to handle checking things out for you, you have now become conscripted in harmony with the surveillance state point-of-sale robot to scan your own products, pay for, and bag them.

It's funny that the big box stores now have almost completely switched over to robot point-of-sale. Half the time these machines aren't working properly. Half the time you need assistance because robots can't be trusted to exclusively transact certain restricted items, but the humans they do manage to have around are even less capable than the checkers the robots replaced. It's a mess. And there's often somebody ahead of you in line who can't figure out how these things work, or wants to turn check-out into a 45 minute life lesson for their six-year-old. These machines end up taking more of your precious time so corporations can make more money.

Corporations screw with you in all sorts of ways. For example, have you ever tried to price-compare two similar items in a grocery store? Maybe it's two jars of peanut butter and near the price tag you have a "unit price" of say, x cents per ounce. Then you try to compare it to a nearby jar and it says x cents per pound. Hey, they gave you the unit price. They deliberately switched it up to keep you from being able to easily figure out which product is the better buy. They do this all the time. They also do shady things like mislead you into thinking that a six pack of one item is more expensive than a 14 pack of the same item. Unless you do the math, you may find buying in quantity isn't always cheaper, even though most people think it is. There's bags of chips with printing that obscures the fact that 75 percent of the bag is empty. Even the placement of items on shelving is scientifically designed to get you to pay more. They have monetized the act of convenience. They have even figured out how to sell broken/defective products, knowing a certain percentage of people won't return them.

I think of myself as an ethical person. I abhor stealing. But years and years of watching these corporations and their minions fuck with me has made me become quite the cynic, and I finally found something to do to ease that tension. It's my way of taxing corporations for forcing me to do their work. It's getting back at them for doing everything they can legally (and often illegally) get away with to make a little more money. Let's call it: POJ instead of POS. Not point-of-sale. Point-of-Justice.

What is POJ? It's the defiant act of getting over on the robots and their corporate overlords. And it's incredibly easy to do, and relatively safe. You just basically act like the kind of idiotic consumer they treat you as - and you can win all

sorts of prizes! Even if you get caught, just admit it was a mistake - no harm no foul, even though it's highly unlikely you will get caught.

Getting Over on the Robots

The robotic point-of-sale machines have all sorts of anti-theft technology. But there are plenty of ways to defeat/confuse the system. I can't go into details of how any particular machine works, but I can cover some of the basics of how these machines try to ensure the sales transaction works the way *they* want. (For example, they employ scales on the bagging area and know the weight of each item. If you scan a product that weighs ten ounces, and then don't put that item in the bag (on the scale), the machine will alert the robot manager to take a look - note that I've never seen the opposite happen, of accidentally scanning an item twice and the machine letting you know it's under-weight! Go figure?)

Some machines also use video "A.I." (another bastardization of the term "artificial intelligence") to examine your motions to see if you're picking up and putting things down appropriately. So all your motions in front of the robot should be fluid and normal. There are some tricks you do *not* want to do, especially since you're on video. This includes scanning one item twice like a cheap bottle of wine, when you have two bottles and didn't scan the more expensive one - it's easier to get caught doing that.

And of course, there's RFID tags in certain items, usually expensive or small items that can be easily hidden. Avoid trying to sneak out any RFID'd stuff. You never know where sensors are.

Here are some specific techniques:

The setup. You typically want to limit the items you try to get past the robot. Don't pick something obvious. Don't pick something too expensive. Don't pick a single of something. Don't pick something large. Don't pick something that can't be bagged with other stuff. Start a normal checkout and have at least one or two bags partially filled with things in the bagging area. Then execute your POJ....

The Double Dip. This is by far one of my favorite tricks. Take two items that stack or nest (like half cans on top of each other, or two stacks of things that you handle as if it's one stack: paper plates, tortillas, or small boxes of things). Know where the UPC symbol is before you grab the stack so there's no fumbling. Pass both the items over the UPC scanner in one smooth motion - it will only register once, and put both of the items in your bag. But at the same time you drop them in the (mostly full) bag, grab the bag and transfer it from the bagging area to your basket. This fakes out the scale. (This is why you have one or two mostly full bags set up before you do the double dip.)

If you're creative, you can find some pretty expensive products you can do this with, like crab meat. Although I'm happy just being able to get a 2-for-1 as payment for my otherwise freely-exploited point-of-sale services I had to provide.

The Miscount. If you're buying three or more of something, I heartily recommend you always miss at least one item. You have five storage boxes? Ring up four. You have ten cans of cat food? Ring up eight. If you get caught, well, you thought the machine rang up everything - sorry I'm not a checker, I'm a consumer. This especially works well with larger items you don't have to bag. Be sure to go through the motions trying to scan everything - the wireless scanner works good for this because half the time it doesn't register so you're always looking like you're trying to scan more than the number of items on video.

