Volume Thirty-Nine, Number One!
DIGITAL EDITION

2600

The Hacker Quarterly

Foreign Payphones

Ukraine. Seen in Dnipro less than a month before the invasion, we can only hope this phone and the adjoining postal box still exist. The building was damaged by a Russian missile on 12 March.

Photo by Svyatoslav Pidgorny

Honduras. From Copán Ruinas, this one has definitely seen better days. The phone itself looks well maintained apart from the obvious issue.

Photo by Nicolas Stavros Niarchos

Malaysia. Discovered on Langkawi Island, this phone exudes a defiant tone. A real fixer-upper.

Photo by Zak Cunningham

Turkey. Found next to an elementary school in the Fatih district of Istanbul, this model looks both heavily used and well maintained.

Photo by Ammar Husami

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 (Do not send us links as photos must be previously unpublished.)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

Missiles

Renewed Hope

The last couple of years have been hell for many of us. But we're cautiously optimistic that we're seeing the end of it, or at least that we've moved past the worst part.

This summer, for the first time in four years, we're having an in-person HOPE conference. That may not sound like a big deal, but for so many of us, it really is - and for so many reasons.

Let's not forget how fractured and divisive our nation has become, and how we started to see this within our own community in 2018 - and how woefully unprepared we were for that. Since then, we've spent a great deal of time improving how we respond to potential issues and in recognizing those issues in the first place. Running a conference is a series of very draining tasks, and it's essential to allocate resources in the right areas. The support we've received has been phenomenal and we've had four years to develop a terrific team. While our 2020 virtual conference was a true highlight of global coordination and a model of inclusiveness, we're really looking forward to doing all of this again in person.

We had already made the decision to leave our old home at Hotel Pennsylvania before being forced to go virtual in 2020. Greed appeared to be the predominant business model at Vornado (the hotel's parent company) when they tripled the rate for us to have a conference, which would have made it impossible for many of our loyal attendees to be there. This, after we had helped the hotel get much better Internet service and also save it from demolition the previous decade. In the end, Vornado's greed came right back at the hotel itself, as they doomed it to destruction, resulting in the loss of nearly 2000 affordable hotel rooms. It will be replaced by a luxury office tower that will benefit relatively few. It's a real tragedy, but we had many good years there - and we all did everything we could to keep it going. It's time to build new traditions and memories.

So three massive milestones are coming together at the same time: our first get-together after our nation went a little nuts with divisiveness, the first gathering since COVID-19 hit us all, and our debut in a brand new home: St. John's University in the New York City borough of Queens. It's a lot to take in. And we know it won't necessarily be smooth as we adjust to so many new ways of doing things. Those of you who were at our very first conference in 1994 can attest to this, as chaos reigned while we grappled with an overwhelmed registration system in our opening minutes. We got through it then - and we'll get through whatever lies ahead - because of the support, expertise, and patience of our amazing attendees. In this community - which goes well beyond HOPE and *2600* - there's nothing that can't be accomplished with our ingenuity and positive outlook.

While HOPE's new home is capable of much larger crowds than the hotel could accommodate, we intend to ease into things gradually so that it's not too overwhelming and so that we develop quality over quantity. If you're amongst the first attendees to this new chapter, you will be a part of history, and you'll help play a big part in HOPE's evolution.

***

As is often the case, new chapters can go in all sorts of different directions. And as we started to take the first steps towards a post-COVID world, along with the recovery came the terror of war in Europe. For the first time since the conflicts of the former Yugoslavia in the 1990s, but on a scale that was closer to the pace of the 1940s, bombs and missiles were dropped on innocent people. A massive refugee crisis was created within days, as millions of Ukrainians fled the brutal Russian onslaught. In very short order, the whole of Europe was on edge, with fears of a much wider conflict developing. Even here in the States, there has been great concern over what Vladimir Putin might do next, as he genuinely appeared to be somewhat unhinged and paranoid, perhaps as a result

of isolation due to the COVID threat.

What has happened since that fateful day in late February when the long-feared Russian invasion began is both horrifying and inspirational. While we can examine and debate how we got to this stage in the first place, what is happening in the present is about as conclusive as it gets. A sovereign nation was invaded by a neighboring superpower simply because they were getting too independent. Civilians have been targeted from the beginning. Clear evidence of mass graves, torture, and executions by Russian forces has been uncovered from multiple sources. Yet throughout all of this, the Ukrainians - both military and civilians - have refused to yield and, at the time of this writing, have succeeded in driving the Russians back, inflicting losses that were unimagined when this all began. Russian soldiers, many of whom were woefully unprepared for this war, were sent in without adequate supplies or knowledge of what they were actually doing.

Numbers and power don't always add up to victory, especially if the other side is determined, thinks outside the box, and believes strongly in their cause. This is a lesson we must never forget.

Of course, in this age of social media, facts can be thrown away simply by labeling them as fake. We've been down this road before with everything from election results to science, but this is much worse. An overtly repressive regime is successfully shutting down all opposing voices in the media, ensuring that only its version of the facts gets out. It's at the stage where even when *victims* of the atrocities in Ukraine try to tell their own relatives in Russia what's going on, they're not believed because of the programming done by mass media, reinforced by social media.

This is where the hacker mentality comes in. While risky, it's essential that the false narrative be challenged and upended. By pooling our resources, possessing an understanding of the technology, and utilizing some clever thinking, it will indeed be possible to get the truth out. Of course, as we've learned in the past few years, that isn't always enough. But it's something.

While tempting, denial of service attacks can easily wind up hurting the wrong people. A programmer recently added some code to a JavaScript library that shared a message of peace - unless the computer accessing it had an IP in Russia or Belarus, in which case all of their files got deleted. While this would have been harmful to a government official, it also would have hurt an anti-war activist in that country just as badly. Clearly, this isn't the way to help.

People affiliated with Anonymous were able to hack a state television channel in Russia and get an anti-war message out to the viewers. Banned newscasts and footage from global media sources are routinely smuggled in with the help of VPNs. The Tor browser was designed for this sort of thing and there are many people in Russia for whom the Internet restrictions are easily bypassed. But again, we're dealing with a repressive regime here and they could go as far as trying to punish people who simply *connect* to one of these services without even knowing what they ultimately use them for.

Just as we need to remember that those who disagree with us in our country are not necessarily the enemy, we must do the same in this situation. People reach conclusions based on evidence and, if they are being given faulty data, that is where the real problem lies. Our evidence has to be better and the lines of communication must stay open.

We have to continue to examine all facts presented to us with a critical eye and call bullshit when we see it, regardless of the source. Those who conjure up massive conspiracies as their default defense or who fixate on disagreeing with the right people rather than analyze what they're disagreeing about have distanced themselves from the truth. When focusing on actual evidence, you may find yourself aligned with people you're not thrilled about being on the same side with. There's simply no avoiding that and it should never affect how you process the evidence you examine. We find that too often, it does.

These are extremely challenging times. But it's precisely these times where the ability to weigh and interpret facts while figuring out ways to get around restrictions and censorship is an invaluable skill to have. If we share what we know, figure out new ways of doing things, and keep communication channels open, we have the potential to do a lot of good in this, and any, fight for freedom.

How to Create a Practical Burner Phone for the Average User

by gh057

Introduction

On January 31, 2022, the Internet Crime Complaint Center (IC3) released a Private Industry Notification (PIN) warning athletes and attendees of the 2022 Olympic Games in Beijing to "keep their personal cell phones at home and use a temporary phone while at the Games" (www.ic3.gov/Media/News/2022/220131.pdf)[1]. In essence, the IC3 is encouraging the use of what is commonly known as a burner phone. This is solid advice for anyone who is entering an untrusted environment or who requires personal privacy above and beyond basic common sense rules. However, how does one go about creating such a device?

When you hear the term "burner phone," what do you think of? Possibly some informant in a crime drama television episode phoning in a tip from the edge of the Hudson River and then throwing the phone in a nearby trash can? Burner phones are often depicted as a tool for those looking to evade law enforcement or to snitch on organized crime. However, they have many practical purposes for the average user and are legal to create and maintain. In this article, I will walk you through the steps to create and maintain a burner phone for when you need (or want) an extra layer of protection and privacy.

A Quick Disclaimer

I am in no way endorsing, encouraging, or supporting illegal activity or behavior. None of the tips and techniques that I am outlining in this article will be a major challenge for law enforcement to overcome and should not be viewed as such. The intended purpose of this article is to give the average user knowledge needed to safely and effectively create a temporary mobile device, commonly referred to as a burner phone, for those times when they might be entering an untrusted environment or require personal privacy above and beyond basic common sense rules. Use of any knowledge gained from this article is at your own risk and discretion.

So... Why Do I Need This?

The devices that we carry with us contain so much more than just a bunch of phone numbers. Unlike the phones from 30 years ago, our modern mobile devices contain our financial information, health information, contacts, likes and dislikes, and so much more; a virtual treasure trove of information which attracts both the good and the bad. When you join a social media site, a public WiFi network, or share your information at a conference, do you really know what happens with that information? Do you really know where that information is stored and who it is ultimately shared with? The reality of our modern lives is that the only person that we can trust to truly protect our data is ourselves. Protecting our data does not just mean not posting it on social media sites. It also includes protecting data that is sent along with any websites that we visit or any services that we use. Having a burner phone enables you to put one level of separation between yourself and those you don't yet fully trust by utilizing a device that is not registered to you with accounts that are not attributable to you. Remember the old adage: "trust but verify."

So how does this help in an environment like Beijing? With a burner phone, the assumption is that the phone will eventually become compromised, so you should keep your personal information off the burner phone and use temporary email addresses and social media accounts which, if compromised, will not impact you negatively; you can simply throw those accounts away and create new ones. Remember, it's called a burner phone because you can use it and then you can lose it.

Step 0: Wait, Do I Even Need a Burner Phone? Can't I Just Use an App with My Current Phone??

- *Pros:* Apps can be easily downloaded and you don't need additional hardware to use them.
- *Cons:* Apps installed on your personal mobile device have the same International Mobile Equipment Identifier (IMEI) and can be very quickly traced back to you or used to track you.

The easiest solution, of course, is to use an app (like Burner or Hushed) with the phone that you currently already have. Depending upon your needs, this may be sufficient. If you're simply looking to create a solution so that you can maintain some level of anonymity when buying and selling through local online markets or when dating via social networks, this may be all that you need. However, when it comes to untrusted environments like the Olympic Games in Beijing, this would be the worst choice. The device itself is still your personal device with your personal apps and personal usage history on it. Should

something happen to that device, it is, as they say, "game over."

Step 1: Get the Phone

The very first step in creating a burner phone is getting the actual phone! There are many places where you can obtain these devices and I outline some of them below with pros and cons.

An Old Phone You Currently Own

- *Pros:* It's free, it's immediately available, and you can start creating right away.
- *Cons:* Depending upon where you got it, the IMEI may be tied to you personally, which means there's still a chance that the phone can be traced back to you or track you.

Much like the app solution above, if you have an extra phone lying around, this is a pretty easy solution if it fits your needs. However, when it comes to untrusted environments like the Olympic Games in Beijing, this would not be the best choice. Depending where you got the phone (i.e., were you the original purchaser and was the phone purchased new), the IMEI number can still be traced back to you and if you are easily searchable online, you can still be targeted. In addition to that, many services capture the IMEI number of devices to ensure uniqueness, meaning that even if you use the same device with two different accounts for a particular service, associations can be made. The whole idea of the burner phone is to subvert electronic identification.

Purchased New/Used From a Retailer

- *Pros:* It's new so you know that it will function the way that you expect and it has a return policy if you're not happy.
- *Cons:* It's not the cheapest route to go. There is a purchase history linking you to that device.

If you can justify the cost and you don't care that the purchase history of the device can be linked back to you, then this is a solid way to go. You get the luxury of knowing that you bought a new device, one with an expected state of quality and functionality without having to risk your safety (discussed next). Phones purchased this way are typically more expensive then the next option since quality and functionality assurances can be made. However, even if you pay cash, there is a purchase history linking you to this device, whether it's a receipt of the purchase or surveillance video of you entering the retailer at the time of purchase. If that is a concern, then this may not be the best option. Remember, outside of the purchase history, unless you associate the IMEI of this device with a preexisting mobile account, this device is not associated with you. Make sure to follow the steps about purchasing a Subscriber Identifier Module (SIM) card below to keep it that way.

Local Online Marketplace (i.e., Craigslist)

- *Pros:* The device IMEI will not be linked to you, there is no purchase history if you pay with cash, and, if you use a burner phone app and/or burner email address for communications with the seller, there is little traceable sales history of the transaction.
- *Cons:* In recent years, Craigslist and other local online marketplaces have seen their fair share of crime associated with meeting a stranger in public. In addition, you don't know what was done with the phone prior to buying it.

The next better solution (and one that I have employed regularly) is to buy a device, only with cash, by way of a local online marketplace like Craigslist. The device IMEI will not be associated with you or anyone you know, unless you have the awkward misfortune of finding out that the seller is actually someone you know. However, you don't know what was done with the device prior to you getting it, meaning, you don't know if the seller is lying to you about its condition, its repair history, if it was stolen, or even if it's truly unlocked. This said, in all my experiences of buying and selling online, I can count on one hand the number of times that I've bought a lemon from someone and it's never been with a mobile device.

A note to mention here is that these local online marketplaces have seen their fair share of crime associated with the transactions occurring from petty theft (i.e., "snatch and grab") to physical assaults. When meeting a complete stranger in public, you should always follow best practices for personal safety, no matter how nice the person seems to be.

Wait, What About the Device Itself?
What Platform Should I Choose??

This is largely a matter of personal preference. In general, the rule of thumb is that if you want to make heavy modifications to the platform, then Android is the way to go. However, if you want something that will generally have a fairly secure operating system out of the box and requires little modification, then iOS may be your best bet. In either case, the steps below, unless otherwise specified, will work for either platform.

Android Alternatives -
A Quick Plug for CalyxOS

Google Android is an open source platform. Anyone can download it, make modifications, and create something new, possibly something

with a greater emphasis on security and privacy. This was the goal of the team who built CalyxOS. If you like Android but would like something a bit more privacy focused, then I recommend CalyxOS. The platform is very stable and the flashing process is virtually painless. If you want to know more, visit the Calyx website (calyxos.org/).

There are many alternatives to the standard Google Android platform out there, including Ubuntu Touch (ubuntu-touch.io/) and GrapheneOS (grapheneos.org/), which I've heard that a lot of folks like (you can find some of these alternatives listed here: alternativeto.➥net/software/calyxos/). I haven't experimented with many of these, but I encourage you all to try them out if you're curious. For the average user who prefers an easier setup process with sizable gains, CalyxOS is a great alternative to the standard Android platform.

Step 2: Obtain a SIM Card

There are a few key steps that are legitimately required in order to ensure that protection and privacy are maintained. I outline them below. The overall goal is to minimize how much association, if any, can be made between you and the purchase of the SIM card.

SIM Card Type Depends on the Phone... and Your Needs

There are two prevailing radio technologies: Code-Division Multiple Access (CDMA) and Global System for Mobile communications (GSM). Most phones these days, especially outside of the U.S., use GSM. However, some U.S. carriers, like Verizon, also support CDMA. The SIM card that you buy will have to be compatible with the technology that the phone requires. In addition, there is a difference between SIM cards intended for 4G phones and those that are intended for 5G phones. Make absolutely sure that the SIM card you buy is properly matched to the phone you are planning on using.

Pre-Pay is the Way

Regardless of what the sales person tells you about the option being "more expensive" or "a pain to maintain," this is what you want to do. For most burner phones, you only need their use for a short time, so having a prepaid solution makes sense. These solutions allow you to add more funds to them should you need to, or you can simply let that SIM card expire and buy a new one.

How Much Data? How Much Talk Time?

Remember what the intent of this device is. This is an emergency "use when needed" phone. In other words, you shouldn't need to match your current personal usage with this phone. However, there's nothing stopping you if you wish to do that; you're just going to pay a lot more for it. Typically, a few hundred minutes of talk time and a gigabyte or so of data is plenty for a relatively short-term need and, of course as mentioned above, you can always add more funds to the prepay solution as needed.

Pay in Cash

This one is fairly straightforward and it should be noted that the same technique will be interwoven throughout this article multiple times. If you pay for a SIM card in cash, then there is not an association between you, your credit card, and the purchase of the SIM card. Typically, I go into a mobile provider with about $100 in hand to make this purchase, but it ends up being around $40. The reason for the overage is that you don't want to be caught off-guard by a difference in the price and not have a cash-based means to cover it.

No, You *Do Not* Have to Give Your Name

This is one where not everyone is going to feel comfortable having this conversation. Keep in mind that it's in the salesperson's best interest, and by association the retailer's best interest, to ask for your name, birth date, or other personally identifiable information. This way they can sell you more stuff. However, there is no law that requires you to give your name, your contact information, or even show a government-issued ID. Regardless of how much they may push, you do not have to give this information. If they are truly adamant, just find another retailer who will sell you what you need; it's not worth the argument. Also, getting loud and combative draws attention to you and, if you haven't noticed, this entire article is focused on doing just the opposite. I've been everyone from "Mark Jones" to "Jesus Christy" (yes, really) just to give them a name when they wouldn't give up. Please note I've been told that the TracFones require personally identifiable information to be activated. For this reason, I typically only use the big four (Verizon, Sprint, T-Mobile, and AT&T) because they've been consistent in the past.

Definitely Make Sure the Card Works *Before* Leaving the Retailer

Using the above process, this creates an "all sales are final" situation. So to avoid burning through good cash, it's best to make sure that everything works before you leave the retailer. Simply plugging in the SIM card and checking connectivity is all you really have to do. There may be a few hours delay with the phone actually being able to make calls due to setup within the system (the salesperson should inform you of this), but the phone itself should immediately connect to the provider.

Step 3: Add Funds to the App Store

Let's face it, there are some apps that we all rely on for stability and security, and many of those are not free. The easiest way to purchase these apps is through the platform's app store, however, that requires a credit card or pre-purchased funds. It's the latter option that we are going to employ here. Simply go down to your local pharmacy, grocery store, or big box retailer and purchase a gift card (again with cash) for that platform app store. Typically, I default to $50 just to cover my needs and any services those apps may require, but this is a personal preference.

Step 4: Create New Account Exclusive For This Phone

The final step is to create new accounts for all of the services that you want to use, and this is the key: zero association to you. This means a new platform account (i.e., Google or Apple), new email addresses, new social media accounts, etc. Make sure to turn on two-factor authentication because while we hope that this device is not compromised, we should operate with the assumption that it is or soon will be. Do not allow anyone who you know in your personal or professional life to contact you on this device with their personal or professional accounts. The only accounts that should interface with you on this device should be other "burner only" accounts.

Wrap-Up/Best Practices

Congratulations! If you reached this point, then there's a high likelihood that you successfully created a customized burner phone for your privacy and security needs. However, the journey is not over. There are some basic best practices to keep in mind when using and maintaining your new burner phone so that you maintain as much of a separation between you and that device as possible.

Never Use Personal Accounts With a Burner Phone

As mentioned above, personal accounts are, well, personal (hence the name). These accounts should stay far away from the burner phone in any capacity. In other words, don't use personal accounts on the burner phone, link burner accounts to personal accounts on social media, or converse with individuals that you know in your personal life from your burner account to their personal account. Be vigilant; we're only human and mistakes happen, but those mistakes are sometimes costly.

Never Connect the Device to Your Home or Work Wireless Network

If there's simply one thing to not do, this would be it. The process of creating a burner phone takes time, effort, and funds. The hope is that when you're done, you have a tool which you can rely on reasonably well for privacy and security. However, if you go ahead and ruin that by associating it with your home or work wireless network, then your efforts will be all for naught. If you need to update it and you require a wireless network, any good coffeehouse or community center should work just fine. Additionally, if the device was just in an untrusted environment, the last thing that you want is for it to auto-connect to your home or work wireless network.

Do Not Have Both Your Personal Phone and Your Burner Phone On at the Same Time

This issue would be more of a concern for those who are going to a place where the potential hostility may be local or national law enforcement, but is generally a practice that I employ whenever I go to an untrusted environment. If you don't trust the environment enough to use your personal device, then you shouldn't trust your personal device to be on in said environment. Instead, power down your phone and store it safely in a faraday bag. Additionally, burner phones can be associated with you if both the burner phone and your personal phone are pinging the same cell towers at the same time. The covert nature of the burner phone is significantly reduced if the owner of said burner phone can be reasonably identified.

After Returning Home, Wipe the Phone

Once you return to a secure environment like your home or place of work, it's time to wipe the phone. Yep, factory wipe that sucker! Assuming that you didn't use the phone to store any sort of files like photos, videos, audio recordings, etc., your loss will be negligible. All you will have to do is set up the phone again with the same accounts you already have access to. If you did take photos, videos, or generate other types of documentation that you wish to keep, you will have to go through additional measures to ensure that those files are extracted in a safe manner, which is beyond the scope of this article.

In Closing...

I hope that this article was helpful for you. Burner phones are a common tool that I employ to keep myself, my data, and my privacy as intact as possible when I am knowingly entering an untrusted environment. While they may have gotten a bit of a seedy reputation from television and movies, they are an effective way of reducing your risk and I highly encourage their use.

[1] Federal Bureau of Investigation. (2022). "Private Industry Notification: Potential for Malicious Cyber Activities to Disrupt the 2022 Beijing Winter Olympics and Paralympics" (20220131-001). Federal Bureau of Investigation. www.ic3.gov/➥Media/News/2022/220131.pdf

Exploring the BACnet Protocol for Fun and Profit

by Teguna
teguna@protonmail.com

I have one of the greatest jobs in the world working in the field of Operational Technology or "OT." I define OT as the place where computers meet the physical world, including devices that control and monitor large infrastructures like power grids, water systems, dams, manufacturing plants, and energy pipelines. OT also includes things as mundane as the computer system in your car, your home alarm system, or thermostats that can be controlled from your phone. My OT world depends heavily on appliances like historians, SCADA servers, Industrial Control Systems (ICS), Human Machine Interfaces (HMIs), and Programmable Logic Controllers (PLCs).

OT professionals depend on a set of communication protocols that are reliable and easy to use, but severely lacking in security features. Protocols like Modbus, DNP3, and Ethernet/IP were developed before security was vogue and they focused exclusively on availability without any concern for integrity or confidentiality. Lately I've taken a keen interest in a protocol called BACnet. BACnet stands for "Building Automation and Control Network" and is the communications protocol ubiquitous with Building Automations Systems or "BAS." If you work in a modern office or industrial building that has HVAC, lighting control, access control, or fire detection systems, then those systems are probably monitored and controlled using a BAS.

Before you blow off the importance of these systems to the overall security picture, please keep in mind that the 2013 Target hack that exposed 40 million debit and credit card accounts started by hacking the store's HVAC system. Attacks on IT enabled by attacks on OT have become much more popular in recent years because of security flaws that are very common in OT equipment. Most of us in the OT industry realize we can be the "soft underbelly" of network security. Expect attacks on OT to become much more common as the demand increases for smart refrigerators, network connected litter boxes, and even Bluetooth and WiFi connected clitoral stimulators. But I digress....

As with other OT protocols, there are plenty of free or open-source tools that can assist us with exploring BACnet/IP communications to understand how BAS communication works and its inherent security problems. BACnet/IP is BACnet communications over IP networks, which is different than BACnet MS/TP that typically uses the RS485 standard for communications. This article will be an overview of two free tools for exploring BACnet/IP and a discussion of the BACnet protocol itself. This is probably an excellent time to advise you that this article has been written for educational purposes only. To use any of the techniques in this article constitutes a thought-crime at a minimum and international terrorism in the most extreme cases. The contents of this article should never be used by anyone... anywhere... ever.

The first thing we are going to need to explore BACnet is a BACnet device. This can be accomplished free of charge by visiting Contemporary Controls, creating an account, and downloading their BASemulator. It is available at the following site: `www.ccontrols.com/basautomation/bastools.php`

You'll be downloading the entire BAScontrol toolset, which also includes Sedona Application Editor (SAE) for programming Contemporary Controls devices. You can choose only to install the BASemulator when you run the install program. The software must be installed on a Windows machine. For this project, I recommend a VM running Windows 10 and using an "internal only" network.

After you finish the installation, find the BASemulator icon on the desktop or in the START menu and load the program. Select the "Start Emulator" button to begin the emulation (the default settings are normally fine). This will also bring up a web page in your browser. The default credentials are "admin / admin." What you have just installed is a complete emulation of a BAScontrol22 hardware appliance sold by Contemporary Controls. Normally a technician would use the BAScontrol22 for control and monitoring of an HVAC or other building automation system. For our purposes, we have a free software device that emulates BACnet/IP in the same manner as its hardware counterpart. If you wanted to set up a BACnet hacking lab, you could certainly set up armies of these emulators.

There are a few things we need to do for the purpose of demonstrations later in this article. In the emulator web interface, select the "System Config" button on the bottom left. At the top of the "System Configuration" page that pops up, change the "Device Object Name" to "Thermostat" and hit the "Submit" button at the bottom right of the page. After returning to the main page, select "Restart Controller" on the bottom right side (nothing will appear to happen, but the controller will reset). Select the "Virtual Points" button in the bottom middle of the page. Double-click "Virtual Point 1" and bring up the Object Configuration page. In the

middle of the page, change the "Object Name" to "RoomTempSetting" and select "Submit" at the bottom of the page. Close the window. Lastly, select the check box under our newly named "RoomTempSetting" on the Virtual Points page. This will allow you to change the value of "0.000" to "72.000". After you have changed the value, uncheck the box and close the window.

A few fun facts about BACnet/IP that you will need to know as you play with this protocol:

- BACnet/IP devices use UDP for communication and BACnet/IP is served on port 47808. 47808 converts to hexadecimal BAC0. Clever and easy to remember, eh?
- BACnet devices are always organized as a series of objects with each object having a set of properties. The device itself is an object (with an object-type of "device") with properties like an instance number and vender identification. Object types like "analogInput", "analogOutput", "binaryInput", and "binaryOutput" are very common in BACnet devices. Expect to find many different properties for each of these objects to include present-value, units, and description.
- You will interact with objects using services supported by the BACnet appliance. The "ReadProperty" service is a mandatory service in all BACnet appliances, but "WriteProperty" is supported across most devices. The WriteProperty service will offer us the most fun as a BACnet researcher.
- When we are "on the wire" with BACnet/IP packets, binaryInput and analogInput object types are read Only. binaryOutput, analogOut, binaryValue, and analogValue object types are both read and write, meaning we can use the "WriteProperty" service and change their values remotely.
- BACnet/IP makes extensive use of Broadcasts for network communications. And yes, it is entirely plausible to conduct a Smurf attack to DOS devices using BACnet/IP protocol.
- A key advantage for an attacker is that BACnet devices are blabbermouths. They just want to tell you everything about themselves to include all the objects and services they support. I'll demonstrate this in the paragraphs that follow.

Let's spin up a Linux machine with Nmap installed (Kali Linux would do just fine) and ensure that it is on the same subnet as our BASemulator machine. Type the following command:

```
$ sudo nmap -sU â€"script bacnet-
➥info -p 47808 192.168.56.0/24
```

Set the subnet to whatever you're using in your lab or just direct the scan at the IP address of the emulator. In my case, I used the VirtualBox default internal network for my devices. Your scan should come back with something like this:

```
Nmap scan report for
➥192.168.56.103
Host is up (0.00035s latency).

PORT      STATE SERVICE
47808/udp open  bacnet
| bacnet-info:
|  Vendor ID: Contemporary
➥Control Systems Inc. (245)
|  Vendor Name: Contemporary
➥Control Systems, Inc.
|  Object-identifier: 2749
|  Firmware: 3.1.28
|  Application Software: 1.2.28
|  Object Name: Thermostat
|  Model Name: BAScontrol
|_ Description:
MAC Address: 08:00:27:D7:C0:D7
➥(Oracle VirtualBox virtual NIC)
```

That is a ton of valuable information from a research perspective, which is why I enjoy this Nmap script quite a bit. Did you notice that the property of "Object Name" above for the device now has the name "Thermostat" like we assigned earlier? You should especially take note of the Object-identifier and the IP address. We are going to use both of those to learn even more information after we install BACpypes on our Linux machine.