The Stowaway. This technique works well in a variety of situations, even when dealing with an actual cashier. Hide an item underneath another item, but make sure the heavy/large item on top has the UPC showing so it isn't moved around. Also, make sure whatever you're hiding underneath the item doesn't have an RFID tag. You'd be amazed what can be "accidentally" found underneath a 40 pound bag of dog food. Again, just remember if you try to do this with something too expensive, it probably has an RFID on it and you'll have problems. But there's lots of stuff that won't.

The Hookup. I routinely do this in big box hardware stores just to see how lazy humans can be. For example, I just picked up some plumbing parts. Different adapters. I attached several of them together with only one UPC tag obvious, and they didn't realize it was three separate items. Even easier to double or triple-dip with the robots.

Now let's talk about exiting the store.... If you're shopping at a store that forces all consumers to wait in line and have the number of items checked and individually counted, this trick is a lot harder to do, and I don't recommend trying in those stores. These are usually the "membership clubs" which actually require you to agree to such exit-gestapo tactics in return for being a member. Regular retail outlets can't "detain" you like this - you didn't sign an agreement to shop there; you didn't pay a membership fee. Once you bought your stuff, you are free to go.

For the non-membership stores, it's really quite simple: just leave the store. Yea, there's sometimes a "receipt gestapo" near the exit, but *never* volunteer to stop and hand your receipt to them. Just blow through the exit, not making

eye contact and holding your keys in one hand, receipt in the other like a good little efficient consumer. If they're checking somebody else's receipt, blow by them and head outside. It's perfectly normal. They are not expected to check everybody's receipt, and most of the time they are not allowed to chase after shoppers who don't comply - that's a liability issue for them. Most big box stores even have a policy to not chase obvious shoplifters. If you're stopped by the receipt gestapo, let them take a look. They are unlikely to do a full audit of your basket - they'll just look for obvious items on the receipt. They aren't paid well enough to give two shits that you paid for three cans of soup but have four in the basket - not that they'd catch it anyway. And if they do catch a discrepancy, you simply say, "Really? I thought I scanned that." Big whoop. Go back and scan it. That's the worst that could happen.

Additional guidelines: Do *not* be greedy. The objective here isn't to generate a lot of money. The objective is to penalize the corporations for their anti-worker, pro-profit-at-any-cost mentality. If I can get one item free every time I go to the store, I feel like I've "won" a small skirmish. It's now a point of personal pride to hone my skills in this respect.

It's important to note that every big box store has an allotment of acceptable "loss." They can lose inventory a thousand different ways, and they don't really care. They make up for it a million other sleazy ways as I've explained earlier.

For those that say, "Don't do this. It will only cause product prices to increase and you'll end up paying for it later." Ha ha... not buying it. This notion is predicated on the bullshit idea that shareholders should make their money first and foremost before they'll ever cut consumers any break, and is the whole reason why more people should be doing this. If we're second class citizens and the rich people getting richer is the priority, all bets are off. I'll serve my own interests before yours every chance I can get, just like you'd do to me. It'll cost you more to "pass it on to the consumer" one way or another. I *refuse* to accept it as a universal truth that executives will always get paid while the little man gets the shaft. And you shouldn't buy into that notion either. That's the same mentality that claims unions hurt workers more than they help. It's BS.

Good luck with your POJ training!

An Atavistic Freak Out, Episode Six

by Leon Manna

This story is a work of fiction.

I have dark circles around my eyes.

Leon holds up... I know that. I don't know why though. They still think that's who I am and apparently haven't even considered the fantastic possibility, or the reality, that I'm *not* Leon. I just can't figure out how. It doesn't make sense. Did I really fine tune him to be that believable? They didn't get my DNA before I "died." Maybe some bureaucratic error fucked it up? Paperwork got shuffled wrong, or placed into the wrong file cabinet, or a shredder, or an evidence room that caught on fire? But why question a good thing?

They had Moe take an MMPI test - Minnesota Multiphasic Personality Inventory - and he matched the personality type I had after they did a profile. So close, in fact, that I see them as morons for not considering if we knew each other beforehand, because we did. Moe was one of my best friends in high school. He did me one last favor: he didn't tell the FBI that I was actually named August, I faked my own death when I was 19, and I've been living under a synthetic identity since then. He didn't lie; he just neglected to tell the truth.

…

Pierre was a tall guy Lenny knew down at the bottom of the U.S., the Atlantic southeast. They were friends when he was there, I believe. He had black hair and a smile on his face. You're in good company. He insisted that he wasn't French, despite his name. I think he was Irish.

And now we had Georgia's best compulsive boat thief. It was his specialty, his art. Usually he disables the GPS on the boat, drives it around, and then puts it back where he found it. He never keeps the boat. I guess he's just a nice guy. He's also a math genius, which I think helped his navigation skills. I watched him hash a string by hand with a pencil and paper. It took him seven minutes and the hash was correct. And he could get us to Cuba. Somewhere else from there, maybe....

We were driving through this tropical jungle in Savannah, Georgia when Lenny suddenly started shouting to pull

over. I did, and we were outside of this construction site for an almost finished house. Lenny reaches over and honks the horn for me. Thirty seconds later I see Pierre shamble to the doorway with a gasoline can, leaving a trail behind him. Holy shit, I thought, I think I know what's about to happen. He tossed the cigarette on the trail, and walked up to the car with that smile.

"Who the hell is this?" I asked Lenny.

"Drive! Drive, motherfucker, drive!"

I knew better than to stay. As I floor it and the car bursts forward, the great red bang of the house's final breath went into the air, shattering my ear drums and any sense of peace. I took two hydroxyzine tablets. He filled the basement with gasoline.

"I used my lucky cigarette. Last one I'm ever smoking," he said. "Ever."

They got us in Miami. There we were, standing on this dock, the three of us, drinking some rum because we had *just* made our grand escape and now we were off to start a new life as we had a ride to Cuba. And we were just ready to get on our way when I saw someone walking down the pier towards us. Me and my attorney squint to see who it was, and it's some guy around my age wearing some joggers and a hoodie. He comes up to me and shakes my hand, says, "Leon?"

And so I said, "Who might you be, you... Fuck?"

"Are you Leon?" I look at this hoodlum who can be no older than me, thinking, what harm could it do? He doesn't *look* like a cop, he's just some dude. Maybe Lenny knows him.

So I look at Lenny, who stares at me silently, and I look back and say, "Yeah. That's me."

From behind me, I hear Lenny say, "Idiot."

And then, all these years later, it hits me that this is Moe. This is Segev, that many years older, with a sharper jaw and a beard, and now he was wearing his glasses. It's been so long, I didn't recognize him. You know, I wasn't even mad I was getting arrested. I saw my old friend again, even if he's taking me to prison.

And so he throws some cuffs on me and says he finally got my ass when it hits me, and as I look behind me I notice he's taken his badge out. I'm pretty drunk at that point. Immediately my attorney jumps towards him, screaming about probable cause and demanding that he take the cuffs off me at once.

"They have someone coming for you too, don't worry."

Lenny cusses at him and cites some legal code that I didn't know. Moe made a weird face, and said, "Whatever. But you're not going in the same car." I turned around to see what Pierre thought, but there was nobody behind us. Just an empty harbor, the waves churning peacefully.

In the back of the unmarked car, we drove towards a police station somewhere... I don't remember. Me and Moe made eye contact for a second through the rearview, and both chuckled. We had been making frequent phone calls, which started out as him trying to convince me to turn myself in but turned into friendly conversations and then a verbal backhand from me at the end before I abruptly hung up.

"I finally got your ass."

I said, "You know, I shouldn't have doubted you."

"You should have seen the office after what you did. First our computers stopped working... heh... and then, when the evidence room caught on fire, the front desk guy... he.... Hahaha.... He shat himself!"

I'm starting to see a pattern. It's like my presence, or even the very *ghost* of my presence makes people shit themselves. Or maybe I'm just schizophrenic. "That wasn't me. It was Luke. Luke Lemon."

He smirked. "You're so fucking dumb. Hehehehe...."

"I lied, his name was Nash Nashville. He was from Memphis, Tennessee."

Moe chuckled.

"No, actually, it was a man named Austin. Austin Texas."

When the unmarked car got to the station they had both - this time deviating from the pattern - vomited from laughing so hard. But the taxes paid for the car to be cleaned. I don't think they ever really got it all out, and there was a little ketamine in my vomit so the car is forever tainted when it comes to evidence.

Our story is almost over. There's one more part I have to tell you before I say goodbye.

Are we going to prison? Maybe! Find out next time!

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.

December 27-30
Chaos Communication Congress
Hamburg Congress Center (CCH)
Hamburg, Germany
events.ccc.de

January 20-22, 2023
ShmooCon 2023
Washington Hilton Hotel
Washington DC
www.shmoocon.org

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

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

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

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

For Sale

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."

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

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

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/

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).

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.

Help Wanted

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

VIRTUAL ASSISTANT/PROGRAMMER NEEDED. I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 97051

Announcements

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.

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.

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

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.

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!

Services

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

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

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/

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.

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

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.

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.

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.

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.

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

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.

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.

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: 12/9/22.

INTRODUCING
A NEW HOPE FLASH DRIVE

That's right, we have every talk that was given at this 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.