BACpypes is a BACnet module for Python. I always keep it in my arsenal because it's freeware and can support anything I want to do in BACnet/IP. Use the following link for simple instructions to install and configure BACpypes. Download the git repository to your home directory in Linux for the rest of the examples in this article:

```
bacpypes.readthedocs.io/en/latest
➥/gettingstarted/gettingstarted
➥001.html
```

Configuring your BACpypes.ini correctly is particularly important, so pay attention to that area of the tutorial. Our network does not have a BBMD so don't sweat it. The ~/bacpypes/samples directory is chock full of useful tools for information gathering on BACnet devices and manipulating BACnet devices. I think you should explore all of them, but let's cover just a couple.

From your ~/bacpypes directory, type the following command, replacing the IP address with the one you discovered in your earlier Nmap scan:

```
$ python3 samples/ReadObjectList.
```

```
➥py 2749 192.168.56.103
```

The blabbermouth BACnet device is going to tell you everything. In this case, you are using the ReadObjectList program to get a list of all objects on device instance number 2749 at IP address 192.168.56.103 (both were passed to the program as parameters). The BASemulator has responded with a complete list of all object types, instance numbers, and object names presently on the device. In the list, you will see the "object Identifier" enclosed in parentheses. The object identifier is a combination of the object type and the instance number and we will need it later. Two stick out because we changed their object names when we set up our emulator:

```
('device', 2749): Thermostat
('analogValue', 201):
➥RoomTempSetting
```

Assume for a second that a similar device is servicing an HVAC system in a large office building. I would expect that the engineer programming the device is going to use descriptive object names in order to identify where the device is (for example, "HVAC Plant BLDG 1234") and what points it monitors ("RoomTempSetting", "ChillWaterTemp", or "OutdoorTemp"). This practice will allow technicians to better service the device during trouble calls. Object naming makes BACnet/IP a powerful tool for simplifying programming and maintenance, but it also makes reconnaissance against BACnet devices much easier than OT protocols like DNP3 and Modbus.

Let's read some values from the device using BACpypes's ReadWriteProperty program:

```
$ python3 samples/
➥ReadWriteProperty.py
```

The program will present you with a new prompt ">". Enter the following command:

```
> read 192.168.56.103
➥analogValue:201 presentValue
```

If you followed my instructions earlier, the program should have responded with "72.0" and given you another prompt. Let's pretend for a second that we are an attacker, and we want to turn up the temperature in the boss's office. Let's try:

```
> write 192.168.56.103
➥analogValue:201 presentValue
➥88.0
```

The system responds with "ack" and gives us another prompt. We were able to write to the point because analogValue is Read/Write and we can use the "WriteProperty" service to change its properties remotely. If you repeat our previous read command on the same point, you'll see that that "RoomTempSetting" presentValue has been increased to 88.0.

But what about digital? Let's choose a random binaryOutput object from our list and execute a read command:

```
> read 192.168.56.103
➥binaryOutput:18 presentValue
```

The system responds with "inactive" and gives us another prompt. Binary values, as you know, are either 1 or 0, true or false, high or low. In this device, inactive refers to false. In order to make this point "active" or true, we enter:

```
> write 192.168.56.103
➥binaryOutput:18 presentValue
➥active
```

The system will respond with "ack" and a new prompt. Repeating the read command from earlier will show that the presentValue property of the binaryOutput:18 object has switched to "active".

I have merely given you a taste of BACnet and I encourage you to explore BACnet more in your own lab. The BACpypes package has a variety of sample programs that are fun to play with and can be used to learn more about BACnet/IP. Be sure to use Wireshark and analyze the APDUs that are generated when BACnet devices communicate. Use the Sedona Application Editor (SAE) from Contemporary Control to program your BASemulator. Happy hacking!

Sources

1. Peter Chipkin. "Bacnet for Field Technicians." cdn.chipkin.com/assets/➥uploads/2018/mar/15-19-09-42_➥Bacnet_For_Beginners2.pdf, 2018.

2. BACnet International. "Introduction to BACnet For Building Owners and Engineers.", www.ccontrols.com/pdf/➥BACnetIntroduction.pdf, 2014.

3. Jaspreet Kaur, Jerneq Tonejc, Steffen Wendzel, and Michael Meier, "Security BACnet's Pitfalls." link.springer.com/content/pdf/10.1➥007%2F978-3-319-18467-8_41.pdf,➥2015.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! All of a sudden, the world has dramatically changed and, as of this writing, we're suddenly back to a Cold War footing. For nearly all of my adult life, the world has been getting smaller. I have never thought twice about flying over Russia, or even through it (while I was living in Beijing, one of the best and cheapest ways to fly to Europe was via Moscow on Aeroflot). Now, quite suddenly, each option has become both impossible and almost unthinkable.

This leaves me wondering what the state of telecommunications will become. Many authoritarian countries allow open and unfettered access to telephony (while often also censoring the Internet). In fact, some such countries are even regional telecommunications hubs. They're definitely employing surveillance tactics, but these are also countries with the resources to acquire and use software (such as Palantir) to identify surveillance targets. Other countries, such as the Democratic People's Republic of Korea, sharply limit international telecommunications capacity. This is done both to limit interactions with people outside of the country and to ensure that every call can be monitored in real-time.

One of my favorite things to do in middle school during my lunch break when calling from the payphones (I was always calling something or somewhere from the payphones - often small, obscure airlines to ask for copies of their timetables to be sent) was to make international directory assistance calls. Back then, international calls were connected via satellite after analog microwave hop to the AT&T Roaring Creek Station satellite center in Pennsylvania. To call international directory assistance, you'd call an AT&T operator (by dialing "00") and request directory assistance in the given country. The operator would get you on the line with a directory assistance operator in the other country, drop off the line, and you could then do whatever.

Now, this could be a great way to blue box. You could seize a trunk in mainland China and call outbound from there to anywhere in the world, courtesy of China Telecom (of course, it was a double satellite hop and the quality was terrible, but it was possible). Although Israeli directory assistance was immune to blue boxing (they had effective countermeasures), the phone lines were apparently staffed by bored military conscripts. They were young, and they weren't strictly supervised. We would sometimes add them to a conference call full of hackers and phreaks and they'd just roll with it, telling us about their lives in Israel.

I liked calling Bulgaria directory assistance in Sofia. They put you on hold forever, so sometimes the AT&T operator would just drop off and leave you on hold with them. They'd play a recording in three languages (Bulgarian, Russian, and English) saying "Hold and operator will answer." I'd call up, get put on hold, and hand the phone to a random kid in the hallway. Of course, they didn't know that Bulgaria was a separate country, so they'd think I'd put them on the line with Russia. The "on hold" recording sounded positively Soviet. It also didn't help that Bulgarian directory assistance operators were particularly curt and abrupt.

The one country that was *really* hard to call was the Soviet Union. There were only a handful of available trunks, and directory assistance calls used the same trunks as any other call being placed to there. Although most countries could be direct dialed, the Soviet Union couldn't be. To make a call, you'd first call the AT&T operator, and you'd have to schedule a time where they'd try to get through. They'd first call you back at whatever number you gave them and, once they had you on the line, they'd make the call when the trunk was free. So, imagine a room full of KGB analysts in Moscow and a room full of NSA analysts in Pennsylvania, all listening intently while you asked a Soviet directory assistance operator for the phone number of "IP Freely" and that's probably a pretty accurate picture of what I was doing. I'm honestly surprised the FBI never showed up at my middle school to ask me to knock it off.

Through free directory assistance calls, I was able to get some phone numbers of McDonald's locations internationally, as well as some random Subway locations in Australia. It was always good fun on c0nfs to call up a Subway "down under" and quiz them about the menu. If you got them during a slow time, they were good sports about it (as Aussies always are). They'd shoot the breeze with you until a customer came into the store. McDonald's locations were harder because these were always busy and it was usually the manager answering. They didn't have time for chit chat; you'd have to pretend you were calling from headquarters with a business question in order for them to spend any time talking with you, and they'd hang up on you immediately when they realized it was a prank call.

One popular location for blue boxers to call was Scott Base, Antarctica. A phreak who had worked at McMurdo Station in Antarctica put the Scott Base phone numbers into a text file that circulated on BBSes, and one of the phone numbers was the bar at the station. McMurdo and Scott Base are adjacent to one another, and the summer population is over 1,000 people. Both McMurdo and Scott Station have a bar, and if you called the phone at the Scott Station bar on a busy night, you'd get to talk to everyone! People working in Antarctica are busy, but they were exceptionally friendly on their off hours and they were seemingly happy to talk to anyone who isn't one of the handful of people they already knew. I'm sure that the Chinese government was puzzled by all of the satellite time used to call Antarctica.

I don't often talk about the past, but it's important to realize that, not so long ago, there were real and significant barriers to being able to communicate with people all over the planet - something we take for granted today. Today's world is so hyper-connected that it's difficult to appreciate how difficult and expensive it was for ordinary people to connect with one another, just because we lived in countries with different political ideas. Long before I began exploring the world physically - visiting 73 countries and territories at last count - I was exploring it virtually by phone. There can still be significant barriers to physical travel, but even as late as the 1980s, the barriers to making phone calls were nearly as high (it could take several days to successfully get a call through to the Soviet Union).

Many readers have grown up in today's world where borders barely exist and where communication has increasingly few barriers. I'm honestly not sure what the future looks like. I do think the more that we talk to one another, the less power that centralized propaganda can hold over us. Propaganda works - whether it's Fox News, Russia Today, or CCTV. However, person-to-person communication is one of the few things that can effectively break through propaganda, and this is one of the reasons why governments try so hard to limit it. I personally hope we don't return to the Cold War of telecommunications.

And with that, I wish you a peaceful summer. I'll be at HOPE in New York in July. As of this writing, my formal participation is not yet confirmed, but I hope to see all of you in a wonderful new venue that I'm really excited to experience. Until then, stay safe, and don't forget your red box!

References

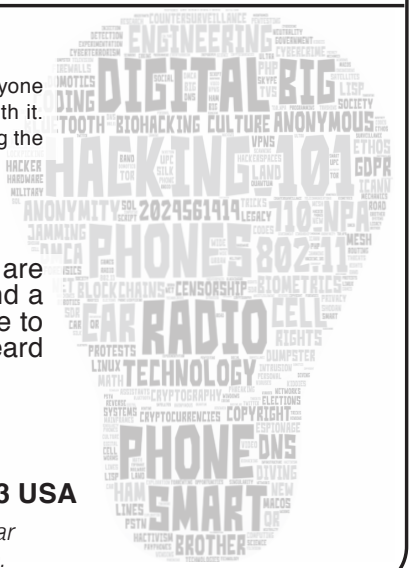
https://en.wikipedia.org/wiki/
➥Roaring_Creek_Station

WRITERS NEEDED!

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

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

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



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

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

How to Use Gmail to Send Emails From an SMTP Server That You Do Not Own

by duykham

I would like to share with you one way to set up Gmail to send emails so that they could appear as if they were sent by an SMTP server that you do not actually own, e.g. your company email. (Normally, many employers do not want you to check and send emails with your own computer so they do not give you the setting.)

In fact, the emails are sent by Google servers. I'm not talking about the services like Google 360 which allows you to achieve the same thing, but you have to pay for it. Also, Google 360 often requires you have ownership of the domain itself. What if you are trying to send emails as your company's email addresses? You do not own the company's domain.

This is a bug of Gmail; I don't think they meant to set up Gmail like this. However, when I informed them about this bug, they didn't seem to understand what the problem was and said it's intentional. Anyway, since I couldn't make the Google employees fix the bug, it is still there. Now I'm sharing it with you.

A Quick Introduction of the Bug

Gmail lets us "Send email as" external email addresses (in Settings --> Accounts and Import), e.g. someone@company.com so that you can send emails using the Gmail web interface, but the recipient will have no idea the emails were sent via Gmail. They will look as if they were sent by an independent SMTP server (such as the one belonging to your company). This is a cool feature. But, there are two big problems:

Firstly, when setting up the account, Google does not require you to enter the exact credential for that account from company.com, but any account from any (I really mean *any*) other domain could work. That's very strange, isn't it?! You are trying to add someone@yourcompany.com to your Gmail, but instead of providing username and password to show that you have legitimate access to that account, you can use any username/password from any other accounts that you personally own (e.g. soneoneelse@yourdomain1.com, whoever@yourdomain2.net,...).

Secondly, the confirmation of authentication to that SMTP account happens only once, at the time of setting up. That means, every time you send emails ("Send email as" from Gmail), it will not verify your username and password again. It just sends emails as if the account is still valid.

Thirdly, Google makes it worse by falsely affirming that the email was sent by company.com's SMTP server (via TLS, even). (You can check this info by showing the detail information of the email on the recipient's email client.) This is a white lie! They are all sent via Google's servers. All the emails are still sent perfectly even if the username/password has changed or either company.com or yourdomain1.com or yourdomain2.com does not exist (at the time of sending the emails) anymore.

Consequences? Suppose later on, you lose the access to the account (either you are unsubscribed from the service, you are fired from or quit the company you worked for, etc.), you still can perfectly send emails from Gmail as if you still own that company's email. Imagine, once you quit the company and one day you decide to scare all of your former customers with some fake and shocking news. They will believe you because they think you were still working for the company. All thanks to Gmail.

Of course, there are also other good uses to take advantage of this bug; it doesn't have to be all malicious. I will let you decide and choose what suits you best.

I will just provide some technical insight. The rest all depends on your creativity.

So here we go. This is how to setup Gmail to send emails as if they are sent from an SMTP server that you do not own.

Goal

Use your Gmail to send emails as if they are sent by someone@company.com. (This someone@company.com can be either your own company's email that you currently have access to or it's just from one of your careless colleagues that happen to leave their laptop screen on, I don't know....)

Prerequisite

You can read the emails of someone@company.com at the moment of setting up (only that moment is enough).

Setup

1. First, log in to your Gmail.

2. Go to "Settings", and then click to "Accounts and Import" tab.

3. Under "Send mail as:", click "Add another email address".

4. A pop-up window will appear. You fill in with your Name (e.g. "Someone") and the Email

address (e.g. "someone@company.com"). The click "Next Step".

5. In the next screen, you will need to fill in SMTP server, Username and Password. Here comes the interesting part, you *don't have to* use the setting of the email you entered in the previous step. Instead, you can use any of the SMTP account settings that you know, even some free ones on the Internet.

6. Make sure to check "Secured connection using TLS". Yeah, why not?! And click "Add Account".

7. Next, Gmail will check if the SMTP setting you entered is correct. Note that, Gmail *does not check* if this setting comes from the same domain as the email address you are trying to add (which is company.com). Since you own the SMTP account, I suppose you entered the correct info and that there will be no problem with the username and password.

8. Next, after verifying the SMTP setting, Gmail will send an email notification to someone@company.com with the "Confirmation code". This is when you need to check someone@company.com and read the email from "Gmail Team" and get the code. Normally it's nine digits. Fill that in at "Enter and verify the confirmation code" in the next screen.

9. Click "Verify".

10. If you follow exactly what I said, you should be done by now. You can verify it by going to "Settings" and "Account and Import" again. You will see that someone@company.com has been added to "Send mail as".

How To Use

It's straightforward: every time yo want to send an email with someone@company.com address via Gmail, just select it from the "From" drop down menu in the "Compose" window.

Happy "cheating" - I meant, hacking!

FOIA as Weapon

by Radar Lock
radarlock@protonmail.ch

FOIA - the Freedom of Information Act - is a citizen's most powerful tool in the fight against government corruption. This federal law, and its state level counterparts, are (in the right hands) a battering ram for breaking down government secrecy and shining a spotlight into places bureaucrats do not want anyone to look. I spent four years as a newspaper reporter and, much like a hacker, I was always looking for new exploits in the way the law could be applied for investigations. Eventually I grew tired of the dog-eat-dog world of journalism, learned how to code, and jumped ship for the tech industry. But I learned a few tricks along the way (and developed a few of my own) that might be worth sharing.

Tip One - Everything They Have is Fair Game

Most FOIA users ask for conventional items: letters, emails, documents. Don't limit yourself to these, because the interesting stuff lies elsewhere. If, for example, you have reason to think that the county prosecutor is up to shenanigans, ask for his entire web browsing history. His complete phone records can usually be found on his phone bill. Asking for all his emails would be considered excessive, but asking for the metadata for an extended period - subject, recipient, timestamp - is not and may point you in the right direction. And if our prosecutor is unlucky enough to be the user of a government-issued cell phone, or is receiving a government stipend for his personal cell phone, every record therein contained is yours for the taking, up to and including the official's voicemails and Spotify playlists.

Tip Two - Format Your Request as a Question

Government officials are rarely under any obligation to answer your questions, and they do not have to create new records in response to your FOIA requests. However, if you word your FOIA request as a question, it can force them to provide the answer through documentation. For example, if the municipal dog pound is not releasing data on how many animals it euthanizes, you might word a request thusly: "I request such records as would demonstrate how many animals were euthanized in the third quarter."

Tip Three - File a FOIA on Your Own FOIA

This is called a Meta-FOIA. It lets you know how the government processed your FOIA request - who was talked to, where they looked, and oftentimes exactly what they think of you.

Tip Four - Blackmail Their Lawyers

A lawyer values nothing more than they value their law license. This is an Achilles' heel that can be used in your favor, and it is my favorite trick. *Always* try to get a governmental body to handle FOIA requests through their lawyer. When they deny your request for some invalid reason, you can leverage the "Rules of Professional Conduct" (which most states have adopted as their code of ethics for lawyers) to force them into fulfilling your request.

For example, I was once on deadline for a major story, and an agency's lawyer denied my request for critical documents. I was faced with months of delays if I challenged this the conventional way when the story was needed immediately. Luckily, this lawyer had broken a state FOIA law, which I pointed out was a violation of the "misconduct" section of the ethics code. The ethics code also has a rule called "Respect for Rights of Third Persons," which states that "a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person...." Finally, I contacted the managing partner of the firm where this lawyer was employed, explained the violations, and pointed out that a managing partner is just as responsible for the violation under the code of ethics as their subordinate.

All I had to do once I had laid out the ethics violations was threaten to file a formal complaint against their licenses. They emailed me the documents I wanted the next morning. Learning the rules was boring, but once I knew them I was able to wield them with great power. If anyone tries this technique on an NSA lawyer, please let me know how it goes.

Final Thoughts

Since so many of *2600*'s readers bring politics into their submissions, I - a rare "little l" libertarian reader - cannot resist doing the same. Many seem especially concerned about January 6th, which was an event where a group of people who were largely unarmed trespassed on the Capitol, took some selfies, and stole Nancy Pelosi's dias - mostly while remaining between the guide ropes. And who knows if any of this would have happened if undercover FBI agents hadn't infiltrated these groups and apparently goaded these people on?

The fact that this event looms so large in so many imaginations is a reflection of how media distracts us from real issues. I am watching in real time as Biden's 16 percent inflation rate is destroying the wealth of my older relatives. This is not as sexy as January 6th, but it is an actual systemic problem, rather than a distraction. Never forget that BLM sucked all the oxygen out of Occupy Wall Street - and that is exactly what our corporate overlords wanted.

Instead of worrying about "systems of oppression," realize the oppression is built on individual instances of injustice. Go out, find some of those instances (evil is hiding in plain sight, I promise), and use the FOIA toolkit I have provided above to go out and slay some dragons. In my career, I brought down two prosecuting attorneys - one who let a dangerous rapist go despite having a substantial case against him, and the other who indicted a man he knew was innocent. Their scalps are a source of immense pride. You too will find that rooting out corruption is endlessly more satisfying and effective than marching down the street with a placard addressed to no one in particular.

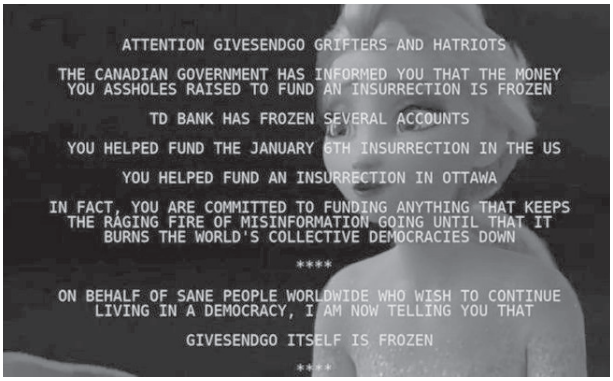
Data Analysis as the Next Step

by Tim R

In *2600,* you see a lot of pieces about reverse engineering, systems knowledge, phone phreaking, and other interesting things a curious person can learn about. In this piece, however, I'm going to advocate for a broadening of horizons, and suggest that data science and data manipulation get added to this list of topics. Take a moment to think through all of the data leaks that have forced important changes in culture and brought about world changing events: the "Collateral Murder" video, the diplomatic cable leak, details on PRISM, the Panama Papers, the Paradise Papers, and the list goes on and on. While it's great that these pieces of information make it into the hands of journalists and academics who take the time to research and find the proverbial needle in the haystack, have you ever attempted the same? Perhaps you've taken the time to actually download these troves of data, but have you taken the time to sift through them yourself to see what speaks to your community or what poses danger to what you find important? I think the time is right to suggest that examination of data at scale is the next step you should be taking in your pursuit of the hacker ethos.

An anecdote might help motivate the discussion. In January of 2022, a convoy of disgruntled citizens established an occupation of downtown Ottawa as a way to protest what they believed to be unfair restrictions on freedoms through the implementation of vaccine mandates and enhanced procedures at border crossings. This occupation of Ottawa was a real mess, both figuratively and actually. Daily life came to a standstill and the government, both federal and provincial, as well as police, seemed reluctant to do anything about the situation. Taking a step back for a moment, clearly the lead-up to the convoy's appearance in the capital city of Canada required a buildup of people, support, and enthusiasm. It can be said without any surprises that creating such a moment as this requires commitment of all sorts and undoubtedly money to make it happen.

As is common today, the organizers of this movement took to crowdfunding to get the word out and to solicit donations. As the motivations of this group were a bit dubious, or at least not apparently clear where motivations fell, the initial crowdfunding campaign using GoFundMe was frozen. Looking to find a viable alternative, the organizers of the group moved to a lesser known, and probably poor choice, of GiveSendGo. If you've been paying attention to the news, GiveSendGo has a known history of poor security and a lax approach to site updates. Quite suddenly and with great surprise, suddenly the site redirected to an alternate domain, `GiveSendGone.➥wtf`, and, instead of a page outlining ways to give and totals to date, a page was presented stating that "GiveSendGo itself is frozen," and also presented on this page was a link to a 40 megabyte spreadsheet of leaked donor information: name, email address, donation amounts, IP addresses, and anything else you could think of that would identify and provide insights about who contributed.



Here is where curiosity got the better of me. This development happened fast and, by the next morning when I finally realized something was up, I attempted to find the dataset. However, the hacked website was gone as was the spreadsheet. Curious and interested to see what was in that spreadsheet, I attempted to retrieve it by a generic web search and only found a series of different results analyzing portions of the data, all of which were very insightful and clever[1]. In the days that followed, a veritable flood of analysis pieces were published. While all these works were great demonstrations of data journalism, I still felt compelled to continue digging to get exactly what it was that I wanted. The next step I followed was to find the wiki page for the leak on Distributed Denial of Secrets[2]. Once there, I was greeted with a message saying that those interested in the information would need to contact DDoS directly to request access. The presumed purpose of this step was to ensure that responsible use of the information was adhered to. I respect the rationale and motivation for such a move, but I was still curious. I wanted to see if anyone at the same organization as me contributed to the group by foolishly using their work email address. I

also wanted to see if the funding was in fact coming from foreign bodies.

Enter the next step in the process, something that should be in the toolbox of anyone who spends time online: the Internet Archive Wayback Machine[3] This invaluable mechanism of Internet history is able to take snapshots of web pages over time and present these snapshots fully rendered in a sensible interface. The Wayback Machine is extremely useful for so many different venues of research and, delightfully, it throws a little bit of a wrench in the usual operation of the Internet, which usually functions as an actual memory hole. Within minutes, I was looking at a capture of the .wtf domain mentioned previously and was also in the possession of the spreadsheet I was so compelled to find.

Armed with the data, the next step, of course, comes down to how to analyze it. Here, yet another tool came into play. Simply put, the Jupyter Notebook, made available via Anaconda[4] or through various other means, such as Google Colab. If you've spent time using Python for traditional programming projects or for scripting, this represents yet another paradigm that you can use your skills for. In short, it is a web page that allows you to embed chunks of Python code and render their output by executing the code in a specifically deployed virtual environment. A search for "Python Pandas" will provide the broad strokes of how to interact with data using this suite of tools. Another site worth consulting is Kaggle[5]. It provides interactive tutorials on data manipulation using the Notebook paradigm. As an alternative, another platform worth considering is R, or more specially a cloud hosted platform called RStudio. While just as powerful, it isn't my default as I spend so much time with Python that I don't want to lose my fluency with that language.

Now, armed with the data and the proper tool to explore it with, the fun could begin. Some simple first things to explore: comparing donation amounts based on postal codes in my community (think the Canadian equivalent of a ZIP code) , analyzing the full-text of donor comments to see just how seditious they might be, and finding out what IP addresses associated with government agencies might be on the donor list.

Bringing it back to the original thread, I hope this narrative compels us all to think of the full story of how a leak should play out. Not just the discovery and distribution, but also the analysis and evaluation. The hacker mindset is about discovery, curiosity, and ingenious thinking. Often we see this come to life by circumventing roadblocks imposed by DRM, or by helping disseminate information acquired by whistle-blowers at great risk to larger audiences and to the mainstream popular media. How often have you spent the time systematically working through a leak, or providing someone the tools and know-how to do something similar? I'm hopeful that the answer is something non-zero.

If this isn't compelling enough an example, I encourage you to dig into this idea of operationalizing leaks by looking at the technical tools that the International Consortium of Investigative Journalists[6] have developed that are used to comb through terabytes of documents in order to find meaningful information that takes down despots and fights fascism. These are marvelous tools built on top of large scale data analysis platforms, all open source, that allow you to use your command line knowledge and Python skills to sift through vast amounts of data. Better yet, what about helping a local journalist or community group utilize these tools to make meaningful discoveries? There is a steep learning curve for people not acclimatized to working with computer systems, let alone large caches of files, to even make sense of how these tools can be used to serve the greater good, let alone to have the wherewithal to bootstrap these systems and to seed them with data. Imagine handing over a refurbished machine, now air-gapped, running an instance of Ubuntu on it preloaded with gigabytes of data and an intuitive web interface as the way to interact with it to a person who is just waiting to be given the tools that will allow them to crack open a very important investigation.

Platforms like SecureDrop and end-to-end encrypted communication channels do wonders for allowing those who are vulnerable to get in touch with trusted organizations so that they can provide information on nefarious dealings, but what about the last mile? What about enabling and performing the analysis in the first place? This is a step that I hope is part of the hacker ethos that will continue to be important as inevitably more and more leaks surface.

Links

[1] www.cbc.ca/news/politics/convoy-➥protest-donations-data-1.6351292

[2] ddosecrets.com/wiki/GiveSendGo

[3] archive.org/web/

[4] www.anaconda.com/

[5] kaggle.com

[6] github.com/ICIJ

Web 3.0 is Bullshit

by aestetix

Every so often, a new buzzword permeates through the tech world, inspiring endless blog articles, conference talks, and empty corporate announcements. The most recent of these is "Web 3.0," which is being hailed as some kind of "decentralized Facebook using the blockchain." From both a technical and a conceptual view, Web 3.0 is bullshit, and in this article we will attempt to explain why.

Let's quickly cover the framing that tech pundits are trying to use to delineate between Web 1.0 and Web 2.0, and then look at the actual turning point. In many discussions (and on Wikipedia), we can see people making the argument that Web 1.0 started in 1991 and lasted until 2004. This is mostly reasonable.

They then proceed to say that Web 1.0 was "read-only," static pages with no user interaction, and wasn't capable of showing ads. This is completely wrong, and only establishes that the pundits making this arguments never *used* Web 1.0. In the mid 1990s, we had sites like GeoCities, which allowed people to log in and create their own web pages, and sites like Slashdot had - and still have - massive post interaction; in fact, Slashdot gave us the term "Anonymous Coward," used to describe someone posting comments anonymously. As far as advertisements, technologies like pop-up blockers and ad-blockers were a direct response to the constant barrage of advertisements from websites. And all of this was happening long before 2004.

A better marker for Web 2.0 is at the protocol level. With Web 1.0, while we could do all of the things that tech pundits now claim we couldn't, viewing updates *did* involve refreshing the page. That is, the browser would make an HTTP request, get an HTTP response, and that would be the end of it. Web programmers came up with ways of making websites seem interactive, using tricks with hidden divs, as well as JavaScript and CSS elements; however, the real innovation came when we realized we could use a JavaScript object called XMLHttpRequest to make a new HTTP request from the browser, grab the response with JavaScript, and parse it back into the page *without refreshing the page*. This fundamentally transformed the web. It enabled things like real-time updates without the need to click an "update" button, and opened the door to a lot of drag-and-drop web technologies we now take for granted.

We also realized that because JavaScript - like many programming languages - is Turing Complete, we could use it to recreate almost all of the software we used on the computer, such as email clients and word processors, in the web browser. We now take tools like Gmail and Google Docs for granted, but in 2004 such an idea was revolutionary. In many respects, these uses of JavaScript brought us into the modern Web 2.0 era.

Defining Web 3.0 is a lot trickier. As soon as the term "Web 2.0" was coined, tech pundits were trying to slap the label "Web 3.0" on every new craze. Some said that Web 3.0 was Big Data systems like MapReduce. Others suggested it was the advent of mobile devices (iPhone vs. Android). Still others ensured us it was the walled gardens of Big Tech itself. It's a bit ironic to watch the same pundits who once said that Web 3.0 was Big Tech now announce that Web 3.0 is the technology that will help free us from Big Tech.

But let's take the pundits at face value and assume that Web 3.0 is what they claim: using blockchain technology to allow people to set up applications in decentralized systems that are free from Big Tech. The problem with this claim is that both Web 1.0 and Web 2.0 were already decentralized, without needing a blockchain. In addition, questions that many tech pundits are now posing regarding how to curb censorship while preventing crime with Web 3.0 have

already been addressed, as the same issues have arisen time and time again over the last 30 years.

Web 3.0 purports to enable data ownership, but we can already do that. All we need to do is set up our own websites on our own servers, which is now easier than ever. If the issue is interoperability, we have all kinds of technology to do that. If we want to find a list of open systems and protocols, we can simply look at technologies that Big Tech companies initially embraced and then abandoned to force everyone into their walled gardens. It might be worth asking why Google killed off Google Reader, which used RSS; or Google Talk, which supported XMPP.

Regarding the questions of censorship and free speech, this is not a new debate. In the early 1990s, we had the debate on whether there should be an "Internet Driver's License" when the Internet was known as the "Information Superhighway." We then saw the advent of laws like the Digital Millennium Copyright Act and the Communications Decency Act, both passed in 1996, attempting to address issues of digital ownership and speech. We also had websites like WhiteHouse.com (a porn site), and Nissan.com, a small family owned computer company which has been fending off lawsuits from the massive car company since 1994. And, for that matter, consider the decades of debates within ICANN about whether to create a .XXX top level domain.

In conclusion, Web 3.0 is bullshit that simply revives old ideas, and the only new insights revealed by the current "discussion" are the level of absolute ignorance of tech pundits and the depth of greed of venture capitalists who are probably trying to recoup losses from bad investments into crappy cryptocurrency startups. Slapping a blockchain onto a website is not going to magically solve everything. Then again, what more can we expect from the ruling class that is attempting to usher in the "metaverse?"

Book Review

***Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, Andy Greenberg, 2019, ISBN 978-0-385-54440-5**

Reviewed by Br@d

I received a free copy of this book back in late 2020. The author and senior writer for *Wired* was the keynote speaker at a virtual user conference for a security vendor that I was working with at the time. I was one of many attendees who won a free copy of this book by taking part in the conference's gamification. This involved attending various sessions as well as visiting the virtual exhibitor's hall to interact with sponsors. Not only did I win a free copy of the book but with some basic enumeration, I was able to upgrade my prize winnings to a higher level (the details which will be left for another time).

Around late 2021 I finally got around to reading this book. It had been on my to-do list for a while; I just never had the urge to dive in. Once I finally did get to it, I was pleasantly surprised at Andy's flow of information. It was very easy to follow (regardless of your technical background) as it took us through more than a decade of the world's most well-known cyber attacks. More important to current times, this book covers a lot of background information that better put in light the current political and technological struggle that is happening between Russia and Ukraine (and the world).

This book is filled with various references that go into extensive detail, yet is still an easy read for the tech and non-tech savvy alike. Not only was this an informative and enjoyable read, but it was also scary at times, bringing the hard realities of how acts in the digital realm can have a significant (and even fatal) impact on our physical world.

WHY YOU NEED TO SELF-HOST

by Byeman

On December 14, 2021, Google published an article titled "New Notifications When Drive Content Violates Abuse Program Policies"[1]. This rolled out to all Google Workspace customers, as well as G Suite Basic, and Business customers. What does this mean? Whether you're a small business, an activist community, a Fortune 500 company, or an individual, Google is monitoring your data, data that you're paying Google to store, and deciding for you what you can and cannot save. There is no admin control for this feature.

Google doesn't know, or care, about the context of the files stored. Let's assume you run a non-profit fighting racism in your community. You collect the hate mail you receive, the threats, pictures of the people protesting you and your work. All Google sees is a bunch of hate speech stored in your account and, presto, your files are locked down.

If you're a Fortune 500 company, you clearly have resources to fight this. And hopefully your legal team and IT department can advise you about what you should and should not store in the Google cloud. Once again, the little guy is the victim. What can be done?

Self-hosting!

I could use every single page in this magazine to tell you a fraction of what you need to know. I haven't approached the folks at *2600* HQ about this, but, wait, wait, no they're shaking their heads, can't do it. And honestly, I'm not qualified to do it. What I am qualified to do is encourage you to dust off your hacker caps and get to work.

I hang out on several forums related to self-hosting and the various platforms that can be hosted. I see people making the same, even worse, mistakes than what I made. I'm new to this. In the early months of the pandemic I needed a distraction. I screwed up. Oh lordy, I screwed up. But you know what? It was okay that I did. I was learning. And secondly, I chose to learn using a Raspberry Pi and a virtual private server (VPS). Why was this important?

Rule One: You're a student, not a master. Choose an inexpensive gateway to the drug that is self-hosting. VPS hosting can be had for as little as $5 a month and a full blown Raspberry Pi setup can be had for well under $100. If I had decided self-hosting wasn't for me, I wasn't out much money. But there's a second much overlooked benefit. It's trivially easy to do a hard reset. If you've completely hosed your server, just destroy it and create a new one. This process takes about 15 minutes on a VPS and about the same on a RPi. Which brings me to...

Rule Two: Don't make any of this your daily driver. You're not ready. Continue to use Google Drive, OneNote, Dropbox, and Gmail. I really feel bad for people when I see their pleas posted at 2 am saying they had moved all of their photos into their Raspberry Pi and now the Pi won't boot and when they pop the SD card into their laptop, all it can offer is to format the memory card. Before you migrate, be sure you're using robust hardware and have a backup strategy implemented before you move your data.

Rule Three: The community will help you if you help yourself first. It was rare that I had to post a question to any forum because I was not the first person to have the issue. Use the search function first. If you find a thread and still have questions, ask on the existing thread. If you can't find it, start a new one, but in both cases you need to help us help you. Asking for help on a poorly described problem will get you ignored and following up with "isn't anyone going to help me" will only make you a pariah. At a minimum, we need to know your operating system, your hardware, what you were trying to do, what were you doing when the problem started. Before you even think about asking for help, search the error message. Review your logs and search on the error codes and descriptions you see. You'll be amazed what you'll find. If you show the community you did your homework and provide them with enough information, they'll be happy to help you.

Rule Four: Give back. If you post a problem and find a solution, tell us about it! Please. The next person with that problem will want that information. As you learn, browse the forums and jump in to help whenever you can. Believe me, the community will get to know you, will trust you, and will be more willing to help you as you continue to grow and get more advanced in your self-hosting journey.

How to get started? Pull up your favorite search engine and ask "how to get started with self-hosting" or something along those lines. Some of the better resources include:

```
cyberhost.uk/getting-started/
www.reddit.com/r/selfhosted/
docs.standardnotes.com/self-
➥hosting/getting-started/
```

I hope this inspires someone. My next article will discuss cool tools you didn't know you needed that can be self-hosted, solving problems you didn't realize you even had.

Happy hacking!

```
[1] workspaceupdates.googleblog.
➥com/2021/12/abuse-notification-
➥emails-google-drive.html
```

Should I or Shouldn't I? Ransomware Negotiation

by lg0p89

Ransomware's successful use as a malicious tool is growing. Way back when this began as only encrypting files and systems, the affected party or business would receive the usual message to pay for the decrypt key in Bitcoin. If no payment was made in a reasonable amount of time as determined by the attackers, you generally were out of luck. There was no appealing to any level of moral fiber, but only "pay me." At times, people would get lucky and find the decrypt key in code or a file left somewhere on the system. This was not the norm, but occasionally the person/company would be fortunate.

This evolved with additional forms of encryption and, as a tangent, instead of only having the option of encrypting, the attackers added exfiltering the data and threatening to publish it unless the ransom were to be paid. Now the targets had two issues to possibly contend with.

As ransomware has become much more profitable with an ROI (return on investment), the attackers operationalized this into an industry. This is so prevalent that it even has its own acronym: RaaS (Ransomware as a Service). Gone are the days of the lone attackers targeting businesses from his own system. The bad actors have businesses set up and working with ransomware attacks as the corporate goal. As the ease of use continues, this is only going to get worse until a robust, reliable set of tools becomes available to combat this directly.

If there is any doubt on how expensive ransomware can be, just do a quick Internet search.

- The CNA insurance company dealt with a ransomware attack in March 2021 that cost $40 million.
- Acer had a $50 million ransomware demand that same month.
- In June 2020, the University of California at San Francisco paid $1.14 million.
- In early 2020, Travelex paid $2.3 million.
- In May 2021, the North American division of Brenntag paid $4.4 million.
- Colonial Pipeline in 2021 paid $4.4 million.
- CWT Global, a U.S.-based travel services company, paid $4.5 million in July 2020.

These are only the large and published payments. Adding to the attackers' revenue are all the other smaller successful compromises and payments. This line of work can be lucrative, which is what continues to drive this forward.

The question is, if you happen to be infected, what is the next step? Do you pay or not pay? If you don't pay, get ready to spend a lot of money on new equipment. If you pay, you may be a victim of BOHICA (Bend Over, Here It Comes Again), as they know you will pay.

The choice boils down to economics. When there are viable backups which are recent and go through periodic checks, you may not need to pay. If, on the other hand, the backups are done quarterly and the system has never been checked other than to look at the record when the backup was last done, the company and their insurance carrier may want to get their checkbook out. If you choose to pay, you may ask yourself if you can negotiate with them. Maybe you could pay a little less and still get your files back or they'll promise not to disclose the files.

The attackers have lofty goals for the revenue generation from ransomware. The amounts they are seeking are probably not in line with what the business and/or their insurance company, if they have the coverage, are able or willing to pay. In the attackers' minds, you have a massive treasure chest of gold, when you have enough for a month or two of cash flow. This perception has been furthered by the large payment mode by companies who really didn't have a choice. This is where the ransomware negotiator comes into play While the attackers still need to maintain a planned revenue level, there is no blank check for them. With ransomware being so prevalent in the last two years, the negotiator role is relatively new. This role may be used more as the attackers who already have compromised your system ramp up the pressure to pay them with calls of threats and intimidation.

In this case, when you have no other choice but to talk to them, the negotiator is there to mitigate the amount and talk to them, focusing on the relevant points.

Social Engineering Attacks Out of Control

by Stephen Comeau

Before the pandemic, social engineering attacks were prevalent. I used to get calls on them once a week on a regular basis. Who would have thought we would wish we could go back to that once-a-week scenario as being relatively favorable? Social engineering attacks have since taken on a life of their own. Now, I deal with 20 to 30 calls *per day* on this issue at minimum.

Social engineering attacks have not only grown more frequent, they have become more sophisticated. Not only are regular users having difficulty separating the false from the true, but career IT people are having the same problem. And this is particularly troubling, for it directly affects our overall ability to adequately respond.

To focus on the specifics, one out of ten adults falls victim to social engineering attacks every day. Currently, the most prevalent of these attacks is the phishing scam. Phishing scams target email and phone communications alike. There are also plenty of new attack vectors - less common but likewise troublesome. Some involve text messaging. These have come naturally to the fore with the development of emerging technologies within the larger IT realm.

Looking back in time, we see that phishing attacks are not new, and have posed a problem of longstanding duration. However, since the pandemic, these types of attacks have increased exponentially in a way that had not been properly predicted, causing them to occupy center stage in modern efforts to keep communications systems secure. Phone scams (or phone attacks) have increased by more than 150 percent since the start of the pandemic. In fact, phone attacks have become so problematic that the Federal Trade Commission has taken particular and serious notice of them, putting the weight of the federal government behind a larger national effort to mitigate them.

Over the summer (July 2021), the FTC began enacting statutes requiring providers to implement Caller ID authentication. This new regulatory focus represents one of the most extensive campaigns undertaken by the federal government to combat the phone scam epidemic. This overall effort has been particularly aimed at reducing the growing number of robotic phone attacks.

While this federal-level effort is reassuring, it is at best a temporary Band-Aid solution. It will undoubtedly help to stem the overwhelming tide of phone attacks for a short time. But, as we know, the "game of cat and mouse goes on," with bad actors becoming ever more sophisticated in their own efforts. As expected, new software has already been developed to evade the FTC countermeasures. Some of it involves a novel implementation of traditional cloning technologies, making use of cloning software that is readily available and simple to use. All that remains to do, upon utilizing such software, is to dial the first unwitting victim's number. Beyond that point, it takes only two seconds after the individual accepts the incoming call for his or her phone number and device identity to be acquired. This device identity, or IMEI (International Mobile Equipment Identity), is a 15-digit identifier that links the phone with a specific phone number.. On the victim's end it looks like the scammer's call is coming from you. All this occurs with your active participation, yet without your knowledge of what has actually occurred - and the FTC countermeasures are evaded. Scarry, right?

As previously noted, cloning software like Dr.Fone and CLONEit is nothing new, I remember messing around with similar software for learning purposes a decade or so ago. I further remember some of the troubling discoveries I made. It was scary then, it is scarier now. In the old days, you needed to be physically near the victim's phone to compromise it. Nowadays, such attacks are far easier to implement and with more sophisticated software that is more readily available. You don't have to be an uber-hacker to run a cloning phone attack on the average phone user anymore. Anyone with enough knowledge to run a kiddie script level attack could easily deploy one nowadays. This accessibility highlights the need for preventative measures to be adequately employed. Some such basic measures are as follows:

- Always keep your phone software current with the latest updates
- Always keep you phone properly locked down

A minimal level of security on any phone

should always include:

- Having a passcode lock on your phone
- Encrypting your phone to protect your information, especially your IMEI number (Encrypting your phone in this way makes efforts to steal a copy of this critical number vastly more difficult.)
- Never leave your phone unattended, especially in a public place
- Do not leave Bluetooth on when you're not using it

Protect yourself by educating yourself as to the sophistication and diversity of modern cyberattacks. Attackers will often use several different techniques to get what they want from you, some of which we have covered, and others of which we will cover now.

The first of these techniques is the social engineering attack, by which you pose as someone else, likely someone important, working for ether a regulatory agency, key vendor, or authoritative management team within one's own company. So, if you are ever unsure of the legitimacy of a call, hang up. Then call back the specific agency or company on their known public line to verify their identity.

Another technique phone attackers or scammers will often use is to create a sense of urgency. They will create a scenario where you will need to do something or give them something right away to keep something else bad from happening. Note that nothing is ever urgent enough for you to avoid properly verifying their claims. Never provide any personal information or financial data to anyone who calls you whose authorization to receive such information remains in doubt. To emphasize, you can always hang up and call back the agency or company's legitimate known number for verification.

Also know that official government agencies like the IRS will never call you randomly. Doing so is a clear indication of a scam. Always verify any call you get from a party you would otherwise hope to trust, especially if what you are hearing sounds too good to be true. I can't emphasize this point enough!

Another sure sign of a scam attack is a demand for immediate payment. No company or agency will expect you to respond on the spur of the moment without adequate thought. Additionally, if they demand a specific form of payment, like a gift card or Western Union payment, this is a sure sign of a scam. Hang up.

Also, never let anyone you don't know have access to your personal devices. You have no idea how many times I have heard the same story. "Oh Mr. (Blank) called me from (Blank) Company and asked for access to my computer to fix (blank) issue I was having." No! Wrong!! Do *not* give anyone unauthorized access to your computer or personal device without first verifying the legitimacy of that access. A legitimate company, without a partnership or vendor relationship, will never ask you for access to your device. Remember, as before, to verify this request by phoning the company on their main line as the best way to handle any access issue about which you have significant concerns.

Another method of dealing with scammers is to record the number you were called from, and then to block it on your own phone.

Finally, you should always report any phone scams or phone attacks to the FTC (Federal Trade Commission). It is very important that you remember to fill out the pertinent - and simple - form at the FTC website. By reporting the scam attempt, you are helping the FTC keep track of changes in and frequency of different attacks. You are, in the process, keeping others from being victimized. The FTC has the power to flag compromised numbers through phone companies and to place those numbers under review. By this means they can hope to apprehend those who have compromised phone identities. You can report any such issue to the FTC here: `reportfraud.ftc.gov/#/`.

I do hope this article serves as a needed wake-up call (no pun intended), adequately informing the public on how social engineering and spoofing attacks occur, and in particular from a phone attack perspective. It was also my intent to describe what should be done to prevent this form of attack from occurring on such a large scale in the future. My hope is that with some effort and better public security education, the attacks I have enumerated in this article will finally start to, once again, become few and far between. We may even return to that more-desired point where we are getting just one social engineering attack inquiry per day. It's a nice dream, right? Either way, it is now clear just how big of a problem social engineering attacks have become, and that something effective needs to be done about them now. Stay tuned for further updates.

The Hacker Perspective

by Rick Swords

Growing up, my father was the director of electronics for a large, cash heavy medical center campus. This meant that he and his crew were responsible for sourcing and maintaining every piece of technology in the place. Sometimes in the summers I would go to the electronics lab with him on the lower level of the hospital and the techs and engineers would let me solder, and tinker, and tolerate my begging for food.

Sometime thereafter, my father would ask me to help him get some things out of his car that would change my life... forever. After some heavy lifting, sitting in our dining room which became an office after he and my mother divorced, there was no more china cabinet, fancy seats and table settings - just an IBM PC XT with dual 5.25 inch floppy drives, 640k RAM a 10MB hard drive, keyboard, IBM amber monitor, dot matrix printer, and a Hayes 300 baud modem. For those of you who don't go back this far, 300 baud is about .3 kb/sec which equals... infinitely faster than nothing. Huge technical books about the PC, DOS, Basic programming, Lotus 1-2-3 (you may know this as some form of spreadsheet), and other floppy disk applications.

My father was keen to get his entire budget and spending practices into Lotus and hand them to higher ups as a signal to back off, give him what he wanted, and generally make his job easier. So the first thing he did was to teach me to load the application; open the proper file; enter the data and formulas in their correct cells, columns, and rows; and save the file. This may not sound like much, but this entailed teaching me the DOS command line for creating, saving, and manipulating files. I caught on pretty quickly - not because I was some sort of financial wiz, but finishing the tasks he assigned meant I had the whole setup to myself until I couldn't keep my eyes open anymore. Then do it all over again.

It was on. I was dialing up BBSes to chat, play games, try to break things, and other fun and mischief. I connected with other kids and adults who taught me tips and tricks of all sorts. My first real game was *Zork*. I quickly learned that I sucked at games and was more into just exploring and learning new things.

Thirty-five years later, my friends still joke that they only knew I was home if they saw the amber screen glowing through the window of our dining room. A yell meant "Yo, u good?" A whistle meant "Pause that shit and get outside - we got some gangbangin' to do!" That was me. Part time geek, part time street kid. This dichotomy of interests would continue to shape my life for a long time. The older kids in the neighborhood knew I was generally smart, and encouraged me to nurture my intellect, and not to get caught up in the street life. I loved my fellow Vice Lords and they knew it. I eventually was given the rank and role of "Minister of Lit." My duties included maintaining the "literature" or rules, regulations, and *creed* of our organization, and maintaining copies of this for new and old recruits. I also kept minutes of meetings and assigned security details. Sounds fancy for some 12- to 21-year-old street kids, but back in those days we had order and maintained it. Period.

Maybe you can see where this is going. Soon all the Lords in my hood had *printed* copies of our Lit, prayers (yes, we prayed), meeting minutes, roll calls, etc. This would eventually get us very high praise when we would attend the larger meetings of groups of neighborhoods to "check in" and generally assemble. We became known as a group that had our shit together, and I became known as the "go to" for teaching other MOL officers to keep tight records. Please note, although there was plenty of unlawful action going on, record keeping was strictly from an organizational standpoint. Internal and clerical - same as any other private social club or similar group.

I was young, smart, tough, chubby, wore glasses, and I was honest. These traits were unique in the body politic, and I was cherished and protected by the older members. I felt the love and returned it. I needed it to survive outdoors.

One day in eighth grade science class, the principal got on the PA system and asked if I was present. My teacher answered in the affirmative, and she responded by saying that I need to come to her office immediately because "we think his house is on fire." It was. My school was one block away and I could see the smoke as I left the schoolhouse. I made it there to a scene of fire trucks, police cars, smoke, water... *lots* of water, and the bottom half of my childhood home dripping and smoldering.

The other thing I saw was my father. He was leaning on his car, smoking a cigarette and talking to the Red Cross and firefighters. My father grew up in the Bronzeville area of Chicago, was a Navy veteran, and was a cool customer. He was like me, but better. He was smart, tough, and well respected. I'm saying this to say, we didn't exchange too many words. "What happened, Dad?" "They don't know yet" was enough for both of us. We were more interested in the next plan of action.

First thing was two brown paper sacks from the Red Cross that contained underwear, t-shirts, and socks for the both of us. My father finished some business with the firefighters - they left. Then the insurance company chatted with us and gave me a thick stack of lined paper, and gave my father a check. You get three checks when your life burns down and you're insured. That was "check #1" right there in front of the dripping house.

Some of you reading this may have seen homes burn down on TV or something similar. When it happens to you, the finality of it is staggering. Your forks and spoons, couches, secrets, clothes, sundries, photo albums, your *history*... is gone. It hits you in waves. As you think of something to go get, or use, or equip yourself with, it's gone. But that night, my father and I cashed the somewhat large check, hit the mall, locked down an arms hotel for a month, ordered food, and hunkered down with the stacks of lined paper to write down *every* single thing we had in the house to claim for its monetary value. My father was an honest dude, so we stuck to reality - no hacking the insurance system. This was the necessary duty to get "check #2."

The next day I went to school in my ill-fitted jeans and NGO t-shirts. I answered all the questions about the fire and, it being close to the end of the school year and time for high school, I graduated and made it through the summer. My father meantime got check #3 and ordered the contractors to finish our house by the end of summer. They did, and we moved into a brand new house on the same land and filled it with brand new stuff and, most importantly, we went absolutely crazy with new computer systems. By this time (I'm terrible with dates), I think the IBM PC AT 3.5 inch disks was the hype. The hard drive was 100MBs, the modem was 9600 baud, and the monitor was RGB... for god sakes *R...G...B!!!*

I was back at it. Geeking like crazy at home, gangstering like crazy outside, and failing miserably in high school. My mother wasn't having it. She made an executive decision that I should leave Chicago and live with my ex-Marine, self-made millionaire uncle in the suburbs of Maryland to finish high school.

It was great for me. While I was there, my father got remarried, and I spent my time reading from my uncle's vast library of books and teaching myself more computer skills. The town I lived in was full of miscreant ex-pats from Brooklyn, New York, D.C., Virginia, New Jersey, and other places. We were all good/bad kids that needed a change of pace. My background was a good fit with the east coast teenagers. They believed in mental and physical fitness, knowledge of self and being generally a civilized being... with some super rough edges. After a couple scuffles, I was accepted as the Chicago kid. Country as hell to them, but cool.

I got great grades, lost lots of weight, started a videography business, and grew mentally. But there was one problem. Because of my utter failure in gaining credits back in Chicago, the school wanted me to graduate a year late. Class of 1991? Not an option. I was in the class of 1990. Period. My uncle understood, and I dropped out and got my GED and attended University back in Chicago. The *same* university my father worked for on the medical center side. So while I hacked my high school graduation with a General Education Diploma, my father's clout hacked my college acceptance. I was in.

It was 1991 and the Internet was becoming ubiquitous to those in the geek set, and to normies email and instant messaging were the killer apps. I did a couple years and dropped out from party exhaustion and, to be quite honest, I missed the streets. This section I will redact because I was older, nowhere near as smart as I thought I was, and the middle 90s were crazy. Let's keep it at that. I eventually went back to school and discovered they had a computer science degree offering. In 1999, I had an interview with a Fortune 100 technology company and was told by the interviewer that I didn't need the degree, I should finish the classes I was taking, and he would give me a job in his research lab. I knew what this meant: fun, freedom, and an unlimited budget. I was in.

I was having a ball. I worked for an absolute genius, and he gave me all the room I needed to explore *after* I handled the tasks he assigned me. I was used to this dynamic and handled it well. In the early 2000s, I worked on wireless high speed Internet, bluetooth, touchscreen tech, and smart appliances. My boss saw this future we live in now, and let us do what we wanted and needed to create it. My boss has since passed away, but some of my fellow engineers have since formed a great company some of you may know: Ubiquiti Networks, Inc.

During my tenure, I traveled quite a bit. During my travels, I met a young lady. She

was a recent hire at Microsoft. We became fast friends and she began to tell me that her previous job was at GE Capital. She was competitive and, while I bragged about hacking and tech work, she would tell me that I didn't know how to hack the most important thing... *money*. This got my attention.

Before long, she was teaching me how companies were built on paper: from the employer identification number; to aged shelf (not to be confused with shell) companies (companies that were formed in years past and put on the shelf to let them "age"); to financial documents and what underwriters look for; down to a corporate website and virtual phone, fax, and office services to give a company a real world presence in an emerging virtual landscape. Before long, we put together our first multi-million dollar company and began to socially engineer every creditor we knew. We were quickly getting credit lines, travel accounts and cards, auto loans, and whatever we wanted based on these *shell* companies.

Within a few years, we both quit our jobs and began to hack the credit system full time. We both had luxury cars and condos, six figure corporate credit cards, and a money supply from my street connections that required everything from restaurant furniture at 50 percent on the dollar to farm equipment. We would take a little and pay our bills, and travel and have fun with the rest. I thought I was the smartest guy in the world while simultaneously knowing I wasn't.

In 2004, at the height of my powers, my mother, father, and one of my best friends all died within 60 days of each other. Liver failure, lung cancer, and murder by police respectively. I was silently devastated. I did what I could to help bury them and help their other survivors, and put my nose to the grindstone to make as much as I could and get out of the game.

By 2008, we had built a network of shell companies that did business with one another like a pyramid. At the top was me. One day, when I was picking up a truckload of electronics from a location I used for such things, I was quickly surrounded by federal agents. They identified themselves as members of the U.S. Postal Service, Secret Service, and Chicago Vice. I was charged with theft and questioned. I kept quiet and was let go, but the jig was up.

My federal case was hard to indict because the place they interrogated me was being exposed publicly for being an inmate torture site (the feds wanted nothing of this), and I had an all female staff (no male voice, or handwriting, or witness recall) that was pretty stoic. Soon though, the feds kicked in my home door, guns drawn, to find loot and weapons I had for home protection and gave me a state case for them. They seized, froze, and demanded all I had. The federal investigation ripped through my money until I was in tatters, and the state case lingered like a gray cloud over my remaining pennies and self-made hell.