"The lowest form of popular culture - lack of information, misinformation, disinformation, and a contempt for the truth or the reality of most people's lives - has overrun real journalism."
- Carl Bernstein

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: Amit Malsar, Laurie Anderson, Buffy Sainte-Marie, Raja Baath, Mills Brothers, Holger Czukay, Mato Wayuhi
Shout Outs: Shinnecock Nation, Huw Edwards, Hope To See You, Dimorphos, Cheshire, Maverick, NAFO
R.I.P.: l0cke, Peter Eckersley

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 1988-2021
are $7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2021) 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 RETURNING - SLOWLY BUT STEADILY.
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!

CANADA

Alberta

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

IRELAND

Dublin: The Molly Malone Statue on Suffolk St. 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): Kungshallen food court, Kungsgatan 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.

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): Goozlepipe & Guttyworks, 910 King St.
Titusville: Krystal, 2914 S Washington Ave. 6 pm

Kansas

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

Maine

*** Portland (@Maine2600):** Open Bench Project, 971 Congress St. 6 pm

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm
Hyannis: Barnes & Noble, Cape Cod Mall. 6:30 pm

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 Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, 1244 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.
Fairfax: PH3AR/NoVA Labs, 3850 Jermantown Rd.

Washington

Seattle: Cafe Allegro, 4214 University Way NE (alley entrance), upstairs. 6 pm

*** indicates Thursday meeting**

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

Colorful Payphones

Spain. This pleasant looking model was found in Pontedeume, Galicia and is owned by Telefónica, the oldest communications company in Spain. Their old "T" logo can still be seen above the receiver. Unfortunately, the phone is not in service.

Photo by Francisco J. Tsao Santín

Gabon. This grimy but intact model lives in the train station in Booué. But when picking up the receiver, nothing was heard.

Photo by Vernon A. Thorax

Vatican City. Discovered by the Sistine Chapel, this bright yellow phone only works with cards that you can buy at the local post office.

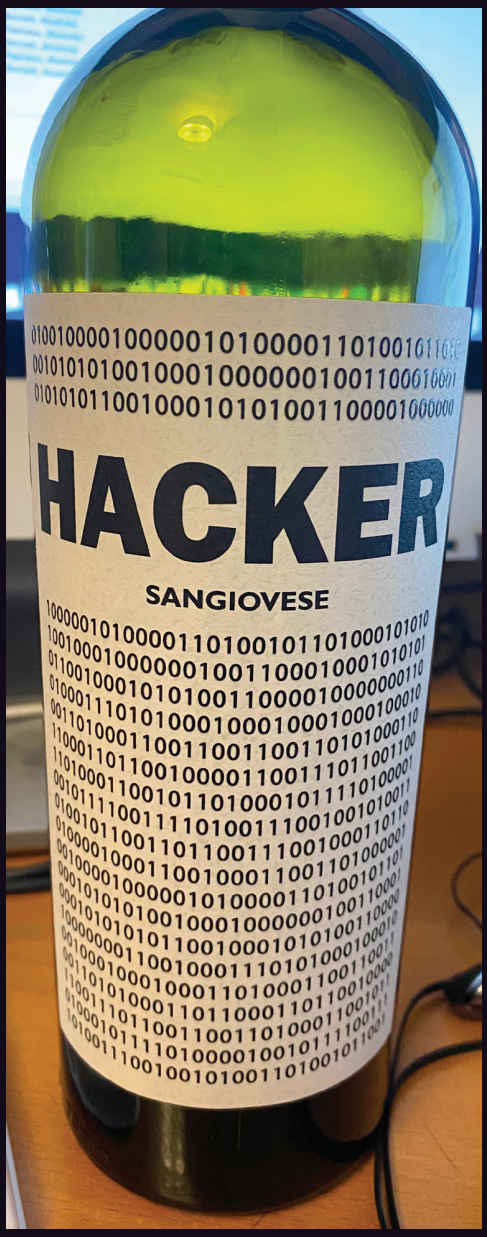
Photo by Matt Anderson

Israel. Spotted inside the old city of Jerusalem inside the Greek Patriarchate, this payphone still has a dial tone, but can be used to make free calls only.

Photo by Babu Mengelepouti

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



This was found by **Brandon** on the 2600th step of the Manitou Incline in Manitou, Colorado and it deserves a special mention because it means he had to actually climb that many steps in order to take the picture. (And it's close to the top as there are a total of 2768 steps!)

Yes, this is quite real. Made by the Ferro13 winery in Verona, Italy and discovered by **Patrick Bureau**, we have yet to try it but fully intend to. They also have wines called Nerd, Link, and Hashtag, among others. None of us were in the mood to try and decode the binary, but we'll probably have done it by the time this issue hits the stands.

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.