My state case went on for three years. During this time, I started a business consulting firm helping people to put together *legal* companies with the skills I acquired in the fast life. During this time in 2010, I kept my eyes and ears to the street. And the word on the geek streets at this time was Bitcoin (the code). I was sucked in instantly.

I thought to myself, now *this* is how you hack money.

Over time, I began to mine and acquire and see the elegance in the code for what it was. I was also broke and in a unique position to see my future with a money that was unconfiscatable *if* I was careful.

In 2011, I was sentenced to the minimum three years for unlawful possession of a weapon and had to do half of that. During my time in prison, I taught GED classes, wrote a patent for music streaming, and read *The Best of 2600* (*wink*). Upon my release in October 2012, I came home to a few bitcoin (the money) on an Apple Time Machine drive and submersed myself back into the code and community. On my date of release, the exchange rate for Bitcoin with USD was around $13. Despite a few slip-ups and clown maneuvers, I have pretty much been dollar cost averaging since then. I cannot believe how far it has come. I now teach Bitcoin security and monetary policy to friends, businesses, and non-profits.

As I write this, the world is in the midst of a global financial crisis and a viral pandemic. I'm seeing many people start to crack. Some of their belief systems and trust are being broken. Their governments are printing money from thin air, and can't protect them as they once believed. This makes me feel for them... and be grateful. Grateful I can teach myself new skills with primitive tools, survive being a child of divorce, having my home burn to the ground, bury both my parents and loved one back to back to back, the streets, time in prison, and starting again with nothing. The world is in chaos at the moment. But it won't break me. I don't see chaos. I see problems to be solved collectively. I see things from a Hacker's Perspective.

Rick Swords (@rick_swords) is a Bitcoin professional and educator. Rick is now spending his time investing in Bitcoin-only startups and running a Bitcoin ATM network with the help of his daughters and young son. "It is my wish to empower all the human families with the only cryptographic money with street credibility: Bitcoin."

Sleuthing Google Apps Part 1: Google Calendar

by Estragon

In a pair of articles, I will describe straightforward but non-obvious ways to see what other people have been doing in an organization you have online access to. In this first article, we will see how Google Calendar can be utilized to see what meetings are occurring, even when you cannot see any meeting details. Then, in a second article, we will look at how the change-tracking mechanisms within Google Workspace applications for spreadsheets and documents can reveal intention and coordination among those who wrote them.

These techniques may be of interest to *2600* readers in organizations that make use of the Google suite of online applications (Google Workspace and related names), or similar cloud-based document management and editing platforms such as Microsoft 365.

The Google suite of applications, like any modern cloud-based software, changes from time to time. I tested the methods described here while writing this article and found that some things had changed since I first observed the behavior - and things can be expected to change again in the future.

About Google Calendar

This article is about Google Calendar. This is the calendaring application in the Google suite, and it is typically accessed via a web browser or a native app on a phone or tablet. The techniques described here have only worked for me via a web browser, at the time of writing. Google Calendar (sometimes shortened to GCal) lets you keep track of your appointments and contacts. It also lets you send and receive calendar invitations to other people, get reminders of appointments, set your working hours, and so forth.

Google Calendar has great interoperability with other calendar apps, which facilitates scheduling of meeting times with attendees in multiple time zones. It also interoperates with other Google suite elements, such as Meet (for audio/video calls), Drive (to share documents), and others.

There are millions of people who use Gmail and can utilize Google Calendar with their regular Gmail login. My focus in this article is on the many thousands of organizations that have adopted the Google Workspace suite of applications. These organizations typically use some of their own Internet domain space to point to Google-operated systems so that their email addresses, documents, etc. are within a Google-hosted enclave, but with their own organizational name, branding, policy, etc.

First, let's get a general description of how Google Calendar is used within organizations. Then, I will share two personal stories, along with an illustration. This first article concludes with some advice on how to avoid information leakage via shared calendars.

Google Calendar Use Within an Organization

The basic scenario, which is typical of organizations that have adopted the Google suite, is that default settings hide your calendar from outsiders. For example, people who are not part of my organization will not be able to see my calendar or calendar events, and even if they are signed into Google with another organization, they won't be able to see my free and busy time.

Within my organization, by default colleagues will still not be able to see details (such as the title and description of an event in my calendar), but they will be able to see my free or busy time - that is, a view on what parts of my days are booked with calendar entries, and what parts are free. This is a very useful feature, since it helps find a meeting time that is open for all parties.

An "organization" in this context is usually associated with one or more Internet domains or departments that have chosen to adopt the Google Suite. For the scenarios I'm describing here, consider a fictitious organization like 2600meetings.net.

To adopt Google Workspace for the organization, the domain administrators of 2600meetings.net might set up Google as an email handler for the domain (by assigning MX records in the DNS and a few other setup steps). Organizational employees or designated members/affiliates would get a Google login to the 2600meetings.net application space in Google.com: mail, document sharing (via Google Drive), the

suite of productivity applications (documents, spreadsheets, presentations, etc.), and a plethora of available add-ons, including some from non-Google providers.

The result is that employees of 2600meetings.net, and anyone else assigned a login to the Google portal for the organization, will be able to utilize whatever Google services are set up for them. They can even utilize the Google login to authenticate to other services (this also works for people using the regular free Gmail.com service).

The administrators of the organization's Google domain can choose which extra applications are available to their organizational users, as well as some default settings and restrictions. For example, document sharing with outside parties might be prohibited. Or a company-wide email signature might be added to outgoing emails. Or a company might even use their own authentication system (via OATH2 or a similar protocol) rather than letting people login with a Google credential - thereby tying that Google identity more closely to the organizational identity. Options like these help an organization customize the Google Workspace experience to meet its needs.

For the Google Calendar app, what I have seen is that calendar sharing within organizations allows anyone to see free and busy time by default. Sharing of additional details, like the event description, location, and other attendees, must be done intentionally by the calendar owner. No calendar details at all are visible to outsiders.

This set of defaults makes great sense for setting up meetings within the organization. There is even more granularity available, such as to assign rights to fully manage someone else's calendar (for example, an office administrator might need to set up meetings for the unit's head, and assign meetings to others in the group).

Here's the thing: Visibility of free and busy time can disclose information about who is meeting together. When physical rooms are scheduled via the calendar (which is another feature), even more inferences may be made.

Example 1: Sleuthing to Find Out When Meetings Occurred

I'll tell two personal stories where unintended information disclosure via Google Calendar happened. In this first story, I had applied for a job in the same workplace my spouse is employed by. It's a large organization, with over 10,000 employees, staff, and others who all utilize the same Google-managed application suite.

My job application had been languishing. I had been interviewed but didn't know whether another candidate had been selected. We knew who was on the search committee, and the name of the hiring official, but none of them were in the same department as my spouse. The search committee members worked in different departments, including the human resources (HR) department.

Google Calendar sleuthing to the rescue! Might we see indications through free/busy time whether the search committee had met after my interview? Or whether there was a meeting that included the hiring official?

In this situation, one of the people who might have also been a candidate already worked for the organization. Could we find out whether they had been interviewed?

We found that just by my spouse's viewing of free and busy time, we could get insights into the communication among search committee members.

There are two ways of doing this in the Google Calendar application. For quick investigations, just set up a test meeting and invite the people you are interested in. When you view "More Options" (or similar) in the test meeting, select "Find a time" (or similar).

You then get a side-by-side view of available time for whoever you invite - as many as you invite.

You can even see free/busy time in the past. This is key: if you want to find out what people did in the past, take a look at past meetings. If you want to find out who they were meeting with, just invite all those people to the test event and GCal will happily show where calendars were aligned in the past.

Of course, you should not actually *send* an invitation to those people. You just want to see when they were all scheduled at the same time, in the past or in the future.

Another way of sleuthing calendars is to use the Google feature to "Add a calendar" to your calendar view. Instead of an individual meeting, this lets you see a group of calendars, all color coded, for whatever range of times you select. Within the web interface to the calendar app, you can navigate backwards and forwards in time just like if you were trying to make a new calendar event invitation, looking for alignment of the calendars you are interested in.

In my situation, we found that the top administrators, and all the HR people, had

their calendars set to be non-visible to others within the organization. Their calendars could not be viewed, and there was no indication of free or busy time.

However, other people on the search committee had their calendars available for viewing. We looked back in time to the day of my telephone interview, and could see them all lined up, in the same "busy" block of time, for my interview.

It was then easy to look for other times they were lined up and make an educated guess that those were the days/times for the other interviews. Scan forward a week or so, and we could see when the committee had likely met to discuss the candidates.

Did they interview the inside candidate? It looked like they didn't - the inside candidate only had occasional overlapping meetings with some search committee members.

What about meetings involving the administrative team, when a candidate would be presented to the hiring official? Well, we could not see the top administrator's calendar, nor anyone in HR. But there was someone who reports directly to the top administrator on the search committee, and their free/busy time was available. Also, we found that the room where the search committee met was in the calendaring system - so that people could book the room for their meetings.

We were able to infer the search committee had met, that the internal candidate was not interviewed, and that the search committee had not yet had a meeting to present their recommendation to the top administrator. All of this was simply by looking at the alignment of free/busy time for those people who had made it viewable across the organization.

Example 2: Sleuthing Collusion

Another example of sleuthing via shared calendars occurred when I and some other people in my workplace suspected that a group of coworkers was colluding on ways to damage the broader organization. Without going into detail, the basic situation is that we had a big membership organization, in which people from multiple other organizations collaborated.

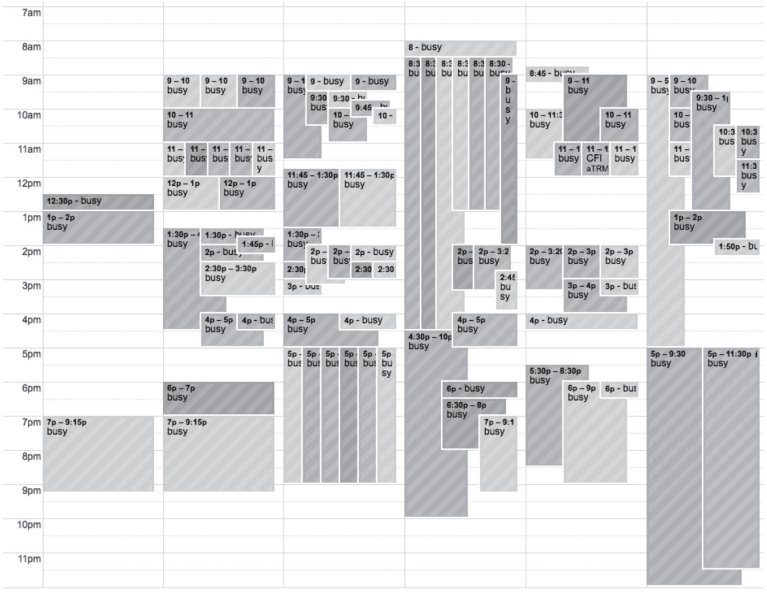
We had a neat Google Workspace setup, where everyone in all the constituent organizations had access to the same shared platform: calendaring, documents, etc. But everyone had a login and email associated with their own organization (functioning as a sub-organization within the Google space).

Here's a made-up example to illustrate. In the *2600* context, you could imagine a single Google domain for 2600meetings.net, and then people in Austin would have austin.2600meetings.net or austin2600.2600meetings.net (or even weareaustin2600.org - they don't need to share the same top-level domain).

This type of setup, in my situation, let people create invitations via Google Calendar with people from across the whole broad organization. We could also share documents and other activities on the Google platform. Very convenient.

When my coworkers and I suspected there had been some meetings among people working against the broader organization, we used the same method as above to look for alignment in calendars, across several people. We didn't have access to see all the calendars, but we could see enough. This also served to discover a few people who we were not sure were part of the collusion or not, and rule out some others.

Since one of the collusion meetings occurred right after an in-person meeting that was publicly known, we even knew where this took place - all without being able to see details of anyone's calendar events. Some people's calendars were completely unavailable, just like the top administrator in my earlier example, so we couldn't know for sure whether they were involved or not.



Aligned free/busy time for a group of people

All this sleuthing yielded precious insights into what had been happening. Rather than old-school surveillance (following people around, secret cameras, phone taps, looking through trash cans...), it was easy to make reasonable inferences of what had been happening simply by using the Google calendar to see free/busy time.

Preventative Steps

Shared calendars are very useful, and the sleuthing I described doesn't involve using calendars in a way they were not intended for. No privilege escalation is needed, and no workarounds.

However, using calendars as they are intended within an organization results in information leakage that may be unintended. Did the search committee want it to be possible for meetings and deliberations to be inferable across the organization? Including whether the incumbent candidate had received an interview? Surely not. Similarly, the collusion meeting mentioned above was in fact a secret - its very existence was withheld from close colleagues who attended an earlier meeting. But by looking at calendar alignment for those who made their calendars visible, the existence and partial attendee list became visible.

This creates a situation where the convenience and utility of making free and busy time visible is offset by the need for basic operational security: where people are and with whom they are meeting. Those with higher needs for operational security, such as administrators, human resources personnel, and others in sensitive or leadership roles may well choose to lock off their calendars from others in the organization. This makes it harder to schedule a meeting or other event; emails, phone calls, etc. will be needed to ascertain when all parties are available.

Whether this tradeoff is worthwhile depends on the role of the people involved, the size of the organization, how spread out people are, sensitivity of organizational activities, etc.

All that said, there are clearly some implications that anyone using a shared calendar, or managing an organization's calendar settings, should consider.

The domain administrator should select defaults deliberately and ensure everyone getting an account is informed of these defaults and how to change them.

Domain administrators should utilize an explicit off-boarding process for people who leave or change roles, so that any access they have to the calendars and other applications is disabled.

Individuals should not open sharing across the whole organization, unless they are sure that is desirable. Consider the number of people within the broad organization, and then consider how many have legitimate need to access any of your calendar details.

Consider a "least privilege" approach to calendar sharing:

By default, no sharing or visibility of a calendar to anyone.

- Free/busy time viewing should be enabled on a need-to-know basis for correspondents and close organizational members (i.e., same department, boss, etc.).
- Full calendar details should only be available to trusted individuals.
- The ability to make edits/changes to a calendar should almost never be granted, except where it makes organizational sense (such as an administrative assistant who needs to schedule meetings for other people).
- Calendars for rooms or other resources should only be available to people with a legitimate reason to use that room.
- Review your calendar sharing settings from time to time. Perhaps sharing was enabled with individuals for particular projects or collaborations and should be removed after the collaboration is done.

I hope this overview of Google Calendars has been helpful to readers. I've been using Gmail and associated tools for 20 years and have been a domain administrator for several large and small organizations, as well as an end-user in organizations I worked for. Information leakage via shared calendars is something I've observed frequently.

The convenience of online calendars is undeniable. The risks of unintentional sharing are important considerations for anyone utilizing such a service and, as with all tools, it's important to consider these risks when making decisions about how to configure and use the tool.

I LOVE SMART WORKING

by blue_elk934

"Raise your hand if you want remote working to last forever."

This question could be asked to pedestrians paying attention to their smartphones or in a post where an elaborate answer is replaced by a heart, a bulb, or a clap. In 2020, I read a LinkedIn post that listed all the advantages of remote working. In 2020, COVID severely affected Italy and, for this reason, one of the first measures enacted was the massive implementation of smart working. It is not surprising that most people happily approved of this decision.

Together with the numerous advantages of smart working, it must also be considered that the pandemic was a tempting opportunity for some bad guys. I want to imagine these guys as if they were in a restaurant. I'll give an example:

Starter: understanding the victim's network infrastructure

Main course: entering the victim's infrastructure network by phishing email for the employee

Second dish: once inside the victim's network, launching an SQL injection to disclose the employee's ID

Side: finding out the managers' emails, telephone numbers, and those of other important people

What about the dessert? There you go: a ransomware that could knock out the enterprise!

My example could be funny for most people, but it's an unfortunately true story. In 2020, the information technology attacks increased by 12 percent. In particular, there were attacks with impacts of "high" and "critical."

In a large part of this alarming percentage, many attacks were caused precisely by:

- The use of personal and non-corporate devices (laptops, smartphones, etc.) (the so-called BYOD - Bring Your Own Device)
- Naive employees attracted by phishing emails who downloaded dangerous attachments or entered company login credentials
- The inadequate security of home routers played a fundamental role (for example, using WPS and WEP ciphers)
- Employees exchanged emails containing top secret data without using cipher email plugins.

Some people may think that this situation was due to the naivety of the employees. However, the companies should have invested more into areas concerning security.

I came up with some ideas:

- First of all, it is important to give companies the opportunity to invest (with tax advantages) in secure fields in order to train employees and enable them to protect themselves from these cyber threats. If companies do not have enough resources to invest, the government should intervene through state contributions.
- Have employees use only company devices, avoiding the so-called BYOD.
- Also involve schools in the training process, because students are more technologically literate than their parents (the employees). It could be an opportunity for discussion, dialogue, and greater awareness of cyber threats.
- Employees should be allowed to report safety issues quickly and easily - every minute counts!
- The use of IDS (Intrusion Detection System) that monitors the behavior of the corporate network.
- Also, simulating calls to employees (social engineering) and ad hoc phishing emails would be useful to understand the degree of "naivety" of employees.

If smart working is the method of working in the future, we need to intervene immediately with awareness and tenacity!

After these years of the pandemic, I think the time has come for the so-called renaissance of cybersecurity to occur in the world. This is a great opportunity for a profound dialogue on this issue that can lead to greater collaboration between computer experts avoiding vanity and popularity, that popularity existing just because you have a resume full of semi-series computer certifications and 5000 connections on Linkedin!

Land Mines

HOPEward Bound

Dear *2600*:

I will be submitting a talk soon for consideration, but still wanted to purchase a ticket while they're available. Thank you *so* much for organizing this! I was there in 2016 and it was a really special time. Hope to see you soon.

Halley

We thank you for your support. As of now, there is still time for people interested in submitting a talk or workshop to our upcoming conference. It's going to be an historic event. Full details can be found at www.hope.net. And your ticket is free if your talk is accepted!

Fixing Phones

Dear *2600*:

Recently, AT&T accidentally killed my dad's Samsung Galaxy S7 which is 4G and compatible with their network. They thought his phone was stolen since the original account holder (my mom) had passed away. His name is on the account. Anyway, it's been three days now and they cannot get his phone to work (as in call or receive calls). Is there any way on our end to somehow deprogram AT&T's kill code? Or are there only two options: asking them to replace the phone or buying a new one?

Barry

This should be possible, but it's likely all of the data was wiped from the phone. Between AT&T and Samsung, this seems solvable, but you need to convey that it was their mistake in the first place so they feel some obligation.

Dear *2600*:

My mother has dementia. She lives out in the desert with my tech savvy father. She walks daily up and down the road with a neighbor and by herself. She knows the area and feels safe (and we feel comfortable with her doing it, the community is constantly driving on the road and people always stop to say hi and chat, and don't hesitate to help if needed). We don't want to take that independence away from her, but at times it gets scary.

She recently lost her iPhone and it was dead, so the Find My iPhone app was useless and the problem was solved with just getting her another phone. Her phone is her lifeline and, as a retired realtor and social person, is a must for her. Texting, calling, emailing is second nature for her (even though now it gets confusing).

I had a coworker tell me about how her young teen just got her first phone and about the app she put on it that literally gave her access to GPS, microphone, video, texts, calls, and whatever else. I looked up the website and it was an app you downloaded, a monthly fee, and the app showed up as a calculator app and you put in a code to access it. This was like a decade ago.

What do you recommend? I want GPS, video, and microphone. I don't want to say money is not an issue - there are a bunch of free apps out there and I just want something reliable.

Max

Ironically enough, the app you're looking for is known as a "parental control" app, which is kind of the reverse of what you want to do, but the description still works. The features you're looking for are almost identical to what parents want to control on their teenagers' phones. Assuming having pornography sites blocked won't be an issue, we believe this could easily work for your needs.

We suggest searching for these "parental control apps" online and trying them out before committing. The average cost is around $50 a year, which is well worth it considering that support and updates are usually included.

Dear *2600*:

I was having new fiber service installed and got talking to the phone engineer. He was telling me how the U.K. is going to be turning off their analog public switched telephone network (PSTN) service in a few years and you would only be able to get data/VoIP services. Kinda made me a little sad, as I have great memories of me and my friends messing with the analog phone system, opening the BT box in our estate, connecting our homemade linesman set, etc. We even found a guide on a phreak message board on how to physically get into most local BT exchanges. That adventure is what set me off down the IT/technology path. Do you think that would be the end of phreaking or do you think it can live on in a VoIP world?

Michael

It's always going to be possible to mess around with phones, no matter what form they wind up taking. And there will always be new devices that we haven't even imagined yet where our imaginations can roam wild. That said, it certainly will be a great loss to not have analog phone service, a phenomenon we're slowly witnessing in the States. We think it's always best to mix new technology with old, as there will always be times when the newer systems will fail. For instance, during extended power failures, your local central office typically had enough battery power and generators to keep your phone connection working uninterrupted for weeks. Newer fiber systems only last a few hours without power. Cell phones have other issues. During catastrophic events when you need a phone the most, a cell tower can lose power or connectivity, making your phone useless. And if you lose power, it will be difficult to charge your phone. During last year's hurricane in New

Orleans, government officials were unable to call the local television station to share information for precisely this reason. Those with old-fashioned landlines had no trouble getting through.

In the end, it all comes down to profit, and the copper network just doesn't provide enough of that for phone companies to continue investing in it. We believe there needs to be a way to keep it running in order to provide enough of a backup in the event of a catastrophic event. They do tend to happen.

Observations

Dear *2600:*

BBC *finally* set up official Tor mirrors and introduced Tor to their viewers/readers. Links are below. Believe it or not, Facebook can be officially accessed using Tor too.

(facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mh ➥bshg7kx5tfyd.onion).

"The BBC has made its international news website available via the Tor network, in a bid to thwart censorship attempts. The Tor browser is privacy-focused software used to access the dark web. The browser can obscure who is using it and what data is being accessed, which can help people avoid government surveillance and censorship. Countries including China, Iran, and Vietnam are among those who have tried to block access to the BBC News website or programmes.

"BBC News in Ukrainian: https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion/ukrainian

"BBC News in Russian: https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion/russian

"BBC News internationally: https://www.bbcweb3hytmzhn5d532owbu6oqadra ➥5z3ar726vq5kgwwn6aucdccrad.onion."

Ilgaz

This actually happened back in 2019, but its importance is being realized now. Of course, the hardest part can be getting the news about the existence of these links out to the affected people. We are learning a lot about control and blocking of the net, and clever ways of getting past these restrictions. The hacker community is key in making that happen.

Dear *2600*:

The information super dirt road! In America.... Get a "forbidden" message trying to access RT News from home through AT&T, but it pulls up fine on my phone. Nothing like good old fashioned thought control.

Robert

Thought control is closer to what is being blocked. You will always be able to find a way to access the lies and hatred of the Putin regime as you've demonstrated. But nobody is under any obligation to help them spread their message. Sites with illegal or terroristic content are generally shut down or blocked. Why should this state-sanctioned propaganda site be treated any differently?

The sad fact is that no matter how much evidence is presented from independent and reliable sources, it will never be accepted by those with a vested interest in continuing to spread lies. We can either continue the dance into perpetuity or take a stand for justice. It really shouldn't be a hard choice.

Dear *2600*:

I was just watching the movie *Hackers*. There was a part where Dade asked his buddies if they knew who Acid Burn was. They said no. But later they did know.

Rostislav

This is actually true. Our theory is they were simply lying. We know this never happens in the hacker world, but it's possible.

Dear *2600*:

The Russians tried stealing my wife's Microsoft account today. Do your worst.

Kaleb

It didn't take long for them to up their game, did it? This will surely be their undoing.

Dear *2600*:

The AWK keyspace iterator should have been written in portable C. I apologize for the inconvenience.

Justin Parrott

It happens. But AWK is nothing to be ashamed of.

Dear *2600*:

I opened an AOL account in 1993 and haven't touched it in 15 years. Holy shit, it's still there. I just logged in.

Chris

This is what digging up an old bone must feel like to a dog.

Dear *2600*:

The Ukrainian military has an "IT enthusiast group" within their ranks that travel around on quad bikes and use drones to drop bombs on Russian tanks. This is every IT desk jockey's dreams realized.

Alex

No reason they can't outsource to bored employees around the world.

Dear *2600*:

Weird first world problem: I use Keepass to store and generate long, complex passwords. If the website allows it, I use caps, lower case, numbers, and special characters and use 20 or more total characters. My problem is that when I'm typing these numbers into my phone, I have a hell of a time telling the difference between a 0 and an O or an I and a l. I end up having to copy my password into MS Word and then change the font to an easy to read font where the letters are unambiguous. That's all. I just find it a little funny. I would not have had the same challenges on a Commodore 64 or Apple][. The fonts on those early devices were pretty well designed for being so low res.

Charles

We're told you can indeed select a different password font. But we know this has been a problem

in many places. And a rather funny one, too.

Submissions

Dear *2600*:

I sent this to another website, so I am disqualified now.

submitting

While true, we still felt it was good enough to share with our readers. So we're including it as a letter below:

Dear *2600*:

I didn't know I could be called a hacker until recently. I have some computer skills, but that's not what would make me a hacker. When someone mentions "hacking," it usually presumes pentesting, programming, or cracking. Those are aspects of it, but what does it take to be a hacker? I think a hacker is someone who is driven to achieve their goals, almost obsessively. I think a hacker demands to live life on their terms, by their own compass, so to speak. Hackers not only want to live life the way they want, they also have the intelligence and ability to make it happen.

When I was young, I read everything that interested me. I wasn't very social, so for many years I had books as my company. I developed talents for writing, psychology, and computers, along with an interest in art and music. I was, maybe still am, a divergent thinker; I thought for myself and I felt good doing it. As a result, I wasn't interested in what the educational system had planned for me. I was not only placed in the "gifted" classes, but I was also held back a grade! My lack of interest had gotten me branded as a failure. My attitude towards the educational and economic system was completely soured. Today I live with my parents and am ineligible for employment. I recently thought that I should have known when to compromise. Still, some things are worth standing up for even when you know there is a cost.

I also learned about P2P systems. Finding and sharing files with people over the Internet brought in exciting new concepts that I wouldn't find anywhere else. They helped define my tastes and skillsets. I was really lucky to be a youth in the mid 90s. I don't think everyone realizes what they are giving up when they delegate their lives to companies like Facebook and Google. I have wanted to live free from interference for my whole life. For quite a long time, I thought that meant fighting the government and corporations.

After school came the insanity. I developed schizophrenia and lost everything. I was housed in a community assistance program. I think most people that I knew expected that my story was over. No! I was pretty messed up for a while. I later had a change in environment and I regained my ability to self- regulate. I learned the skills I needed to get back in control of my mind. I also did very well socially. I didn't give up on myself, I just needed time and a plan. I think it's important to always have a plan. Be willing to change them if you need to.

submitting

This is a great story and deserves to be shared. We think there's a lot more you can say which will enable it to qualify for our "Hacker Perspective" column in the future. As the above was already published online and now printed in the magazine, it would have to be rewritten. But the good part about that is that this version is relatively short, which means there's much left to tell. The column itself needs to be about 2500 words - significantly longer than the above - but we believe there is a great deal more insofar as experiences, philosophy, and, of course, the changing technology of the times described. Like growth itself, there are challenges, setbacks, and surprises when putting together a piece like this. We hope you take the time to tell the story; we believe many of our readers will be interested and inspired.

Dear *2600*:

I'm a network engineer with one of the *big* ISPs out there, and I've bumped into a few things having worked in data centers, backbone (yes, the Internet and P2P connectivity to everything inside my company), and most recently with my IP management operations team. I have a couple of ideas for things I've seen and worked on regarding securing the Internet, and massive hacks I've experienced (I'm talking about things that brought Cisco 9K routers to their knees). Was curious if you'd be interested in this kind of thing?

Chaz

You have us at the edge of our seats.

Requests

Dear *2600*:

I need a login seller
Like Bank logins...
CC logins
Local bank

Hills Mary

Tell us honestly - does this approach ever work? We strongly doubt you can say anything honestly, but it's worth asking.

Dear *2600*:

Hey, is it okay with *2600* if my friend who runs an online publication reprints the *2600* article I wrote? Thank you.

Michael

It's your article, so you can have it displayed anywhere you wish after it's printed in our pages. As a general rule, we ask that the author and magazine are attributed.

Dear *2600*:

I want a link to download fb account

Pramod

Just once we would love to pursue this sort of inquiry to see just what on earth is expected of us. No details of any sort are ever given; we're presumably expected to read people's minds and furnish them with the exact info they're in need of. We can only assume that what's being asked for here is a universal link that allows someone to download any Facebook account anywhere. Because that's what we're all about.

Dear *2600*:

Subject: Article for 2600
teach me how to become a hacker

Florianus

We're curious if other fields of study get people sending these one line requests constantly, expecting to be injected with wisdom and knowledge through the Internet. What was particularly ironic (and disappointing) here was that this email was entitled "Article for 2600" so we were expecting something truly awesome.

Inquiries

Dear *2600*:

Aside from *Sneakers*, what are some other 70s, 80s, and 90s era hacker/phreaker movies or shows?

Matt

We'll open this up to readers so we don't play favorites and/or leave out worthy candidates. But we suggest also including the decades prior to and after your date range. And while there are a bunch of films and television series that focus primarily on hackers, there are even more that touch upon them briefly, as a single episode or small part of a film. And, of course, don't limit yourself to only American material. There is a great deal from English-speaking countries like Canada, Australia, England, etc. Nor should you limit yourself to that either, as there is a ton of material in different languages from other countries that you can see dubbed or with captions. Among all of these, there are examples that are so terrible that they're really worth sharing. And there are also classics that are found in the most unexpected places. We will be happy to share reader opinions on these.

Dear *2600*:

We are two college students from the University of Paris majoring in a master of cybersecurity. We are requested to publish an article in a hacking magazine. We are currently working on an xml injection article and we would like to know if you could help us with publishing our article. If the answer is positive, we would need to know your deadlines and if we have to have a certain template for the article that we'll be doing,

Lylia & Moncef

This is rather unusual, as there aren't that many hacking magazines around, so this assignment seems designed with us in mind. Anyway, you're more than welcome to submit your article to us at articles@2600.com with as much detail as you can include. We prefer straight text, but any format will do. As for deadlines, we're always working on future issues, so that's not something you need to worry about. Just send it in and, if accepted, we'll have it printed in a future issue. Good luck!

Dear *2600*:

Sorry if this is a dumb question. I'm curious to get my hands on a red box to have for conversation and to potentially play with. Is that something I can buy somewhere or do I need to build one?

Matt

Definitely not a dumb question. Just don't expect to be able to use it to make free calls from payphones anymore. There are plenty of schematics available online if you actually want to build one. It's also incredibly easy to generate the tones with virtually any audio software. The tones are simply 1700 Hz and 2200 hertz combined. A nickel is represented by that tone played for 66 milliseconds while a dime is two instances of that tone separated by 33 milliseconds. A quarter is a little different: the frequency is only played for 33 milliseconds and each of the five instances is separated by 33 milliseconds. (They really should teach this in schools.) If you're looking for an actual physical red box that someone may have used in the past, that seems like a great thing to ask for in the "Wanted" section of our own Marketplace, which is free for subscribers.

Dear *2600*:

We are two students in cybersecurity Master's Degree at the University of Paris, and as part of one of our classes we have to publish an article about the way we could build undetectable ransomware in Python in 2022, avoiding Windows Defender.

Do you accept article submissions? If you do, what is the process to do so? We thank you in advance for your help.

Barrault & Fabi
University of Paris, Paris, France

So how many of these are we going to get? Are you all in the same class? We can't wait to start getting all of these French articles.

Dear *2600*:

Why the name *2600*?

Max

Every couple of years, we're obligated to answer this question. 2600 hertz was a frequency used by the phone company. If you sent it down a long distance connection, you basically seized control of a long distance trunk and gained the ability to route calls throughout the world using special multifrequency (MF) tones and completely bypassing billing. When naming our magazine, those numbers were the perfect symbol for what we stood for: exploration, technology, mischief, and occasional free phone calls.

Dear *2600*:

What email list server do you guys use?

Kris

As we tend not to trust outside companies for this sort of thing (they tend to disappear, impose policies we can't live with, or violate people's privacy), we've been relatively content with Mailman. Except for the things it does badly which drive us crazy.

Dear *2600*:

I've got a very good question! What does your passport say when you travel to another country where you owe a traffic fine or appear to be due in court? Will my crimes in France show up in America? Will my past traffic citations show up when I return to Australia or America or Europe or any of those countries?

William

Yet another France-related letter. To answer your question, it really depends on what your crimes are. If, say, Vladimir Putin were to go through passport control in virtually any country in the world, all sorts of alarms would go off. Your traffic tickets aren't going to interest anyone at a border unless they involve a stolen car that you're attempting to drive over that border. Your passport only contains info that is then cross-referenced in various databases. Your identity may be flagged if you're a wanted criminal or on a particular country's list of undesirables. Your traffic tickets could, however, pop up if you try to rent a car and present your driver's license. Good luck with whatever's going on here.

Dear *2600*:

One of the big discussions in the cybersecurity industry right now is whether or not destructive tools are covered by the Second Amendment. Cryptography will likely be contested at some point, and the likely scenario there is that the Fourth Amendment will cover your personal right to strong cryptography. But hacking tools, especially those designed to cause damage, are more like weapons. Owning malicious software has never been a crime, nor has writing malicious software. But as the ability to cause real world damage increases, there will probably be attempts made to limit access to them. A key difference between a software tool that can damage an enemy's computers and a weapon that can kill a person is that the software tool only has that one purpose. It isn't by design a defensive tool, nor do you need one for any purpose other than to harm someone else. But I'm curious what you think. Will hacking tools designed to cause damage be targeted by governments? What about those who use them, or who built them? And if so, should those be covered under existing laws?

Chilton

Amendments to the United States Constitution mean nothing in other countries, so that right there tells you how difficult it would be to eliminate such tools - or to guarantee their protection. And it wouldn't take much to define a malicious bit of software designed to damage specific hardware or software as a defensive tool, in much the same way this logic is used with physical weaponry. One thing is clear: most governments lack a clear understanding of technology, so they will attempt to control things they have no power over. It's certainly possible for penalties to be enhanced if a crime is found to have been enhanced by a specific tool. It happens all the time.

Dear *2600*:

I'd like to ask a question. I am looking for info about the *2600* meetings in Paris, France.

It used to be on the first floor of the Burger King at Republique, but now I cannot find any info any more.

I'd be grateful if you could help me because I'd love to join the meeting if it still exists.

Tatiana

So all of the hackers are in France now apparently. That's fine with us. Concerning the meetings, as of this writing we haven't heard from anyone in France interested in restarting them after the pandemic. Since there are clearly a lot of interested people over there, it's only a matter of time before someone writes in to meetings@2600.com or DMs us on Twitter (@2600Meetings) with location info. It could be you.

Dear *2600*:

Why does the mag not follow the season at the real time? Autumn was released in December and Winter in Spring.... When will you come back to the real seasons? Thanks for the info.

Discovery

This is a direct result of the craziness of 2020 when we were severely affected by COVID-19. Bookstores shut down, issues were thrown out, and we very nearly didn't survive. When the dust started to settle, we were behind by a bunch of months. We didn't want to skip a season or "catch up" by putting out a double issue. Since we're not really tied to seasons in the first place, we felt the best way was to cut time off of each issue's shelf life and get closer to a normal schedule with each passing issue. We had a decent plan in place that would have had us caught up by July 2023, but then our printer had a supply chain problem with paper and we had to push that back to the end of 2023. But we're making steady progress and the day will come when you see the season printed on our covers and at the bottom of our pages once again. We look forward to it.

Further Info

Dear *2600*:

In a recent issue of *2600* (38:3), you received a letter from a Roscoe Village alderman's intern requesting that you address the beat-up *The Hacker* newspaper box in their neighborhood. I have some un/fortunate news.

The box in question is actually owned by *The Heckler*, a relatively well-known (in the area) satirical sports publication. I find it amusing that this intern was not just unaware of *The Heckler*, but also went on what must have been a great trip down a hacker publications rabbit hole and ended up on you.

Enclosed is a nice shot of the box from Google Street View, with a very legible *The Heckler* logo.

J0hnnyXm4s and the Chicago *2600* crew

Thanks for helping to solve this mystery. It's proof that not only do we get blamed for the misdeeds of hackers everywhere, but hecklers as well. But we're thrilled that not only are there still newspapers, but sports newspapers, and also satirical sports

newspapers. We love surprises like this.

Dear *2600*:

I never knew this... saw it on Twitter. If you want all images from a .docx file, just rename it to .zip and extract the media folder.

Austin

And who says you can't learn something from Twitter?

Dear *2600*:

Hello fellow readers of this insanely amazing magazine! Fellow reader since the 90s here! I thought this little challenge might appeal to you all. We have been working on a way to safely transmit signals for our trading systems (and other systems) end-to-end by encapsulating the data into something like the following:

052827154109282846109285912054799621027263066004309903114730008026646308097948174114729050

But we'd like to make sure that no one can actually figure out what it says without us telling anything about how the string was created. Your job is to decipher it. If you figure it out, send your solution to tcarey1053@emailinterface.org. Good luck!

sky henrikssøn

Readers, please don't miss the summer trying to figure this out.

Dear *2600*:

I am writing a horror novel. It is called *Legacy Code*.

Arne

We hope it's more verbose than this proclamation.

Thwarting Security

Dear *2600*:

I found a hilarious way to get around select news website paywalls. In some cases, simply turning on reader view - in Firefox or Safari - washes away all signs of having to subscribe. So far, I know of three websites that this works on: *The New York Times*, *The Epoch Times*, and the *The Daily Wire*. Maybe these websites should consider patching this hole.

Snake in a Lawn Mower

We're sure they're considering that right now.

Dear *2600*:

Me: "I'd like to test your color laser printers please. I'm looking to purchase one for my home office. I brought a sample of what I would be printing often on my USB flash drive."

Staples Clerk: "No problem sir. Do you need my help? If you need extra paper, let me know."

Me: (on the way past the print center on the way out): "Hey, how much do color copies cost?"

A customer doing their own self-printing: "$.57 per page."

Me (pointing at the printers for sale section): "Wow, well I just got $74.10 worth of printing for free just over there."

Hacking skills require innovative solutions to common everyday problems and you don't always need a computer, yes?

Johnathan

We doubt you could get away with that more than once in the same place. While an overall sleazy move, you get extra points for rubbing it in with the poor guy who was following the rules. And for instantly calculating what your 130 pages would have cost.

Dear *2600*:

Would *never* do this, but on American Airlines, Sprint users get free Internet. When it asks for your phone number, I bet you can just keep upping your phone number by a digit until you are matched as a Sprint user.

Eric

It's not quite that simple. First off, these deals are always changing. And T-Mobile has taken over Sprint. Beyond all that, you generally need to have your phone with you, as you're using it to connect in airplane mode. But we're certain there are many tricks you can play while in the air, including sharing the connection you eventually get with others.

Dear *2600*:

This is something I discovered several years ago, brought to the attention of my employer and the software publisher... but no fix has ever come through. Figured it was time to suggest that other people fix their systems. If your employer uses SMAtechnologies.com's product called "OpCon," you need to look and clean up a serious security issue this application installed on your system (if you haven't already).

One of the secrets to how it does its thing is by installing a public key for access to the root account of the target UNIX system. The public and private keys for this account are included in the application distribution file. The public key is installed without notice or prompting, and it is the same key pair used on every single OpCon installation - it is *not* locally generated. So every administrator of a system with OpCon installed on it has root access to *every other OpCon server in the world* they can get SSH access to. I think that's kinda bad.

At my employer, we discovered we could remove the key without any impact on our operations. Apparently this was part of a magic "move files between machines" function we didn't use, in spite of using OpCon extensively.

After discovering this problem, we implemented stuff to make sure that the key didn't get reinstalled, as it did after every OpCon update. The key you want to remove looks like this: "ssh-rsa AAA**{...}**3wfcDE= root@redhat4as". Yes, it is a very old RedHat generated key. This was pulled out of an AIX system, but it appears to be the same key for every install.

Honestly, it scared the crap out of me when I found it on all our servers - a key with a completely undescriptive identifier field? I was quite afraid all our systems had been compromised. The key files exist in the distribution .tar file as bin/sma_id_rsa and bin/sma_id_rsa.pub.

SMA Technologies was not aware of this when I brought it to their attention, and it took several iterations of explanation before they set up a

conference call to discuss it with me. I had to explain to them how SSH worked, how key logins worked, and why a 15-plus-year-old common key for all OpCon installations was a really bad idea, and installing it on the root account was a potential disaster... at which point I heard a quiet "oh shit." And nothing more after that, other than repeated "we are working on it."

Nick

This was shared on one of our Facebook groups, so we certainly hope it's been fixed by now. This is the kind of alertness we all could use more of.

Ideas

Dear *2600*:

OK, crazy thought: electricity and water being so similar in their behaviors (always flowing to low ground; susceptible to resistance, capacitance, and other forms of flow control), it's possible to construct a water-based Turing machine. So in theory, a city's plumbing and sewage system could be designed to also perform computations. Obviously, it would be extremely inefficient, and probably inconvenient for the city's inhabitants, but theoretically....

Deva

Theory is what we live for. Remember, Charles Babbage is considered "the father of the computer" and he lived in the early 1800s, before the age of electricity. We doubt you'll get any grants for this kind of research, but it's sure fun to imagine.

Dear *2600*:

I am not a cryptographer. I am an amateur mathematician. I read Steven Levy's *Crypto* book where Whitfield Diffie traveled the U.S. inventing public key cryptography before it existed. I read about the RSA encryption scheme and thought I'll take the simplest explanation and see if a pattern existed in the multiplication where N=p*q, knowing only N. I believe there are patterns that can be seen in many different equations, three of which I list below - where N=p*q, p being the smaller factor and q being the larger.

Crypto is popular due to cryptocurrency. These equations are specific to the prime factorization problem where a large semi-prime number is factored into two prime numbers, but I hypothesize it could be expanded to logarithmic and modulus problems. I do not know how the prime factorization problem would affect cryptocurrency, but it will break the one way function of RSA.

The equations are complex, but only algebra. There are multiple variations. But I believe in these equations. I even advertised in *2600 Magazine*. I post in a letter and not an article because I have posted these equations on message boards. Also, on first inspection, no one knows if this is correct. So I wrote a letter hoping that some cryptographer will read it.

p^3 - (p^3*N^2) / (N^2 + p)
p^3 - (N^2 p^3)/(N^2 + p)
p^3 - \frac {N^2 p^3} {N^2 + p}

The above equation should be close to zero, but sometimes the error is closer to one.

(p^3 *N) / (N^2 + p) = fraction
fraction/ p = fraction / (N /p)
Sqrt[fraction / (N /x)] * N = p^2

The above equations are the second example.

q = Sqrt[(N*q^2 + q)/ N]
q^2 - (N*q^2 + q)/ N is approximately 0
In the case where N = 85 and q = 17,
q^2 - (N*q^2 + q)/ N is 1/x or 1/5 or 0.2
0.2 * 85 = q or 17 in this example

Bobby Joe Snyder

And if some cryptographer has a comment on this, we will print it.

Memories

Dear *2600*:

Anyone from the 80s remember running your computer overnight to collect 950 Sprint calling codes? Good times.

Paul

*That was one activity, although long distance dialing codes were so insecure at the time that they could even be guessed without the help of a computer. The real fun was in the exploration of phone numbers, where you would leave a smart modem running overnight, dialing phone numbers in succession and logging any that picked up with a carrier tone. Sure, hundreds of phones would ring in the middle of the night. But there was no such thing as Caller ID or *69. Seeing that list of phone numbers the next day that led to computers - BBSes, dialups to secret networks, and more - was part of the magic that drove the hacker scene.*

Opportunities

Dear *2600*:

The F.B.I. 's Silicon Valley counterintelligence field office is seeking qualified people who can help protect computers and computer networks. I think that many readers of *2400 Magazine* have the expertise to lend a hand defending America during this very challenging time that has left America very vulnerable to cyber attacks that can shut down mission critical communication and computers that control electricity, credit card payments, gasoline production, food warehouses, traffic lights, television, radio, cars (cars have 4G modems that allow hackers to send remote commands to engines, brakes, etc.), etc.

Jeff

We'll be sure to pass that along to that weirdly-named magazine.

Dear *2600*:

I can clone your partner's phone and link it to yours without him knowing and recover all deleted messages and chat on his phone so you can see them.

Michael

We wouldn't be surprised if Michael could also see them. Not our recommended route.

Dear *2600*:

Can I trust you? I have a business proposition regarding shipment of gold bars. Get back to me on mg.brewer@beco-techinc.co for more details and as well discuss the terms and condition for cooperation.

SSgt. Brewer Michael

You can trust us. We can't speak for the tens of thousands of people reading this, though. But you knew that when you emailed the letters department, didn't you?

Dear *2600*:

Hi Eliza,

My name is Todd Weiss. I'm a former VP of a Fortune 50 company, so I'm familiar with the corporate grind. I've also experienced the benefits of owning two franchise fitness concepts.

I noticed that you work with *2600 Magazine*. If you're happy in your position there, that's great. And I genuinely hope you are! But if you've ever thought about exiting corporate America, I can help.

Todd Weiss
Franchise Consultant

Well, great. Now we've lost Eliza. Game on, Todd.

Dear *2600*:

Please do as much social engineering on this account as possible! Doing a search of his email and social media presence indicates he is very open with his details of his workplace between Canada and the U.S. and flowery preamble to complain to a company that has wronged him - message headers usually don't provide any info on the targets ("Undisclosed Recipients") but I love the way he spearphishes!

J.

Yeah, we're not going to get involved in whatever this is all about. Suffice to say that using spearfishing techniques to track down a spearfisher can certainly be fun, but it's best to play the game on your own and share your final results. Otherwise it can quickly spiral out of control.

Responses

Dear *2600*:

In response to the letter by Shocked998 (38:3), I have been reading *2600* shortly after it began and had been reading other hacking philes and mags prior to that and after that, although my support of *2600* has waned in the last decade or so and I'll explain why throughout this letter. However, Shocked998 mentioned a letter by 6NdLXzc2 in which they described 6NdLXzc2 as whining. I have not read this letter, so I am not familiar with the content. But, describing a letter as whining about the political bias of the magazine was a tip-off of where Shocked998 was going. So, I'm guessing someone said a bunch of things that Shocked998 didn't agree with, thus it became whining. Typical.

Well, I'll have to agree with the political bias of the magazine taking a really strange turn at some point in history. I noticed it as well, and it appears to be accelerating. After a long departure from *2600*, precisely because of this weird "political bias," I decided to try again with your most recent issue (38:3) and quickly discovered two things: the political bias is still there and the content is rather lacking in substance. It certainly isn't the magazine it used be.

So, now Shocked998 can write back again and complain of another "whiner." Shocked998 then says, "The hacker spirit is not sophism and conspiracies. The hacker spirit is not hatred and apologism..." Well, hacking throughout the ages has certainly entertained a multitude of conspiracy theories, conjectures, hypotheses, and so forth. So, not sure where Shocked998 gets the idea that hackers or the hacking spirit never dove into that arena because it has a massive history of doing so. This is especially true of UFOs and trying to figure out what projects government has done and what they were for and how they were carried out, covered up, financed, etc. Anyone who ever used a BBS system through the 80s and 90s knows this as most BBSes worth a grain of salt had scads of philes and discussion on such subject and often had government documents on various topics. So, yes, indeed, conspiracies were and are still very much a part of the hacking spirit. Further, apologism is a vast part of the hacking spirit, as even *2600* has made a documentary defending a position/person. The hacking community and *2600* are dedicated to defending the position of exploiting technology for the gain of and dissemination of information that other entities and/or people would prefer not be shared. The very nature of hacking pits one against someone else who does not want you to be doing what it is you are doing and places you into a position of defending your position and activities and why you share information. That is the very definition of apologism. So this statement by Shocked998 is very wrong in my opinion.

Shocked998 continues with, "The hacker spirit is not false equivalencies and bad faith. Instead, it is progress. As is humanity. Pushing the envelope and improving." Ahhh, no. That might be what you want it to be, but that is a false point of view in my opinion. The hacking spirit and/or the hacking community is all these things and more. Like anything else, the reality is it is full of good, bad, and all things in between. There is no prequalification to be a perfect righteous person before becoming a hacker. And there is no authority which rules over the ethics of hacking protecting the spirit of it. It is what is, man. It is an all encompassing subculture comprised of people with a passion to exploit, understand, and use technology... and the passion and drive behind this is not uniform across these people whatsoever. What Shocked998 describes is like the unicorn and rainbows version of hacking.

I can tell you that at the height of phreaking, most phreaks were indeed apologists defending their trade, craft, and practices in light of the fact they were basically ripping off the phone companies of the world, rightly or wrongly. And most phreaks wanted to place free calls, either to talk or to connect modems. And the reasons for this varied from just wanting to say hello to a friend to wanting to connect to a government system to see what could be found (conspiracy research, perhaps).

Then Shocked998 carries on with some biased views and arrives at "these radical idealogues cannot be convinced of anything that goes against their zealous belief. Whether it's trying to convince them that the vaccine does not have alien DNA,

microchips, or demon reproductive material; or trying to explain to them that rational and science-based public health messaging will change as new information is presented; or insisting that an attack on the nation's Capitol was not simply equivalent to a tour group, nothing seems to be enough," which is a lot to unpack, but points to an obvious and deep bias.

I've not heard of anyone talking about alien DNA in vaccines and I suspect that might have been said in jest in an attempt to make a particular group of people look ridiculous. However, even if I had heard of such things, I would listen. See, I don't really have too much of a problem listening, as it tends to offer opportunities to pick up new information and ideas that can lead to places and thoughts. I have, however, heard of people who are deeply concerned about the safety of these vaccines and who have very valid points and I have witnessed a concerted effort to silence these voices.

I don't know anything about demon reproductive material, but that does in fact sound very interesting. In fact, I would very much like to hear more on that subject and those ideas. As far as microchips, I personally do not believe there to be microchips, or nanochips, in the vaccines, however, the technology does in fact exist if it were to be used.

One thing Shocked998 has failed to acknowledge is that all forms of technology can be exploited for various reasons. All systems, especially control systems, can be geared toward good or bad purposes. Now, getting back to what I said about the hacking community and spirit, the biotech and pharmaceutical industries are hacking industries. Do they in fact subscribe to the hacking spirit as described by Shocked998? I think it would be naive and dangerous to believe that. It would be very naïve to assume that a control system, such as a government, or a health service, or a vaccine for that matter, is immune to being used as a vector to carry out evil or bad acts/plans. But from what Shocked998 wrote, I would read out of those words that that conversation wouldn't even be allowed by Shocked998. Hmm... now we get to censorship. Is that in the hacking spirit?

You see, Shocked998, you are not the gatekeeper or decider. If there were anything ever true about the hacking spirit or community, it was that dissemination of information was the priority and that each individual was his or her own decider of truth or fiction. And you should be damned, as in really damned, careful what you think is misinformation and what is not. Misinformation is typically a misnomer used by those who rather you know only what they prefer you to know and nothing else.

The hacking spirit and community I grew up with (late 70s to early 90s) consisted mostly of people who held their own personal beliefs but were willing to listen and allow people to have their say and we didn't freak out all the time on what people had to say.

ViSiOn/Strang'r

We'll keep this brief as you've already used a lot of ink. Believe it or not, we agree with much of what you say. The hacker community has always been open to a wide variety of views and has always considered all kinds of wild ideas as possibilities. That's what hacking is all about. But there's another part of hacking that's being left out of your analysis, one that is just as essential. We reach conclusions based on evidence, experimentation, and dialogue. Our minds can be changed when all of that is processed.

The resistance we're seeing is that of people who don't like the conclusions that are being reached. They seem to want a different conclusion and, if the facts don't support that, then the facts are deemed to be false. This is where our paths diverge. Then we then get accused of not listening or weighing the evidence when we've already done precisely that. And those making the accusations justify their conclusions with insufficient or faulty evidence. We are able to easily disprove them, but, as the original writer stated, we can never convince them of this. And that is what's not a part of the hacker spirit.

Sure, we've seen a lot of what you describe in the hacker world: being open to conspiracies, ripping off phone companies, etc. These are basically points in our development where a choice is made as to which path to go down. We consider all sides of an argument, but we generally conclude that it's the one with logic and facts that's correct. We may be tempted to use our interests and skills for illegal activities, but we usually utilize those skills productively and avoid a life of crime. There are those who make other choices, but we believe they distance themselves from the true hacker ethic by continuing down those roads.

A common complaint we hear in many circles is that people aren't allowed to make their own choices or to have a certain opinion. Nothing could be further from the truth. But, as the pandemic has taught us, certain decisions can carry certain consequences. Whether those are consequences doled out by nature or by society, we can't just make them go away.

The hacker spirit is most certainly about pushing the envelope and improving. That doesn't mean there aren't roadblocks and negative elements that must be overcome. But it's that spirit that moves us forward. Otherwise, what's the point?

Dear *2600*:

In 38:4, J accused *2600* of belligerence attacking the "majority" of your readers. J also questioned your trust in science and data using the fact that there were *some* (as in an extremely small percentage) front-line workers who chose to lose their job rather than get vaccinated. J even tried to use this: "It certainly must mean they have quite specific reasons - such as knowledge of likely damages caused by the COVID-19 vaccinations..." as logical support of their rationale that *2600* and most of the world is wrong.

Besides my assumption that J does not speak for

the "majority" of *2600* readers (and definitely not for me), the hacker mentality tends to look at things with an open mind, allowing for us to explore both traditional and especially nontraditional thoughts for any given situation, event, or problem rather than from a shut-off political view. The point J tries to make is not logical, nor has any scientific weight. The number of those who refused to get vaccinated and lost their job is low (and heavily weighted in "red" political areas), and that argument can be the same as saying "I always see nurses and doctors smoking outside hospitals, including cancer research centers. Therefore, smoking must be good for me."

Anyway, keep up the great work, *2600* team! This is one longtime subscriber who is not going anywhere.

Brad

We never thought speaking our minds and following science would be met with such resistance. We used to be amazed at how those who embraced logic and science in the distant past used to be treated. Not anymore.

Dear *2600*:

I enjoyed Gregory Porter's article in 38:4 about scripting downloads of .ts files to save online video. I also do this because my rural DSL line is too low-end to stream video, so I download videos to watch from my local disk.

Here are more tips. There is usually a .m3u file hidden in the HTML source; sometimes it's in a .json file that the HTML links to. Use the browser dev tools to search all requests for .m3u to find it. Download this file and you will see it lists all .ts segments to download.

Here's a bash script that takes a .m3u URL and output file name, downloads the .ts segments in the .m3u, and merges them into the output file. It assumes relative paths in the .m3u file.

```
#!/bin/bash
PLAYLIST_FILE=`mktemp`
TEMP_FILE=`mktemp`
curl -s -L --compressed --retry 3
➥"${1}" -o "${PLAYLIST_FILE}"
BASE_PATH=`echo "$1" | sed 's|\
➥(.*\)/.*|\1|'`/
while IFS= read -r INPUT_LINE
do
 if [ "${INPUT_LINE:0:1}" != "#" ]
 then
curl -s -L --compressed --retry 3
➥"${BASE_PATH}${INPUT_LINE}" -o
"${TEMP_FILE}"
  cat "${TEMP_FILE}" >> "${2}"
  rm "${TEMP_FILE}"
 fi
done < "${PLAYLIST_FILE}"
rm "${PLAYLIST_FILE}"
```

Some more advanced videos separate audio from video so blind viewers can select an audio track with narration over silent moments, or to offer different video resolutions without having to store copies of the same audio with each separate video version. In this case, the .m3u file will list the tracks with additional .m3u files for each track. You'll need to write a script to parse which tracks you want, then go after those second layer .m3u files with the above. Lastly, there may also be a .srt file in the HTML source, which is the subtitles. You can merge all three using: "ffmpeg -y -i subs.srt -i audio.ts -i video.ts -c:s copy -c:a copy -c:v copy output.mkv". If you found a .json file describing the video, you might also find metadata that ffmpeg can add using the -metadata parameter.

David Mooter

Thanks for what undoubtedly will prove to be useful code for many of our readers.

Dear *2600*:

Responding to David M's letter in 38:4: The effectiveness of the easy fix David M suggests is, as he notes, intimately tied to the assumption that there are no inputs that would trick models trained on different data sets. Results from experiments in other (non-cat) problem domains suggest that such inputs do indeed exist, and, furthermore, that the likelihood of finding such inputs increases with the accuracy of the models.

This might seem counterintuitive at first glance, until we remember that the accuracy of a neural network depends on its ability to generalize and detect learned features when they appear in novel data. An accurate model has presumably extracted the most relevant features associated with what we're trying to detect, e.g. "catness," and those features would quite likely look nothing like a cat to the human eye. Our working hypothesis for the explanation of the phenomenon described in the previous paragraph is that two reasonably accurate models have likely extracted and learned many of the same high-quality features during training, and therefore might be tricked by the same inputs where those features appear. In other words, there are a limited number of ways to skin a cat successfully! David M's easy fix works better for models with lesser accuracy and really well for models with close to coin-flip accuracy. Such low-quality models are often useless in practical applications, since they will produce excessive amounts of false positives and negatives.

Finally, I want to stress that these observations are based on early experimental results using image and time-series data, and that more stringent investigation might invalidate them.

Thor M

Dear *2600*:

On the back cover of the latest issue (38:4) is shown Herbert`s, which repairs typewriters and calculators. I think it would be just as interesting to see pictures of places like this as it is to see the payphones for the reason that these are probably soon to be extinct relics. Calculators can be an enormously fun place to start exploring hacks. Case in point: I have built an entire backtesting/trading simulator (for futures, stocks, et cetera) into a TI-89 Titanium calculator (among other cool things),

and if it were to malfunction, I would need such a place (probably). And, in federal prisons inmates are forced to still use typewriters (Swintec) for all their legal paper typings with printwheels costing a whopping $23 and print ribbons going for $7, because G-d forbid they put some kind of Word-like program onto the computers that we, ur uh, *they* use for emailing. Figuring out how to make it print from memory into the same format as a legal motion is quite a challenge. In short, these "primitive" devices are still full of Easter eggs. Perhaps a link somewhere at 2600.com for photos such as these repair shops (not that they can be seen in prisons - wink)? And I agree that we should de everything to preserve this increasingly rare repair knowledge. Cheers!

metaknight

We're glad to see this picture has evoked such appreciation. We know there are many more out there yet to be sent to us.

Spreading the Word

Dear *2600*:

NotTheFed.com is a pentesting company built from several decades of history in the hacker scene.

We were hoping to advertise in *2600 Magazine* and we were wondering if you had any details.

Marcus

Well, here's a mention in the letters section, which isn't nothing. But you can also have a free classified ad in our Marketplace section if you're a subscriber. Email marketplace@2600.com with your text and subscription info.

Dear *2600*:

I run a community hackerspace in Fresno called Root Access. Before the pandemic hit, we hosted our local Defcon group, DC559. Attendance was alright, we'd have maybe five or six people show up each month. (Tech isn't huge in Fresno, but it *is* growing.) Root Access has started hosting meetings again, and we're looking at bringing DC559 back online (or back from online, as it were).

I'm looking for ways to reach out to local sec folks and encourage them to come, and I think that listing in *2600* might be a good option. I know there are some *2600* readers around here because our local Barnes and Noble always seems to run out.

For a meeting to be listed in *2600*, does it have to be strictly *2600*, or do you welcome Defcon groups?

Thanks for all you do; I'm a big fan of y'alls work.

Derek

Hopefully this will help get those meetings going again. We only list our affiliated meetings on the meetings page (www.2600.com/meetings and page 66 of every issue) and those meet on the first Friday of each month. But other groups who meet at other times can get a free listing in our Marketplace section if the person submitting the ad is a subscriber.

Dear *2600*:

Despite the current demonization attempts of all Russian hackers and Russia (including Russian civilians) in general, *shout out* to the subset of Russian hackers who developed the website Library Genesis, a repository of the largest book, comic book, and scientific papers on the interwebz, and therefore by default the number one website in the world and in the history of humanity.

Janet

Sure, that's a good thing. But there are so many others who are risking their freedom and even their lives to fight the horrors being unleashed by their government. We need to figure out how best to support them, contribute to their efforts, and inspire many more to get involved. We agree that blanket demonization is not the way to go.

More on Meetings

Dear *2600*:

I don't see Cincinnati, Ohio listed as having a meeting. There used to be one. Not sure how long ago and if it's still active. Have you had any inquiries for Cincinnati? If not, what do I need to do to start up a meeting?

Donald

The short version is to simply find a decent public space and start getting the word out to people in the area while updating meetings@2600.com with the info. The longer version can be obtained the first time you email that address or in the meetings section of the www.2600.com website.

Dear *2600*:

Hi, My name is Jackson. I am 12 years old. I have an interest in radio spectrum, software, and computer science in general. I am just getting started. My uncle works in cryptography. He suggested I meet with *2600* to meet other great people in this space. When is your next meeting?

Jackson

Our meetings take place on the first Friday of every month, starting at around 5 pm. Check www.2600.com/meetings for the closest one, as well as any variations in the starting time. Our meetings take place in publicly accessible areas with no age restrictions. We hope you find a welcoming environment as well as other people who share your interests. This is the magic of our meetings and of the community.

Dear *2600*:

I've recently moved from Odessa, Texas to Destin, Florida. There were never any meetings in my west Texas area and now that I'm looking, I don't seem to see any in this northwest Florida area either.

I'd love to get some help getting something started in Destin, Florida. What do I need to do?

DISLEX

This is a common problem. But when you consider that people who have started meetings in the past were basically in the same position as you, it becomes much less of a challenge to go ahead and start a meeting in your area. Assuming there aren't already meetings nearby (an hour's travel distance once a month is generally considered nearby) and that you're starting meetings in a place where a good number of people can easily get to them, then we see no reason why you can't just pick a place and see what happens.

Social Media Woes

Dear *2600*:

I am hoping to wean myself off of Facebook, but would like an alternative. I have played around with a lot of them, but wasn't impressed enough with them to use daily. What alternative to Facebook do you recommend?

D

We know a great one called The Front Door. Just open it and anything's possible. There are others known as Reading, Writing, and Telephone. There's also Sarcasm, which is guaranteed to help you feel better about most anything.

The other answer we can offer is that social media is no substitute for being genuinely social. There is an unhealthy dependency on being liked, popular, or visible. While there are certainly good things that come out of these outlets, there are so many bad things and many of today's major problems can be traced directly to them. False news items, rewriting of history, dangerous health advice, mass hatred, bullying... the list goes on and on. And that's not even taking into account the massive privacy issues involved in broadcasting your entire life to the world.

As with any form of technology, there is good and bad contained within. It all depends on how we use it. And the human race is not using social media very well right now. So for those who want less Facebook in their lives, we suggest identifying all of the negative elements you're trying to get away from and then coming up with how you would prefer such a service to work. But if that proves to be impossible, perhaps we're all better off without these services, or at least not being as dependent on them as we are now.

Dear *2600*:

Please excuse using this email address for complaints, but I am or might be banned by now on the Facebook group for *2600*. A guy posted on there asking for email lists. It sounded dodgy, so I said "yeah i got email list contact in private message" so then I could question and confirm his intentions that it was not going to be used for spamming. He would not have publicly admitted this on the group. I have an email list part of database dumps that are publicly available online. I said to the admin that he can't go round making baseless accusations and suggested for him to find out first. Imagine what would happen if police started arresting people cos they seemed like a criminal. I personally never assume anything. He should have checked with the guy first and based his decision on facts. He then started to accuse me of spamming. As I said, I had an email list - another assumption. All this time, I am trying to explain that you can't go making baseless accusations just cos it seems like it based on no facts. People where I live are spreading lies about me, so I know all too well with dealing with the police on the issue what damage a baseless accusation could cause to him. Sounds dodgy what he asked for, granted, but until you know you shouldn't act. He may have very well had a valid reason why he wanted them and, without asking, you just don't know. He then started to threaten me, including a link to my local police station as if to accuse me of breaking laws - which I do not. He does seem to understand that judging a book by its cover is bad. I am an example of this, due to lies spread about me being a bloody pedo cos i disciplined a drug dealer's child for bullying. All went to court and he was found guilty, not me. But when the accusation has been made publicly, that can still cause issues if someone is innocent. He just cannot go around assuming things just because it looks a certain way. This has caused me three years of hell. He's probably banned me out of spite. I have not been back on Facebook yet to see.

i am white hat - he knows that as he checked my profile and posted links on it to me.

He needs to be told. How would he like it if people started calling him a rapist in the street due to a baseless accusation. He said he doesn't care what people think. Well, he would when he got beaten up for someone else's lies.

Please look into this. I'd be surprised if he didn't ban me out of spite. He needs to learn to get along and not accuse somebody of anything without facts, which is why i wanted to ask his intentions in a private message where he is most likely to get loose lipped and I can check.

Please look into this guy. Don't know why he is admin if he goes round assuming things.

Steve

Whenever anyone asks why we don't spend more time in the social media world, we point to letters like this one. We have no idea what the issue actually is, at least partially due to the pronoun issues which makes this read like a confusing movie (is the admin the same "he" as the person who posted?), but mostly due to an overwhelming and passionate desire to not care one bit about these sorts of interactions.

We don't dislike Facebook or other social media, but we don't have the time, energy, or addictions required to devote a whole lot of time to these issues. Our admins have a tough job dealing with managing things as it is. We expect people to not make their jobs any harder, but if they are truly misbehaving, let us know in a non-rambling way and, if at all possible, without supplying more evidence to make it look like you're in a non-ending war against the rest of the world.

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

Filter Bots Stifle Your Speech

Filters are common on online platforms. But anyone who's been put in "Facebook jail" or had their Twitter account dinged knows that these automated filters can't easily determine whether a post actually breaks community standards; they can't check for irony or humor, they miss context clues, and they simply aren't cut out to understand the nuance of written language. What's more, revelations from the "Facebook Files" have shown that at least that platform has a special program, dubbed "cross-check," which gives some "VIP" users a near-blanket ability to ignore the community standards entirely.

Unfortunately, filters are having a bit of a moment in Washington DC. Though not explicitly calling for filters, the "Kids Online Safety Act" would require platforms to limit certain types of legitimate speech - like conversations around substance abuse - from being shown to people below a certain age. Companies that can afford to - the big players - will no doubt use their filters to comply, and either ensure that users who are affected by the law see little to no discussion of the topics that are verboten. The types of content targeted by these bills are complex, and sometimes dangerous - in addition to substance abuse, the law lists discussions of suicide and eating disorders - but discussing them is not bad by default. It's very hard to differentiate between minors having discussions about these topics in a way that encourages them, as opposed to a way that discourages them. What's perhaps worse is that the bill vaguely lists "other matters that pose a risk to physical and mental health of a minor" as content that should be limited. As we've seen in the past, whenever the legality of material is up for interpretation, it is far more likely to be banned outright via oversensitive filters, leaving huge holes in what information is accessible online.

Likewise, Congress is considering a filter mandate bill that would task the Copyright Office with designating technical measures that Internet services must use to address copyright infringement. Right now, sites like YouTube, Facebook, and Twitch use filter tools voluntarily, to terrible effect, but they are not doing so under any legal requirement. But corporate copyright owners complain that filters should be adopted far more broadly. They point to one of the conditions of the legal safe harbors from copyright liability included in the Digital Millennium Copyright Act - safe harbors that are essential to the survival of all kinds of intermediaries and platforms, from a knitting website to your ISP. To benefit from safe harbors, sites must accommodate any "standard technical measures" for policing online infringement - essentially, they have to implement an agreed upon mechanism for removing copyrighted material.

These measures were meant to be "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process."

As a practical matter, no such broad consensus has ever emerged, partly because the number and variety of both service providers and copyright owners has exploded since 1998, and these industries and owners have wildly varying structures, technologies, and interests. What has emerged instead are what you see today: privately developed and deployed automated filters like YouTube's ContentID, usually deployed at the platform level. For decades, influential copyright owners have wanted to see those technologies become a legal requirement for all levels - and the "Strengthening Measures to Advance Rights Technologies Copyright Act" is the latest in a string of bad proposals that would do so. The law would require service providers to adopt "designated technical measures" to police potentially infringing activity - i.e., in many cases, filters - approved by the Copyright Office - despite the fact that these filters aren't able to distinguish between lawful expression and copyright infringement, and that they regularly punish both people who make their living sharing videos online and everyday users.

There are tens of thousands of examples of these oversensitive and inaccurate automated takedowns. Some highlights, which we've memorialized in our Takedown Hall of Shame, include YouTube's system flagging *static* as copyrighted material *five separate times*. Another ironic example: the company flagged video from a New York University Law School panel where *the point* was to explain how song similarity is analyzed in copyright cases. The flag was eventually removed, but only after NYU Law reached out to YouTube through private channels, attempting to get an answer to its questions about how YouTube's filter system, Content ID, and takedown policy worked.

The problem isn't just on YouTube: Facebook heeded a takedown request from Sony and muted a musician's own video performance of Bach, because the platform's filters can't tell the difference between different classical musicians playing public domain pieces. The company only backed down when the musician took his story to Twitter and then emailed the heads of Sony Classical and Sony's public relations.

The problem isn't just copyright filters, of course: in an attempt to battle COVID-19 misinformation, Facebook also kicked the page for Oakland-based punk rock band Adrenochrome offline. (Adrenochrome is a word popularized by Hunter S. Thompson in two books from the 1970s, but which gained recent popularity amongst conspiracy theorists.) The site renewed, then removed the page again, and only restored it after we reached out to them.

Twitch has also had its filter failings: when the live streaming site hosted Blizzard Entertainment's gaming conference BlizzCon on its official gaming channel, it replaced a live performance of Metallica with something resembling the music from an ice cream truck - all while leaving the music intact on Blizzard's own Twitch stream. Given that Metallica put themselves on the frontlines of the fight against digital music downloads in the early 2000s, launching high-profile lawsuits and testifying in front of Congress, it's no surprise Twitch was so twitchy.

So if filters can't tell if one thing is just a copy of another thing, how can they tell if something is definitively hate speech, or a promotion of substance abuse (for example)? What we've learned from the long, painful history of automated copyright filters is that *filters don't work*. And mandates for filters don't just stifle speech, they also have downstream effects on the potential for new providers and platforms to challenge the big incumbents. If a filter mandate were made law, the largest tech companies will find it easy to implement whatever the standard technical measures are (likely using something akin to their current measures, but turning the "filter" knob up to 11). The burden of laws like this falls mainly on users, and small and medium-sized services.

Faced with these criticisms, government officials and politicians ought to back away from these ham-fisted plans to regulate online content through mandated technical measures. But it will take people like you to convince them. We hope you'll join us at the Electronic Frontier Foundation in fighting back against the filter mandates - before the Internet gets remade to serve the whims of today's politicians and the entertainment industry.

The Phreak's Field Guide to Identifying North American Phone Switches, Part Two

by ThoughtPhreaker

DCO

The red-headed stepchild of the switching world; there's really no other way to put it. Siemens bought it, discontinued it in the early 90s as an end office (it survived a little longer in production as a long distance switch), and gave the EWSD the capability to interface with DCO line frames and remotes. Genband bought the DCO and EWSD designs, and made their softswitches do the same thing!

- To this day, the maintenance processor for every DCO in the network is a DEC LSI-11, as were the original call processors for the system. As a result, Siemens kept an original PDP-11/70 in service for software development until 2000 before replacing it with a Mentec clone. At some point, newer call processors (as in, the ones you get when you pick up your phone rather than hit a key on the switch's serial consoles) were ported to a more recent hardware architecture. Given the lifespan of telecom gear, it's likely that in some parts of the U.S., you can pick up your phone and still get a PDP-11 at the other end.
- Won't support GR-303 loop carrier without a third party add-on.
- Early incarnations supported the strange coin detect feature the ESC used without pulling line current. For whatever reason, this was dropped later in its life.
- Commonly (almost exclusively) does AIS-style announcements.
- There's two different models of DCO: CS (toll tandem) and SE (Small Exchange). Both are relatively low capacity switches, so for that reason, you'll most likely find the DCO-SE when you're wandering around the very rural parts of ex-Contel/GTE territory. As for the CS, a lot of small long distance carriers bought these in the 90s. If you can dig up some small toll providers, they might still be using them.
- DCOs have a stutter dial tone with six bursts of dial tone instead of three.
- Has a tone used for confirmation, partyline ringback, etc. consisting of short, 100 millisecond pulses of high tone. No other switch type seems to use this.
- When pulsing your first rotary digit, there's no burst of dial tone when you're done.
- Completely ignores fourth column (A, B, C, D) tones.
- Much like when dialing with the switch's predecessor - the ESC - dialing * in certain places lends itself to odd circumstances. As the final digit as a CAC+0 call (as in, say, 101-0288-0-212-555-121* - it's important that it be the last digit), it appears to put the call through! What it's sending isn't entirely clear. In SS7, a destination phone number is sent using binary-coded decimal, as opposed to plain ASCII in ISDN-derived protocols, so the only possible combinations to send are 0 through 9 and A through F. With a * as the final digit of a local call, strange recordings will occasionally play, such as permanent signal (if you'd like to make a call, etc.).
- Like the GTD-5, its processing of the # key isn't entirely clear. For example, 101-0288-0# won't tell a DCO to stop waiting for digits and to put the call through. Instead, it generally seems to keep waiting for digits, as if considering it part of the destination. Unfortunately, this makes CAC + # (as in, just the carrier access code; no called party number) impossible to call, severely limiting some fun things that can be done with long distance tandems.
- Flash behavior on coin (and possibly home) phones isn't entirely clear either. For example, on a CO-controlled coin line, flashing after the switch releases a call will make it send coin return voltage, but only keep someone on silence.
- Really hard to find! Playing with a DCO up close is a rewarding experience for anyone keen on introducing unorthodox input into the phone network. Considering many of them only serve far-flung rural areas, this requires planning, the willingness to drive a considerable distance, and the ability to find a payphone once you get there. Street View is your friend, kids....

Ringing number: 337-666-9009 (CNAM returns CENTURYLINK; likely unused pair in the central office)

Remote call forwarding prompt: 218-834-9934 (ETC Digicept providing voice samples)

Unknown dialtone: 815-537-0006 (beware that this doesn't supe. Being able to transmit over the toll network before supe is a whole other topic, but a carrier like MCI/0222 (read: not Worldcom/0555) is ideal for this. What it's looking for isn't entirely clear, though; the switch will wait for a seemingly infinite amount of digits before inevitably throwing you to an error recording. At the recording (and this isn't a hardware fault, they all seem to do this), the switch will arbitrarily hang up and call the recording back - or sometimes just throw you off the call entirely. Given how long it waits for so many digits (this would really make more sense

with a passcode rather than a destination), it's possible this is another way the switch has of handling call forwarding.

EWSD

Outside the U.S., the EWSD, Siemens' pride and joy, is everywhere - from Argentina to Iran. Inside the U.S.? It just comes up here and there. What it's like depends pretty heavily on who runs it, though. AT&T has trouble understanding *how* to run it, and it's occasionally poked at by their techs for that reason. In any case, their dialplans aren't exactly bulletproof. Verizon tends to be a little better about dialplans (some of them even have custom prompts on their Cognitronics machines!), but they have their own weirdness; in this case, a CAC - 0110. Instead of sending you to a long distance carrier, it originates whatever you put next locally.

- In a strange gesture of switch apathy, AT&T's EWSDs do pretty much no checking of your destination numbers. As a result, you can route calls to almost anything of your choosing like 0xx codes, and it'll put it right through! No weird routings, no CACs needed, no workarounds. Let it be known that nothing good ever came from talking shit about your phone switches.
- The 0110 CAC seems to be a thing on all North American EWSDs, even the independent ones. Curiously, on most other switch types, the ability for someone to take advantage of this is hit and miss at best.
- The EWSD stands as one of the only switches (the DMS-100 being the other) to have two different types of ringback tones. As far as I can tell, this has to do with the generation of hardware. Paul Timmins, the guy who runs Telcodata, was nice enough to post the install dates for most of the Ameritech EWSDs in Michigan. On that list, one clear pattern starts to come up: all the Type 1s were installed sometime before 1995, with the first Type 2 showing up in 1993. Unlike some of the more common switches, the EWSD never really became popular until the mid 90s, so the vast majority, partly thanks to DCO conversions and CLECs, are Type 2s. Type 1s only seem to occasionally show up in RBOC exchanges near the Midwest and eastern parts of the U.S.
- While EWSDs seem perfectly capable of generating milliwatts (they can all do more complex 105-type tests), almost none of them do. Instead, they have a test set that sits on an analog line, and answers with a 102-type milliwatt. In between the silence, if you send it touchtones, you'll get all sorts of weird tones.
- When getting an error recording, the default behavior is to let an announcement play once, and quickly hang up.
- The digit "D", typically rejected by most switches in one way or another, will translate to 0 on an EWSD.
- Like the DMS, some EWSDs have been noted to make soft clicking noises as calls progress. In this case, they tend to be less subtle than the DMS's. While nobody seems to know for sure what causes this, I have a pretty strong suspicion it's caused by how the EWSD handles lines on loop carrier systems.
- Our resident EWSD resident, JmanA9, was kind enough to get some information on the EWSD's test functions. The ringback circuit, surprisingly, is an actual, physical test device that physically removes you from the line card, and takes over the function of running your phone line. This function is used very rarely, but is especially unusual on a switch that's preferred for all-ISDN networks, like some in Europe.

(Type 1) Ringback tone: 203-453-0994
(Type 2) EWSD Milliwatt: 541-384-0100
Ringback tone: 608-663-0126
Reorder tone: 608-663-0130
Remote call forwarding prompt: 888-345-8672, pick any switch from the IVR.

AXE-10

Like the metric system or a sensibly-sized pickup truck, what's common to the rest of the world is somewhat uncommon to the United States. The AXE-10 is no exception. While it holds the title of being the world's most popular phone switch, it's little more than a footnote in the North American network, with many being replaced by their more popular counterparts as quickly as the early 90s. In former US West and Southwestern Bell regions however, a moderate but persistent crop of AXE-10s stands firmly in place.

A certain Greek AXE-10 running part of Vodafone's network holds a particularly unique place in telephone folklore, having been host to a rootkit written in PLEX, the switch's proprietary programming language, that concealed the wiretapping of the Greek prime minister and several other officials. Wikipedia's write-up of the story gives an air of mystery to the incident, as well as the cringeworthy opsec failure that led to a suspect being identified in the case.

- Quite a few of the ones in the U.S. are near the Mexican border. This may be because Mexico uses so much Ericsson gear; AT&T will occasionally call on Mexican switch techs to help them fix stuff.
- Unlike other manufacturers, Ericsson appears to have stuck to developing in-house CPUs until a relatively late date, with off-the-shelf components being introduced into APZ (main CPU) designs towards the late 90s.
- Like the DMS-100, it seems to be married to an announcement machine. As far as most non-softswitch designs are concerned though, they stick out like a sore thumb. Unlike a lot of the non-AIS announcements, they never, ever ring, and they're always very clean sounding. Ericsson

made it fairly easy to let you directly upload recordings.
- Impatient! Only has a five second waiting time for partial dial conditions.
- Reorder timing is slightly faster than most American switches, but not as fast as a DEX-450/600, one of the toll switches occasionally found in the ex-MCI (0222; the non-Worldcom one) network.
- When dialing, the fourth column DTMF digits A, B, and C mostly seem to react as if you dialed a *, depending on where it's inserted. D, however, is another story.
- Can drop you to an announcement *fast*. In the fraction of a second that most switches can bring you to reorder, the AXE-10 can start up a recording.
- Typically is filled with a bunch of strange tones in its test ranges, like out of spec milliwatts (next to real ones, no less) and seemingly arbitrary 815 hertz tones.
- AT&T AXE-10s allow NPA-0xx-xxxx.
Ringback tone: 970-887-0051
Busy tone: 405-382-9154
Announcement: 405-382-9137
Weird tone: 325-235-0500
Off frequency milliwatt?: 325-235-0514

CS-1500/C15

What do you get when you put a DMS-10 CPU in a 2U rackmount box and slap some ethernet interfaces on it? A CS-1500! Not much more to say really.
- Like the GTD-5 and the EWSD, this switch is married to an AIS; pretty much all installs come with an Innovative Systems APMax. The increasing number of APMaxes being paired with DMS-10s has made an already tough exercise of telling the two apart even harder.
- Telling a DMS-10 and a CS-1500/C15 apart can be really hard; they use very similar software, CPUs, and even the same line frames. As far as I know, the only way to tell them apart is to try finding a 105 type test, or possibly a loop; independents, where you'll most likely run into this scenario, will likely put a 105-type test in a place like 9105 or 1105. 9108/9109+1108/1109 is a good place for loops.
- The stutter dial tone you get on a CS-1500 when dialing *67, *82, etc. will be normal speed; the DMS-10's is noticeably slower than the speed most switches play it at.
- Does not have the offhook tone with the weird modulation sound in it like the DMS-10's.
- Cannot support dialpulse trunks, among a few other trunking arrangements the DMS-10 does.
Remote call forwarding prompt: 828-297-9999
Reorder tone: 906-524-9966

CS-2000/C20

The CS-2000, as Nortel's internal hardware guide puts it, isn't a new product, but effectively a new hardware revision for the DMS-100. The software was ported from SOS (Switch Operating System; Nortel's proprietary RTOS) to Linux, and a virtual machine layer took the place of some of the hardware. The CS-2000 also runs on PowerPC 750 and 7410 CPUs, much like the newest DMSes. The C20 is a redesign of this hardware by Genband to fit into an ATCA blade chassis, along with a completely different source of call progress tones.
- In ATM mode, this switch is quite literally indistinguishable sounding from a DMS-100. Supports many of the line frames and peripherals of the switch as well. Despite being ATM, internal signaling channels will still be done via IPoATM cells.
- In IP mode, the CS-2000 uses the same tone set as the DMS-100 in three-way mode. While it still supports DMS-100 hardware, some installations will do weird things, like fade out as it disconnects, as if there was some sort of packet loss concealment. Other installations have a subtle, but still noticeable level of latency.
Remote call forwarding prompt: 610-799-9900 (this isn't the best reference; the exchange itself is a DMS-100, the CS-2000 seems to be for an affiliated cable company)
Non-working number recording: 620-371-6111 (uses DMS-100 EDRAM circuit pack, stock announcement)
Non-working number recording: 702-722-6222 (uses CS exclusive Audio Server, stock announcement. Note that very new Genband C20s may use a different announcement, as evidenced by the very last of the AT&T 1AESS to C20 cutovers in 2016/2017)

Safari C3

This switch pops up occasionally in small patches. Some west coast Comcast, some Charter, some Atlantic Broadband. The switch is optimized for voice over PacketCable networks, and can be identified by a fairly distinct ring, and its breathy voiced stock announcements.
- This was very hastily thrown together by Cedar Point, a headend equipment manufacturing company, before eventually being acquired by Ribbon/Genband. This will occasionally result in weird feature limitations. For example, it'll support ISDN PRIs natively, but only NI-2 flavor PRIs. Or, as its manual cautions, if you insert a high density media gateway card into the last slot on the chassis, the switch will overheat.
- As of 2021, while Ribbon appears to fully back the product, it's unclear who continues to run these. Changes in LERG, audible ringback, recordings, and other factors appear to suggest major cable companies are phasing these out. This would be consistent with the relatively short lifespan (less than 20 years, whereas some DMSes have continually run since the 70s, albeit with severely evolved/upgraded hardware) softswitches seem to encounter. A cursory search

for some press releases suggests South American cable operators might still be using them. A search on Shodan revealed one on the public Internet operated by TV Rey (as in, TV King. I can't say it with a straight face either), a Mexican cable operator.

When I first started writing this, this is where I put numbers for the C3. Today, any secrets these awkward boxes of overheating breathy voices held were taken to the grave along with the example numbers I wanted to give out.

Taqua T7000/OCX

One of the many designs from the telecom boom (and bust) of the early 2000s. The switch was initially embraced by small companies, but seems to have fallen flat on its face, like a lot of other switches introduced at the time. What differentiates it from products like the Coppercom CSX and Gluon CLX is it survived, still retaining an audience within Sonus/Ribbon's halls.

ANAC: 229-236-0102

Remote call forwarding prompt: 760-928-5900

Remote call forwarding prompt: 806-350-0099 (alternate prompt set)

- The call forwarding prompt sounds very close to the DMS-10 and CS-1500 call forward dial tone, but listen closely to the way it comes on. There's two bursts of stutter dial tone, a (relatively) long pause, and another of those two bursts. There's also a few other differences, like stock recordings and its reaction to keys like *.
- Stock recordings sound weird and fucked up for some reason. Some iterations of this switch seem to have a completely different prompt set.
- Incorporates a SPARC machine running Solaris, though its role isn't entirely clear.
- Really hard to distinguish T7000 and 5ESS ring.
- Architecturally, all cards on the T7000 (or OCX; same thing) are designed to be functionally independent of each other - the resources needed for billing, features, switching, etc., are all self-contained.
- Typically run in small patches by Paetec/US LEC, Allstream/Electric Lightwave CLEC properties (the former apparently only for IP traffic; they appear to be run alongside 5ESSes), but relatively rare overall, with a handful already being replaced by the early 2020s. Getting a chance to fondle T7000 dial tone has been anything but easy.

MDX384/IGX/HDX/SLICE

Built to be very modular, and because of their unusual design, wind up in very strange places. Their very low capacity (IGX supports 96 lines per shelf, MDX384 supports 384 lines) is ideal for places like ghost towns, and fanless operation makes them ideal for extreme parts of Alaska and the Yukon. They're popular as military PBXes as well, having survived a number of tours in Iraq. The SLICE, seemingly a 1U version of the IGX/HDX - or at least running the same software, has gotten its rite of passage into the U.S. military. In some places where HDXes have historically been used, they've been swapped out with SLICEs for portability reasons. Some FTTH deployments in the middle of nowhere are done with SLICE hardware too.

- Despite their age and different generations of CPU cards (the IGX is believed to run on a 68k), the IGX, SLICE, MDX, and HDX appear to be all be running ports of remarkably similar software.
- Card stock between the HDX, IGX, and MDX are interchangeable.
- Each shelf in an HDX switch can have a maximum of 512 timeslots assigned to it, with additional shelves being connected together with a ribbon cable to allocate up to 4096 channels on the system's TDM bus to up to 32 shelves. This limitation is suspiciously similar to the H.100 bus used in hardware-accelerated telephony cards for computers, with its maximum of 4096 timeslots, 32 independent serial data streams, and its big, IDE-like ribbon cable used to link cards together.
- The HDX has been described as both a softswitch and circuit switch before. Redcom's marketing tards need to make up their damn minds. Both generations work on circuit packs, the 90s generation of which look like they're using a few *very* old designs with hand-woven PCBs. It appears the presence of a TRANSip (media gateway) card is what qualifies it as a, uh, "soft" switch, an increasingly hilarious misnomer that switch manufacturers seem intent on abusing. By definition, a softswitch, such as Asterisk or CallManager, runs on off the shelf hardware. Nothing here, carrying a "next-generation" moniker for over 20 years or otherwise, meets this definition in the slightest.
- Has a BASIC interpreter on it! No, seriously.
- One of the few switches in the world to still support magneto phones.
- The integrated AIS sounds like the voiceover person had a stroke. This is apparently a design choice associated more with newer Redcom systems, though not absolute. While an IGX can still sound like it lost all feeling in its throat, it's far more common to use a scratchy sounding announcement card, more often than not with the voice of the switch tech in some far flung place with an equally scratchy carbon mic.

Supervision test: 831-389-9103

AIS report: 831-389-9108

Loop: 907-293-1108/1109

Announcement via older IGX hardware: 907-293-9990

GTD-5

What do you get when an obscure phone company designs obscure hardware? The GTD-

5 EAX! That's a "General Telephone Digital #5 Electronic Automatic Exchange" for those of you who actually pay attention to acronyms. There's a certain saying in telecom: "one is good, two is great." Just to show they really were a phone company, GTE duplicated *everything* in the processor complex not just once, but twice. A single card has two processors running the exact same instructions and comparing them, while an identical card does the exact same thing. All the digital trunk cards on the system are likewise duplicated. Internally, the system communicates using 12-bit PCM words over a parallel bus, and runs on software written in a custom version of Pascal. Like some of the other designs such as the EWSD, the system has no announcement cards, and leans entirely on external equipment to generate any recordings. For that reason, most of these were sold with units from the Cognitronics company to make this happen.

Random facts:

- Around 2000, Lucent completely redesigned the GTD-5 switching network. Little is known about it other than, well, it exists and it's different.
- Like any good obscure switch, the GTD-5 will almost always let you dial 0xx codes. You don't need to put a CAC in front, unlike on a DMS-100, but probably won't be able to dial nine digit numbers. The tradeoff is the alternate dialplan for vertical service codes such as *67 on GTD-5s *will* generally block 0xx.
- The GTD-5 is more or less married to an AIS to provide any recordings in most configurations. Typically, these are run of the mill Cognitronics machines, but occasionally will be an ETC Digicept, a really old Cognitronics machine, or in some really recent cases, an Innovative Systems AP or APMax. However, some very old GTD-5s have actual, drum-style announcements. Mount Olive (217-999) is one of two I've ever heard equipped this way, and is living proof that the hardware even allows this.
- Some switches, most notably the GTD-5 in Logan, Iowa (712-644), seem to have strange, newer retrofits used to generate recordings with text to speech. This is incredibly rare, but might be a sign of things to come if more of the older Cognitronics boxes fail.
- Sometimes this switch will have a noticeable pause between certain tones, like offhook or stutter dial tone, even during off-peak times like four in the morning. It's unclear what causes this, but it might imply tone cadences are generated by non-dedicated hardware.
- Has a strange way of handling permanent signal (not dialing anything at the dial tone) conditions. Some have the announcement machine play something, some just give reorder, others a solid high (480) or low (480+620) tone, or even just silence. Sometimes you'll get a combination of all four. Always stay on after the reorder to be sure.
- According to Chuck, a seasoned GTD-5 tech, it may be possible to gain some insight into what software version a GTD-5 is running by the way it handles someone leaving their phone off the hook. It can be any combination of reorder, high tone, low tone, offhook tone, or all of the above. Supposedly though, there is no way to change what combination of these it uses in software. The most common way of doing things currently is to use all four (reorder, low tone, high tone, offhook tone).
- Outgoing voicemail system trunks, some of the most locked down outgoing trunks you'll find, tend to get ANAC, directory assistance, and other things most switches never, ever allow. This switch is *not* good at toll restricting! Some GTD-5s have adopted the peculiar behavior of sending offhook tone down voicemail trunks when presented with an SS7 message indicating all circuits are busy.
- The behavior of the # key as the first digit of a phone number is unclear. Where most switches assume you're using a speed calling code, the GTD-5 seems to wait for an unusually long string of digits, so long as the first or second digit isn't 1 in most cases. Notable exceptions to this are 0, 2, 3, 6, and 8; with 1 as the second digit, they'll keep listening.
- One of the few large CO switches to be designed (at least originally) for fanless operation. Newer hardware doesn't necessarily follow this trend.

Unknown older hardware generating offhook tone for a GTD-5: 712-374-1256

Feature recording via weird TTS thing: 712-644-1275

Remote call forwarding prompt via ETC Digicept: 906-341-9983

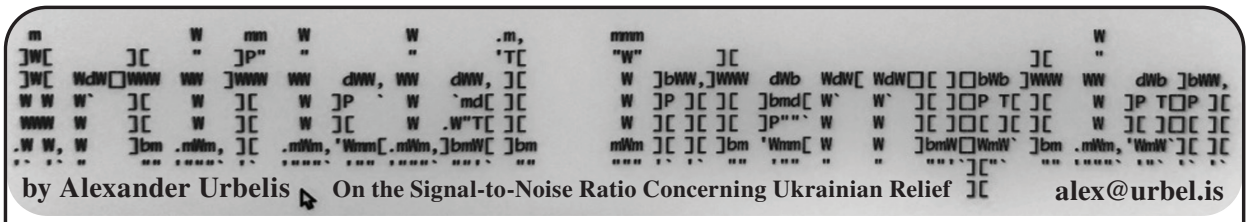
Remote dial tone: 231-773-9996 (for unknown purpose; doesn't look for a destination phone number)

Softswitches I Know Nothing About

Metaswitch [early/mid 2000s ATM + IP core Compact PCI softswitch: popular with the rural telcos who change their switch as often as their underwear. Later systems use an ATCA chassis rather than cPCI. Very common within larger LECs as a voicemail system or for IP trunking]: 406-347-4800 (voicemail), 503-266-1021 (ANAC)

Coppercom CSX [early 2000s softswitch design. Few survive now]: 517-436-9000 (ANAC)

Special thanks to: Scott from the Socal bridge, Scott from the not Socal bridge, the people who wrote the Wikipedia switch articles, dmine45 (maintainer of telephoneworld.org), Evan Doorbell, Paul Timmins, JmanA9, Jim Somerville's LinkedIn profile, Shadytel for keeping it as real as it gets, trmg. You guys seriously know your stuff! This article would've been a lot less interesting without your bits of wisdom to stick in here.



by Alexander Urbelis On the Signal-to-Noise Ratio Concerning Ukrainian Relief alex@urbel.is

This column left off discussing a humanitarian disaster that was ongoing in Myanmar and the need for empathy among strangers. Since then, Russia has invaded Ukraine, there is a full-blown war on European soil, and the world's nations, including finally the United States, have accused Russia of perpetrating war crimes.

The world has become familiar with the heartbreaking images of fathers pressing their hands to the windows of trains as a final valediction before their families, now refugees, are carried away and they must return to the frontlines to fight the Russians. We have all the seen the horror of a mother and her two children killed in plain daylight while crossing the street, we've seen images in the aftermath of a woman nine months pregnant injured by a bomb before her death and the death of her unborn child, and there are untold and unspeakable horrors happening to the people of Ukraine on a daily basis as Russia continues its siege and its indiscriminate and persistent bombing of civilian targets and areas.

As of the writing of this column, despite the supposed sophistication of Russian operators, the war has hitherto had very little to do with cyber operations. Though Conti, a ransomware gang known for both its excellent customer service and connections to the Russian government, vowed to support the Russian incursion by breaching and encrypting the data of Russia's detractors, this notorious bunch of threat actors quickly walked back that threat less than 24 hours after its utterance. Before they could, however, a Ukrainian security researcher released for public consumption nearly 100GB of Conti chat logs, training materials, and other internal documents.

On *Off The Hook* in March, we had the pleasure of hosting Emma Best of Distributed Denial of Secrets. DDoSecrets has published close to a terabyte of leaked Russian materials, from official documents of the Russian censorship agency (the Roskomnadzor) to troves of documents that relate to oligarchs' oil interests and Russian state-affiliated companies such as Transneft and MashOil. Also on *Off The Hook* as a guest was Karina Shedrofsky, head of research at the Organized Crime and Corruption Reporting Project. Karina and her colleagues have been tracking the assets of Russian oligarchs for years, and put together an interactive Russian asset tracker that sheds great light on the hidden assets of Russian oligarchs and the jurisdictions that provide them haven.

A concerning trend, however, is for the target of hacktivism or leaks to claim that the hacktivist groups responsible for the attacks are actually operating at the behest of a hostile foreign nation. Branding hacktivists in this manner is not simply misinformation or deflection - it could signal that those responsible for the actions are being classified as enemy combatants. When dealing with a country like Russia which has had no qualms on multiple occasions with targeting enemies of its state for poisoning and assassination, that is a scary classification for anyone to carry.

Indeed, from saber-rattling with nuclear weapons to clamping down on news media and protesters, Russia has been trying exceedingly hard to discourage individual or collective opposition to its illegal war and to prevent actively supporting Ukrainian relief efforts.

Around the globe, we are all wondering how we can support Ukraine, and our inability to do so has left us wanting. With this in mind, I have observed a curious trend in the Domain Name System (DNS) since the outset of the war. Right around the time that the hostilities commenced, I began to monitor and track domain names that contain the string, "ukrain*." That word stem would capture "Ukraine' as well as "Ukrainian" and other variations. Since the beginning of the war, I have identified thousands of new domains, with daily registrations peaking at around 500 at the outset of the invasion and then tapering off to about 125 new domains appearing every day in April 2022. Nearly immediately, however, I noticed a very significant spike in domain names about donating to Ukraine.

By way of our steady, old friend grep, it was easy to identify domains that pertained to donations, aid, relief, NFTs, and, of course, cryptocurrency. As of writing this column, there were nearly 800 new domains that incorporated strings relating to aid and relief together with the string "ukrain."

This is very much the type of gray area in which Russian operations thrive. Indeed, an often overlooked yet critical piece of understanding Russian politics is the role that Vladislav Surkov plays in advising Putin. Surkov was and is a manipulator who came from the world of the theater before rising to political power, holding the position of deputy chief of the Russian Presidential Administration from 1999 to 2011. Turning Russian politics into a shapeshifting mess of coalitions and ever-changing alliances and conflicts - and then letting it be publicly known that Surkov himself had artificially generated these coalitions and conflicts - was the Kremlin's tactic of keeping the masses confused, distrustful, and always questioning what was real and what was artificial.

Not surprisingly, on the heels of the invasion, there has also been an uptick in reports of donation fraud concerning Ukraine. Though many of these scams may originate on social media or via text message, much of the fraudulent activity will

eventually rely on a domain name to host content, harvest credentials, siphon credit card details, or otherwise act as some form of pass-through for data or communications.

From the perspective of Russia, these domains and the fraud associated can be beneficial to their war efforts on several levels.

On one level, decreasing the signal to noise ratio (or increasing the noise to signal ratio) serves Russia because this type of fraud, and the media attention that it generates, will cause ordinary persons to have misgivings about donating to Ukrainian causes or relief efforts out of fear of being defrauded. From a policy perspective, given so much may be riding on the Ukrainians' ability to withstand sieges and sustained shelling and urban onslaughts - which would require aid and relief to withstand - it is not inconceivable that Russia could be encouraging this type of behavior under the table or turning a blind eye to criminals who engage in such fraudulent activity.

On a deeper and more sinister level, if Russian actors were behind the fraud themselves, they would be accomplishing the goal of deterring others from donating resources to Ukraine while also absconding with the funds and resources that well-meaning persons from around the world intended for Ukrainian relief.

And on yet another - albeit less - sinister level, there are many domains that track to Russia, either by registrar, registrant, NS records, or IP addresses. And if these domains relate to ordinary Russians, as some of the Whois data indicates, and those domains are not fraudulent, then given the authoritarian crackdown on dissent - or even contrary dialogue to the Kremlin's official position on the invasion - then those domains and the persons behind them should be lauded as heroic.

But then again, going back to Surkhov's playbook, how do we know what is real and what is fake, what is charity and what is fraud, what is a legitimate humanitarian effort and what is a dangerous honeypot of a brutal regime? It is one thing to talk about the dissonance and difficulty of ascertaining fact and fiction and another thing entirely to see it. For that reason, I am dedicating some space in this column to listing Ukraine-focused domains with Russian connections. And while I encourage readers to exercise caution and discretion if they intend to visit any of these domains, I am also very curious about what information from and connections between these domains can be derived.

To that end, I encourage readers to reach out to me directly via Twitter (`@aurbelis`) if they would like to receive the full list of all newly registered and aid-focused Ukraine-related domains, and I wish you all, in the meantime, happy hunting.

Domain	Name Server	IP Address
Aboutukraine.info	ns1.beget.pro	87.236.16.73
Aidforukraine.site	ns2.reg.ru	194.58.112.174
Aid-ukraine.info	ns2.webhost1.com	91.236.136.57
Airdpukraine.shop	ns1.reg.ru	31.31.196.22
Cats-dogs-ukraine.com	ns2.fozzy.com	88.212.244.12
Charityforukraine.org	ns14.domaincontrol.com	178.248.234.146
Chernobylukraine.com	ns05.domaincontrol.com	178.132.201.54
Diplomukraina.org	ns1.eurobyte.ru	46.30.41.23
Donate-to-ukraine.world	ns4.nic.ru	195.24.68.29
Donate-ukrain.com	ns1.mchost.ru	185.105.110.4
Donateukraine.charity	curitiba.porkbun.com	78.40.217.96
Donateukrainenow.online	ns1.reg.ru	194.58.112.174
Donateukraine.online	ns1.nethouse.ru	185.84.110.85
Flowers-ukraine.com	ns2.beget.com	87.236.16.9
Forukraine.world	ns2.lighthosting.net	62.122.190.67
Freeukraine.site	ns10.uadns.com	185.165.123.36
Goodsfromukraine.com	ns45.domaincontrol.com	185.129.100.113
Handofukraine.online	----------	23.105.244.169
Helpsukraine.xyz	----------	23.105.244.169
Help-ukraina.space	blocked2.nic.ru	194.85.61.76
Help-ukraine.auction	pid2.srv53.org	94.103.188.153
Helpukraine.icu	ns1.he.net	81.28.13.179
Help-ukraine.website	ns2.reg.ru	31.31.196.4
Hosting-ukraine.com	ns.parktons.com	46.8.8.100
Iherb-ukraine.com	ns2.timeweb.ru	92.53.96.18
Ilyaukrainets.com	ns1.reg.ru	194.58.112.174
Interview-ukraine.com	ns3.nic.ru	89.104.84.244
Jewsprayforukraine.com	ns4.zomro.su	81.91.178.41
Legal-support-ukraine.com	ns25.domaincontrol.com	185.165.123.36
Lifeukraina.online	ns8.nic.ru	195.24.68.8
Market-ukraine.xyz	ns1.reg.ru	194.58.112.174
Much-ukraine.xyz	ns2.beget.pro	185.50.25.57
News24-ukraine.store	ns1.beget.com	87.236.16.13
Newukraina.com	ns2.masterhost.ru	90.156.201.101
Ngchildrenukraine.net	ns2.ukit.com	185.129.100.127
Osteology-ukraine.org	ns116.inhostedns.com	185.165.123.36
Polandviza-ukraine.com	ns2.parktons.com	46.8.8.100
Prayforukraine.space	ns2.hosting.reg.ru	31.31.196.4
Razonforukraine.com	ns1.hosting.reg.ru	31.31.198.124
Razonnforukraine.com	ns2.hosting.reg.ru	31.31.196.230
Russia-ukraine.com	ns2.beget.com	87.236.16.254
Saveukrainenow.company	ns3.nic.ru	91.189.114.21
Saveukraine.site	ns2.beget.pro	87.236.16.247
Saveukrainetoken.com	ns4.timeweb.org	92.53.96.222
Saveukrainewarefare.com	r.ns.arvancdn.com	91.218.247.43
Saving-ukraine.com	ns3.digitalocean.com	141.8.195.65
Sendflowersukraine.com	ns2.netangels.ru	185.93.109.240
Setukrainefree.com	ns1.hosting.reg.ru	37.140.192.220
Slavaukraine.fun	ns1.justhost.ru	185.22.155.64
Slavaukrainegeroyamslava.xyz	ns2.hosting.reg.ru	37.140.192.82
Slava-ukraini.site	ns1.beget.com	5.101.152.161
Smile-solutions-ukraine.agency	dns1.registrar-servers.com	185.129.100.113
Ukraine-save.com	ns2.hosting.reg.ru	31.31.196.42
Ukrainewarvideo.com	ns2.beget.pro	87.236.16.75
Ukraineweek.com	ns2.reg.ru	194.58.112.174
Ukraingood.com	ns1.reg.ru	95.191.131.143
Ukrainian-analyst.com	ns3.timeweb.org	92.53.96.12
Ukrainianparty.com	ns2.beget.pro	87.236.16.251
Wikirusiaukrainewar.com	ns.parktons.com	46.8.8.100

Has the CIA Cloud Service Become More Secure? Negative

by Duran (Hong Kong)

Lately, the U.S. intelligence community has been gradually migrating their business to cloud services. The CIA already did cloud work with Amazon several years ago. The CIA's former chief technology officer for the chief information officer Gus Hunt also revealed in an interview four reasons for the transition to the cloud: "speed, efficiency, innovation, security." Of course, the first three reasons aren't in doubt, but the last one - security, really?

The answer is in the headline. Security is not a good reason for migrating to the cloud, at least in my perspective. Why do I say this? Hmm.... You need a pre-knowledge list here:

- James Clapper Jr.: "'Double-digit' cuts coming for intel budget" (washingtonpost.com, October 17, 2011)
- "What to Cut and How to Cut? Historical Lessons from Past Reductions in the Intelligence Community" (Capstone Project, RAND IPC, 2012)
- "Transparency Takes a Hit in CIA Budget Cuts" (sunlightfoundation.com, 2013)
- "The Details About the CIA's Deal With Amazon" (theatlantic.com, 2014)
- "Securing the Cloud" (www.jinfowar.com, April 2014)

Once you have read the above materials, follow my analysis on them.

First, in the book *Permanent Record*, Edward Snowden told us he was building some cutting edge technology for the CIA's private cloud with his contractor partner in 2011 when he was in the U.S. Please take note of the time period. It was the moment when the U.S. government made a decision to cut the intel budget. Director of National Intelligence James Clapper said that "he was going to try to 'protect people' and that he hoped to find 'one half the savings' by reducing overlap among the myriad computer systems now operated by the 16 intelligence agencies that make up the community." Clearly, the CIA had already made a plan for budget cuts, using cloud services to solve the "silos" problem - "the problem of having a billion buckets of data spread all over the world that they couldn't keep track of or access."

Second, the Bush School of Government and Public Service made a capstone report for RAND IPC. In its "Recommendations" section, it says "A decrease in manpower without corresponding reductions to the tasks assigned to the IC creates ineffectiveness, as evidenced by the Korean and 9/11 case studies." and "Policymakers should be aware of the danger of exacerbating the collection-analysis balance. Personnel reductions must be accompanied by corresponding cuts to intelligence missions. If this prioritization does not occur, the IC will be overwhelmed with data, and will lack the ability to process the data in a timely and actionable manner." and "When policymakers cut personnel, they should be wary of the assumption that analysts are completely fungible. Technical and regional expertise is highly valuable, and assuming an expert in one field can move to another field and perform effectively is unrealistic." Overall, we can see this report does not advocate personnel reduction, so the IC have to turn to seek efficiency from science and technology. This represents "speed, efficiency, innovation."

Third, the more secure cloud is *not* real. Why is that? Everybody knows the safest way to store something is to lock it in a vault, whether it's gold or information. We usually make a paper copy of important files in daily life; people always think that virtual things are unreliable. The ultimate object representing the wealth of a country is gold bars.

"The Amazon-built cloud will operate behind the IC's firewall, or more simply: It's a public cloud built on private premises." The saying from the article "The Details About the CIA's Deal With Amazon" from *The Atlantic* actually told us the IC data center facilities were located in a safe place, which can be verified from the paper "Securing the Cloud:" "C2S is housed in a private data center on government premises." Obviously, the agency is very concerned about the physical security of the facility. Besides, according to the description in "Securing the Cloud," it seems that the task of cloud security is left to NSA: "NSA's Information Assurance Directorate (IAD) is heavily involved in projects related to security for cloud architectures to meet the future computing needs of the Intelligence Community. NSA is leveraging this technology for optimum advantage while providing confidence in data security." and "As part of its

IAD mission, the NSA will continue to provide expertise for protection of U.S. National Security Systems whether the data is stored in traditional physical computing systems or cloud-based virtual systems." It is funny to read the word "confidence" in that sentence, it can be seen that the security of cloud services is indeed a complex and severe problem. In this article, the author enumerates various security issues, which is worth reading.

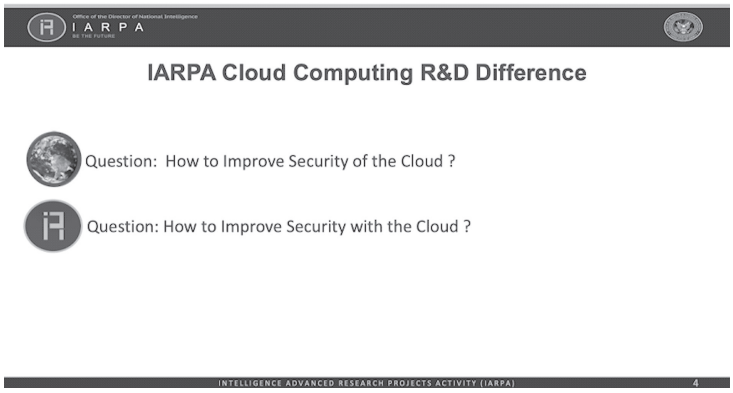
Current Incumbent	Acquisition Description	Estimated Dollar Value
AMAZON WEB SERVICES, INC.	IGF::OT::IGF The purpose of this action is to award a Task Order to Amazon Web Services under a Central Intelligence Agency IDIQ contract for Commercial Cloud Services.	$1,247,284

FY21 Budget

Contract Awardee Name	NAICS Description	PADS Orig Award Date	PADS Ultimate Completion Date	PADS Total Award Value	ITD Obligation
AMAZON WEB SERVICES LLC	Data Processing, Hosting, and Related Services	24-Jul-2015	30-Jun-2019	428,328.00	352,372.00

period budget

Additionally, Intelligence Advanced Research Projects Activity (IARPA) from DNI's Office also tries to convince the public about the cloud security problem. Its explanation mainly illustrates a question "How to Improve Security with the Cloud?" More interestingly, they proposed a concept "Defining Protection Benefits/Costs as a Function of Time" in the slides.



Slide snapshot from IARIA 2018 Cloud Computing Conference

Finally, let's look at some evidence that was obtained from the Department of Energy.

Description of Requirement	Vendor Name	Action Obligation
IGF::OT::IGF THE PURPOSE OF THIS ACTION IS TO AWARD A TASK ORDER TO AMAZON WEB SERVICES UNDER A CENTRAL INTELLIGENCE AGENCY IDIQ CONTRACT FOR COMMERCIAL CLOUD SERVICES.	AMAZON WEB SERVICES, INC.	$44,372.00

FY14 Budget

Numbers tell it the best. The cloud service budget increased from $44,372 in 2014 to $1,247,284 in 2021. This is just the budget of the CIA. It shows the CIA cloud business growing rapidly and this will increase in the future. The government can slash the budget through data center integration, even at the expense of being criticized for cutting off some units (such as the CIA's Historical Collections Division). However, they still have to pay larger costs on cloud security, including hardware and software, as well as "Redesign the Legacy User Environment Leveraging AWS EC2."

Snowden wrote in his book that "The aim was to unite the agency's processing and storage while distributing the ways by which data could be accessed. In plain American, we wanted to make it so that someone in a tent in Afghanistan could do exactly the same work in exactly the same way as someone at CIA headquarters." It is true that the United States can use its super technical power to do something, but the strongest fortress was broken from the inside. More advanced and intelligent things do not mean more security. Legacy systems are often reliable, which has been proven with countless facts. Besides, if an employee can access it from Afghanistan, so can the enemy.

The Author Does Not Exist

by Variable Rush

It started years ago, around 2010 or 2011. I was a big fan of *Final Fantasy XI*. I played Yugdaba on the Valefor server. At some point I discovered there were a series of novels based on the game, but they were only available in Japanese, French, and German. There were no plans for an English release.

I had a German-to-English dictionary and thought I could read at least one of the books by translating each word individually. It was the summer, school wouldn't start for another few months, so I bought a German language edition from, you guessed it, Amazon.

In the few days before the book arrived, I thought of Google Translate. Could it translate faster and make more sense than me translating using a book? To test this idea, I found a German language fairy tale on Project Gutenberg - a German translation of a Japanese fairy tale, as luck would have it - and translated it using a combination of the dictionary, Google Translate, and a friend online who knew German and English. It worked. Within a couple of days, I had created a translation of a short story that had never been translated to English before, if Google was to be believed.

When the *Final Fantasy XI* book came in, I set to work on it right away. I felt great about my translation. I eventually contacted Square Enix's marketing department (I didn't know where else to go) regarding them paying me to translate the whole series. They said no.

I next made a mistake. I translated the entire book of fairy tales and sold it on Amazon. This was a mistake in that some of the fairy tales had never been translated to English. My selling the lot on Amazon counted as them being published, so I was unable to monetize the translations further by having them published in literary magazines.

I translated several more books this way. I also discovered Babelcube. Babelcube is a site that connects authors to translators. I signed up as both a translator and a writer. Several of my translations were translated to other languages by other people, and I myself translated several works to English from German using my tried-and-true method.

That was it for a long time. The intervening decade has been a strange decade for me. I got married, lost close family members, moved, changed professions, went back to college, moved again, and so much more.

So for most of this time, I added nothing to my translation empire. Each month I would be sent a royalty check from Amazon for ten or 20 dollars. Most of the sales were from a translation of an erotic fiction novel written by the same man who wrote *Bambi*. Yes, that Bambi.

Since one erotic fiction novel was about 80 percent of the money I was making in royalties, I sometimes thought how to increase the amount I received, figuring that if I increased the amount of stories I was selling that I could increase the 20 percent on the other side.

I tried using a site like Fiverr to pay people five dollars to write more erotic fiction, but after hiring two people who then sent me the exact same story, I stopped using the site.

During the summer of 2019, I came across a site called "Talk to Transformer." It was a demo of using an AI to write text. Fast forward two years and I find that demo has become something called InferKit. I tried it out. You can just press "generate text" and it will write off the cuff or you can feed it key words to make it write in a particular direction. So for my first pieces, I filled it with the kinds of keywords you would expect to find in a piece of erotica.

Those early pieces I made with InferKit are more, "wham bam, thank you ma'am" than the more nuanced, somewhat story-focused pieces I would later create with it. Granted, editing still has to be completed on each output. Sometimes characters change genders or do things that are impossible or say things that do not sound right or get hung up on a word or phrase (yesterday I had to edit the phrase "all of the colors" out at least a few dozen times as one of the characters in this LGBT story the program generated had a vibrator that contained a light that changed color). Each work comes to 2,000 to 5,000 words.

These new AI-written books make money for me in three ways.

1. Each costs a reader $0.99, so I get $0.35 on each one.

2. They're all in the Kindle Unlimited program, so for each 100 pages read, I get somewhere around $0.04 (more books equals more pages).

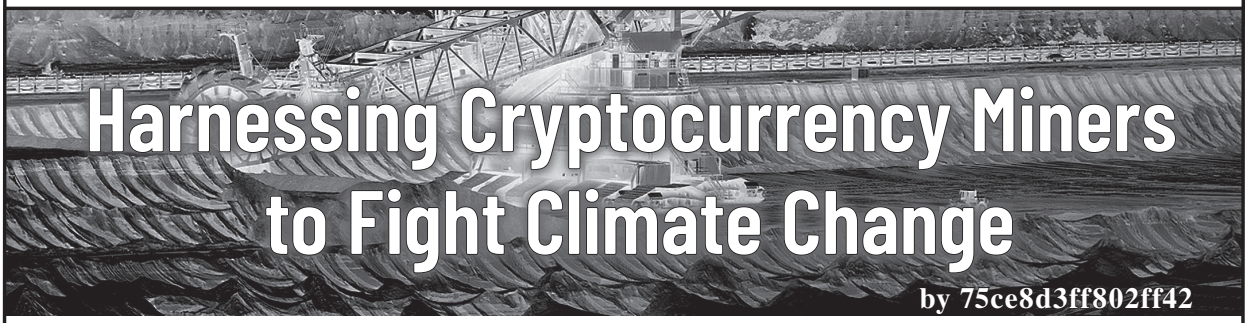
3. They each contain a sample of the original German-to-English erotica book to entice the reader to purchase that book at $2.99 and, of that, I get $2.

Since starting this new venture, I have not broken $40 per month in sales, but it's getting there. I recently broke $30 for the first time. I have

opted to, so far, only publish so-called vanilla erotica. I have not moved into Chuck Tingle-esque territory or anything more risque. The AI gets confused very easily at this stage.

I have two author names going right now for the erotica. I have one with a male name, for those stories that are told from a male perspective, and a female name for the female perspective stories. The pictures for the authors came from a site that makes AI-created faces of people that do not exist. Those names are Samantha Cherry (so named because I don't know a Samantha, yes, I laughed too much at that) and Benedict Urlaub (Urlaub is the German word for Vacation, what I hoped my foray into erotic publishing would net me). I have toyed around with the idea of "writing" other genres.

The InferKit program I have been using has been extremely fascinating. I can see how in the future it and programs like it will constitute the equivalent of duct tape in books, that an author who can't write action scenes or love scenes will use it to piece aspects of their stories together. And yes, I know that by using a program I am technically what is known as a "script kiddie." But as the ninth of the Ferengi Rules of Acquisition states: "Opportunity plus instinct equals profit."



Harnessing Cryptocurrency Miners to Fight Climate Change

by 75ce8d3ff802ff42

One of (if not the) biggest obstacles facing the widespread adoption of renewable energy (wind and solar) is the lack of a way of efficiently storing electrical energy at scale. We can store small amounts in battery packs, but large-scale storage is still a trillion-dollar problem. This leaves electrical grids with several unattractive options:

1. Overbuild so much wind and solar farms that there's still power available even on calm nights.
    - Extremely expensive and wasteful 99 percent of the time
2. Build expensive and inefficient energy storage facilities.
3. Supplement wind and solar energy with fossil fuel energy when necessary.
    - Often *less* green than 100 percent fossil fuel systems because on-demand fossil fuel generators are less efficient than always-on generators

I would like to propose, as a thought experiment, a way to harness the money behind cryptocurrency mining operations to expand green energy production. Yes, I know that I just proposed cryptocurrencies as a solution to a serious problem, but please hear me out on this.

My proposal: Designate 90 percent of surplus green energy produced at any given moment to a pool that is distributed to cryptocurrency mining operations in proportion to how much of the grid's production capabilities each operation has contributed. Contributions to the grid can be in the form of wind and solar farms or cash payments for the grid to spend on building/expanding wind and solar farms. As an added measure, consider adding an additional tax on all cryptocurrency mining operations that rely on fossil fuels for electrical energy.

Such a setup would give every mining operation an incentive to assist in building out the grid's wind and solar capabilities; an operator could invest in the grid and reap the rewards of effectively free power indefinitely (a small fee for maintenance may be required long-term). Some operators may choose to run their own wind and solar farms, but buying into the grid's system gives operators two advantages:

1. Geographic diversity provides more reliable power.
    - It may be calm where your operation is situated, but the odds are that it's windy *somewhere* on the grid's footprint
2. The option to simply pay the grid to expand wind and solar production saves mining operators the trouble of building actual wind and solar farms.
    - Just "let the professionals do it"
    - This also has the benefit of allowing for smaller mining operations that don't have the large capital required for building wind and solar farms

In my humble opinion, the jury is still out on whether cryptocurrencies are a net good or ill for humanity. Hopefully, a setup that encourages miners to contribute to green energy production would move the dial towards "good."

An Atavistic Freak Out, Episode Four

by Leon Manna

This story is a work of fiction.

5:43 AM on a Monday. Typing furiously into my laptop as the sun starts to rise, realizing that I intended it to be a late night and it ended up turning into an early morning, another maniacal, amphetamine-fueled organized keyboard mash which, by some ridiculous odds, turned into something that you could comprehend, or maybe even *read*. If you wanted to, that is.

I'm not Leon Manna. He was always just an idea when they stack the cards which, of course, are stacked against me. Leon Manna.... The name sounds like a stranger to me. Some barrier was crossed, a bridge to a terrible life filled with excitement, after declaring myself dead to escape The Machine. There was something funny about it. Your, no, *my* whole life destroyed in an hour long funeral service, nobody in the casket as they lower it down. Never again.... Now it's just checks and guns and cheap CVS cell phones that I drop into puddles. After the whole thing was over, I became Leon Manna. I lied to you, and I am truly sorry. Take the back door on your way out. The show goes on. It won't ever stop! Never! Don't count on it! Ride the wave! Mindfulness! You wouldn't like it!!!

So let's get back to my story. There I was, sitting on my couch like an idiot, waiting for the blotters to kick in, watching a mosquito fly around my room. Someone was knocking. They were like gunshots, Vietnam flashback to my old neighborhood, KDY at night, putting my nerves on edge, electrocuting my brain, 110 volts, neurons firing too fast to comprehend anything as my pupils dilated from the blotters and I saw the world in full color, not one, not three, but the entire range the human eye can even process.

No thoughts, just open the door. It was Lenny. His shirt was stained red. I stared at him for a second. The way he was just standing there, staring at me with this possessed, demonic look on his face was amusing. I knew I was supposed to be scared, but it was almost like he was trying to amuse me. I laughed and said, "Jesus man, are you okay?"

He groaned and his face turned red. "You left me on that beach! I'll brace you for this!" He swung his arm at me, missing by what, a foot?

"Hahaha.... You shat on a five-year-old and punched me in the chest! What else did you expect me to do?" I cackled a couple more times.

He let out a guttural noise and started staggering towards me. I backed up and pulled a switchblade out of my pocket. "Lenny... heh... I'll stab you! I swear to... *hah*... I swear to god I will! Please man! Hahahaha...." My organs were starting to hurt. I couldn't stop laughing.

His eyes were glazed and unfocused. Red spot, he missed his vein. Telltale signs of the type of junk addict who *wants* you to stab them. Maybe I should, for his own sake.

"You wouldn't do that.... You're gonna have to stab me.... Hehehehe.... Don't you live above the landlord? You spent too much time in drug dens as a teenager. Your mom was right about you! I had a whole talk with her last night over dinner. Bitch! Haw!"

"My mom went missing and is assumed dead, Lenny."

We stood there for a second and made eye contact, both totally silent waiting for the other to say or do something. But neither of us did; we just stared at each other. Then I chuckled, and so did Lenny. Now, rolling around on the floor, unable to control ourselves at all, a tenant peeked out of her door and then promptly slammed it shut. I laughed so hard I pissed myself. Is Lenny my friend? I'd hope not.

SECURE MESSENGER:

2600 Magazine: Yo

leon_3k: what's crackin goldstein

2600 Magazine: Why do you call me Goldstein?

leon_3k: Goldssten.

2600 Magazine: HOPE this weekend

leon_3k: hope for what

2600 Magazine: The conference. You coming?

leon_3k: Yes, of course. I'm gonna write about it, in your magazine, and I will be smoking crack the whole time. Then I'm gonna let a coyote loose inside the building.

2600 Magazine: do you have a job?

leon_3k: I am self employed, I invest in imaginary encrypted money and the stonks markets.

2600 Magazine: How high are you

2600 Magazine: Oh, the other thing I had to tell you is that we got a letter from the FBI about you, they don't appreciate some of the things you write about.

leon_3k: Kyle better be there.

2600 Magazine: No seriously, don't write anything crazy. We got subpoenaed last time.
leon_3k: F

Hackers On Planet Earth! How could it have slipped my mind? Why would it? And it was that year, so once more I would atavistically make a trip to New York no matter the distance I had to go, just to dive right into the very center of The Machine, all while being far too deep into some second life with too little correlation between the two to ever be able to turn back. I can see the point of no return through my rearview mirror, the exit I never knew I had to get off at until it had passed.

Me and Lenny started the trip. He loaded around three suitcases, which was strange considering we'd be there at most four days. He wouldn't tell me what was in them, but they seemed way too light. All I brought was some weed. I'm done with these research chemicals and the only thing I was researching was how high they would get me. Right as we got on the road, Lenny took out a needle.

"Put that shit away man! Not in the car! You need to drop that before it's too late. Have you ever read William Burroughs? I bet you can't even read and some sort of idiot algorithm in your heroin brain calculates it for you...."

"Shut up, shut up! I need it! You fucking nerd.... My chest hurts! *Uuaahhhhh!*" Unhinged.

Idiot! I lit up my first spliff as we were driving. It was high quality weed. I felt very calm as my attorney suffered from a borderline opiate overdose next to me. It was nice to *not* be on some crazy psychotic chemical. Things felt peaceful.

And here I am now, flying down Interstate-95 in light blue denim pants, cuffed up twice, waterproof Vans, glasses hanging onto my face by a thread. The car was going about 70 MPH on a highway in SC. My shirt was in the back seat, because the AC didn't work and the heat in Charleston was reaching 94 degrees Fahrenheit. Lenny had his head back with his eyes shut, sweating and groaning every now and then.

I was focusing on the road when suddenly it all made sense. The FBI asked me to sing them a song yesterday... or maybe it was right at Sawtooth when they asked. Three letter agencies are better than no audience at all. Do I sing to them? I don't think I'm even capable of knowing when I am.

26 was the number on my shirt. What did it signify? I didn't know. I had thrown a suitcase together in a hurry at the last minute, a mixture of Khaki pants, shorts, white shirts, and socks. The amount of days we would be there outnumbered the clothing items by 26. And that somehow matched the number on my shirt, which matched my age, which matched the date. Was there a meaning? Or was this magical thinking? Did Lenny agree? Did Goldstein? Do you?

I looked up. I was standing outside of Hotel Pennsylvania in New York, not moving, with a dumb look on my face. This was where HOPE was (at the time) being hosted. Me and Lenny were staying in a shitty motel across the river in Hoboken, New Jersey. The parking was better out there, and we took a train to get into NYC.

My daydreaming was cut short by Lenny. "Stop staring at the hotel and let's get started. I wanna interact with these freaks so goddamn bad...."
"They aren't freaks. They're actually great people."
He laughed, and said, "If they're anything like you, they're freaks."

There was a journalist sitting at a table near an auditorium. I don't consider myself a journalist, but something *like* it. Still, that's giving myself too much credit. I just write stories. We started talking, and he asked me my name.
"Ocha. I go by my last name."
"Alright Ocha, you okay being in a story?" He looked at me intensely.
"I was going to ask you the same thing." Crooked grin.
"Who are you writing for?"
"I'm doing a story for La Palma Tech."

He said some random online publication I'd never heard of. Then he mentioned that he had some cocaine, and asked if I'd like to do a line with him.
"I'm supposed to be in that talk."
"Let's just go to the bathroom real quick." He grinned at me.
"I don't think that's wise. I heard they're going through people's bags while they're in talks. Hotel rooms too, the ones who are staying here! They're looking for drugs and weapons. Intel says there's about three firearms in the building right now. They already caught eight people for coke, and seven more for psychedelics. Didn't you see them taking people out?" I tried to look concerned.

His face changed. He got scared. Everything I just said was completely false. I don't really know why I was fucking his brain up the way I was. I think I just wanted to see if I could. He was pissing me off anyway, and besides, anybody who offers random people cocaine

deserves it. They weren't actually searching anybody's bags, I just wanted him to be in a constant state of fear that they would.

I don't remember what the talk was about, because I was too focused on trying to spot FBI agents. I wasn't able to, because all the FBI agents were dressed in normal clothes. I declined the journalist's offer of cocaine. He decided he was just going to snort it right there in the auditorium, and was taken out by security ten minutes later. I remembered the lie I told him warning him about this and wondered what was going through his head as they took him away. I pretended I didn't know him and stared straight ahead.

Then I heard a scream, and turned to the back of the auditorium. I saw Lenny's silhouette standing in the doorway. He rushed over and sat down next to me. The dude on stage let out a very wet fart.

"I gotta go man, I'm freaking out. They're taking people away left and right! We have to leave." He sounded afraid.

"Hold on, just wait it out. We'll be fine, we didn't do anything," I whispered.

"Cmon, let's go!"

"Alright, alright, we'll leave. You have a point. I saw the pigs take some poor nerd away 30 minutes ago. Then security kindly had a journalist escorted away."

"I saw him on the way out.... They didn't look happy. As your attorney, I advise you to leave so we don't end up like him."

We got up and exited the auditorium. We chose not to take the elevator, but rather go down a restricted stairway. Neither of us were allowed to do this. We made it downstairs and into the lobby, when I heard a shout.

"Stop! Don't move!"

I looked behind me and saw a U.S. Marshal, some fat, middle-aged walking handlebar mustache. He looked like a freak cartoon version of Hulk Hogan after drinking beer and smoking cigarettes for 15 years straight. I looked at Lenny and we ran. Lenny barreled right into some silver-haired kid with a guitar, knocking him over in an instant. I dashed out the front door. We managed to outrun him, because he was about 240 pounds, and got into a nearby subway station.

TRANSCRIPT ISSUED AT REQUEST OF LAW ENFORCEMENT VIA SUBPOENA

[Dial tone]

Goldstein: Did you get away?

Leon: Oh yeah.

Goldstein: It's gone to shit. Someone burglarized our hotel room and stole two passes. We still don't know who did it, and they won't share the CCTV footage with us.

Leon: I'm sorry, what?

Goldstein: Yeah, someone got one of our staff to disclose our hotel room, and then somehow got in and took a pass.

Leon: ... I'm gonna have to call you right back. [Phone call ends.]

So *that's* how Lenny got our passes!

We saw the first palm tree at the bottom of North Carolina. We made it to Charleston, and Lenny said he needed a swim. We got to a beach and went down to the water. I smoked out of my hash pipe quickly and we got into the water. After a moment, I said, "that was crazy...."

"You're telling me? How long were we there for anyway?"

I laughed. "One day. It was supposed to be three. It was pretty funny when you let that scream out and burst into the auditorium."

He chuckled. "Yeah, I did that on purpose. Did you see their faces? The nerd on stage looked like he shat himself!"

"He did shit himself! I heard it! We outran a U.S. Marshal. We must be extremely lucky."

"No, we're extremely smart." I noticed he was talking about both of us, and not just him. I'd never seen him as relaxed and friendly as he was.

"You proved yourself," he said.

I was shocked. "What?"

"You're someone I can respect and view as an equal now. And why? Because you actually listened when I told you we had to leave. I'm your goddamn attorney, and for the first time you actually listened. You're an idiot genius who doesn't know what's good for him. A lot of my clients don't listen. But when someone does, they've proved themselves. Besides, the pig could hardly keep up with you."

I didn't say anything for a second, just smiled. Then I laughed and asked, "What was in those suitcases anyway?"

"Hah! A couple servers I stole out of a server farm, seven laptops from the editor's room, a bunch of HOPE passes, four USB drives I stole out of a police station, and then one very very sensitive government document I really needed to get rid of."

My smile disappeared. Awful jackass....

What will happen next? I don't remember, so we will both find out when I read my notes next time.

HACKER HAPPENINGS

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

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

June 16-17, 2022
RVAsec 11
Omni Richmond Hotel
Richmond, Virginia
rvasec.com

July 1-3, 2022
CircleCityCon 9.0
Westin Downtown
Indianapolis, Indiana
circlecitycon.com

July 13-17, 2022
ToorCamp
Doe Bay Resort
Orcas Island, Washington
toorcamp.toorcon.net

July 22-24, 2022
A New HOPE
St. John's University
Queens, New York
hope.net

July 22-26, 2022
May Contain Hackers
Scoutinglandgoed
Zeewolde, The Netherlands
mch2022.org

August 3-10, 2022
BornHack 2022
Funen, Denmark
bornhack.dk

August 6-7, 2022
Vintage Computer Festival West
The Computer History Museum
Mountain View, California
vcfed.org

August 11-14, 2022
DEF CON 30
Caesars Forum, Harrah's, Ling, Flamingo
Las Vegas, Nevada
defcon.org

August 12-14, 2022
Fri3d Camp
Hopper Youth Residence De Kluis
Sint-Joris-Weert, Belgium
fri3d.be

September 22-24, 2022
Texas Cyber Summit
Hyatt Regency
Austin, Texas
texascyber.com

October 13-14, 2022
GrrCON
DeVos Place
Grand Rapids, Michigan
grrcon.com

October 21-22, 2022
SecureWV 13
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

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

For Sale

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

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

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

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

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).

Help Wanted

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

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

Announcements

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!

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

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

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

NSolve[(x^4/(85^2 + x)) == 1,x] In Wolfram language X^4/(85^2 + x)) == 0.84 where 85 is the known SemiPrime and x is the smaller factor. As x approaches zero within error then x is found. In the above < 1, x value is found between 0 and 1. https://www.scienceforums.net/topic/124453-simple-yet-interesting/page/4/#comments

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

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

Services

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

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.

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.

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

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.

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

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

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

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

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.

Personals

DO YOU WANT TO BE A HACKER? I've had some write to me asking for tips on this or that, but based on what I read in the Letters, there are many of you out there who could use a bit of coaching. Long gone are the days when I billed out at $250/hr to save a datacenter's day or other such emergency. I'm in prison. You can look me up on the TDCJ website and see I'm no weirdo. I do have plenty of time on my hands. Lucky you! So, don't delay, write to me with your problems, questions, pithy comments, or exploits. The best way is to use the messaging app www.jpay.com. Looking forward to hearing from you. Ryan Sumstad, Ph.D., #01918058, Wynne Unit, 810 FM 2821 West, Huntsville, TX 77349.

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

I AM A 37-YEAR-OLD FREE SOFTWARE ACTIVIST, interested in all aspects of copyright, trademark, and patent law. Looking to meet similar minded women, 26-43 in the greater Seattle area. My interests are GNU/Linux, social justice, Mexican food, ghouls, model trains, and video games. Just a Crash looking for my Burn. I have strong opinions about obscure media formats. I like drinking, cooking, doodling and wildlife. Let's hit the clubs, make each other laugh. I like a laugh, chat, bit of a debate, an argument. I like life. Goldentee@gnu.org

GREETINGS FELLOW KEYBOARD COWBOIS! *smirk* I am an anarchist (prisoner of war) held illegally in the state of TX for a crime I did NOT commit. I am seeking good intelligent conversation and casual debate. Preferred subjects include but are not limited to: politics (world or domestic), technology (especially automation), ecology and sustainability, sci-fi, and sociology. Intersections of the above are a bonus. Write to the following: David Danforth - 02250914, Wallace Unit, 1675 FM 3525, Colorado City, TX 79512 or JPay.com - and remember: we do not forgive and we do not forget!

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

Deadline for next issue: 6/23/22.

A New HOPE
July 22-24 2022
St. John's University
Queens, New York City

The Hackers On Planet Earth (HOPE) conference will be an in-person event in 2022. There is still time to make your plans to be part of A New HOPE!

Visit www.hope.net for tickets and the latest news about the conference program.

A New HOPE will have talks, workshops, performances, and many other opportunities to learn, teach, socialize, and enjoy. Topics will include hardware hacking and do-it-yourself electronics, information security, hacking culture and ethics, and much, much more. It's quite likely you'll still have a little time to submit a talk or workshop idea after reading this - check our website!

The theme, "A New HOPE," recognizes the amazing challenges and changes the world has gone through. HOPE will highlight the losses, strife, and upheaval of our times. It will also celebrate the triumphs of science, technology, and creativity.

HOPE's new venue is St. John's University in Queens, which offers more space and greater opportunities than ever before. There is on-campus housing and discount deals at hotels in the area. St. John's is easily reachable from New York City's public transit system and airports. We have a detailed travel guide on our website that will show you how easy it is to get to HOPE!

Volunteers are welcome! Visit www.hope.net for volunteer opportunities and how to get in touch. You can also stop by the Information Desk at HOPE to find out more.

A New HOPE
July 22-24 2022
www.hope.net

"There's just not that many videos I want to watch." - Steve Chen,
co-founder and former Chief Technical Officer of YouTube

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
typ0

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber, olssy

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: King Missile, Twisted Sister, Jandek, Havana 3 A.M., Andriy Khlyvnyuk, Pussy Riot
Shout Outs: Dee Snider, Sergiy Kyslytsya, Karina Shedrofsky, Emma Best, Chris Smalls, Mark Critch, Dmytro Kisilenko, Maksym Lutsyk
B.I.H.: OAN

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

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*,
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $31 individual,
$60 corporate (U.S. Funds)
Overseas - $44 individual, $75 corporate

BACK ISSUES:
Individual issues for 1988-2021
are $7.25 each when available.
Shipping added to overseas orders.
All back issues (1984-2021) available
digitally as annual digests at store.2600.com

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

***2600* Office/Fax Line: +1 631 751 2600**

MEETINGS

WE CONTINUE TO REBUILD 2600 MEETINGS WORLDWIDE. WE HAVE ADDED A BUNCH OF NEW MEETINGS FOR THIS ISSUE. PLEASE TAKE PRECAUTIONS WHERE WARRANTED AND BE SURE TO GET VACCINATED! WE HOPE TO BE BACK TO NORMAL IN THE NEAR FUTURE. KEEP CHECKING THE WEBSITE BELOW FOR THE MOST UPDATED LISTINGS AS WELL AS ADDITIONAL INFORMATION.

CANADA

Alberta

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

IRELAND

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

SWEDEN

Malmo (@2600Malmo): FooCafé, Carlsgatan 12A.

Stockholm (@2600Stockholm): Kungshallen food court, Kungsgatan 44.

UNITED KINGDOM

England

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): Gamers Guild, 2223 S 48th St, Suite C/D. 6 pm

Prescott: Merchant Coffee, 218 N Granite St.

California

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

Colorado

Denver (Lone Tree) (@denver2600): Park Meadows food court.

Fort Collins: Starbucks, 4218 College Ave. 7 pm

Connecticut

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

Florida

Jacksonville (#Jax2600): Goozlepipe & Guttyworks, 910 King St.

Kansas

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

Maine

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

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

Michigan

Lansing: The Fledge, 1300 Eureka St. 6 pm

Minnesota

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

Missouri

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

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York (@NYC2600): Citigroup Center, 53rd St and Lexington Ave, food court.

Rochester (@roc2600): Global Cybersecurity Institute, 78 Rochester Institute of Technology. 7 pm

North Carolina

Raleigh (@rtp2600): Sir Walter Coffee, 145 E Davie St. 7 pm

Oklahoma

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

Pennsylvania

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

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Dallas: The Wild Turkey, 2470 Walnut Hill Ln #5627.

Houston (@houston2600): Agora Coffee House, 1712 Westheimer Rd. 6 pm

San Antonio: PH3AR/Geekdom, 110 E Houston St. 6 pm

Utah

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

Virginia

Arlington: Three Whistles, 2719 Wilson Blvd.

Reston: PH3AR/Nova Labs, 1930 Isaac Newton Sq W. 7 pm

Washington

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

*** indicates Thursday meeting**

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

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

www.2600.com/meetings

Payphone Booths

United States. Seen outside of the local independent Pymatuning Telephone Company in Transfer, Pennsylvania, this booth wins awards for its association with the cool sounding names - and for simply existing and providing shelter. The phone itself is a functioning second generation GTE 120B.

Photo by Maya King

England. While this Oxford booth looks just like the real thing - and no doubt was at some point - it's actually an ATM, at least on one side. Someone had the bright idea of attaching an actual payphone to the outside, which is one of the strangest things we've ever seen. And yes, it works.

Photo by Jeff Alyanak

Cuba. These booths are just plain weird. Found in Havana in a place that advertises the country people are already in, these look like museum exhibits somehow. They are certainly the clearest booths we've seen in a while.

Photo by c

United States. This Seattle phone booth, seen in the Maple Leaf neighborhood, is torn between being a phone booth and a library. The phone doesn't work and the shelves are empty. Stay tuned.

Photo by Jesse Arnold

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

What's funny here is that we assumed this was the seafood restaurant that grabbed the Twitter handle before we could for our *Off The Hook* radio show. But guess what? There's *another* seafood restaurant in Bethany Beach, Delaware with that name and *they're* the ones with the now seemingly abandoned Twitter handle. It's all good - it's only Twitter - we don't care. Thanks to **murph** for reminding us.

What a great picture, *also* found by **murph**. It's a little gas station sign in Hope, New Jersey and a great reminder of our upcoming HOPE conference in July. It also reminds us that we didn't get the Hope Twitter handle either. Amazingly, that one appears to be abandoned, too. Again, we're fine. Frustration is what keeps us moving forward, after all.

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.