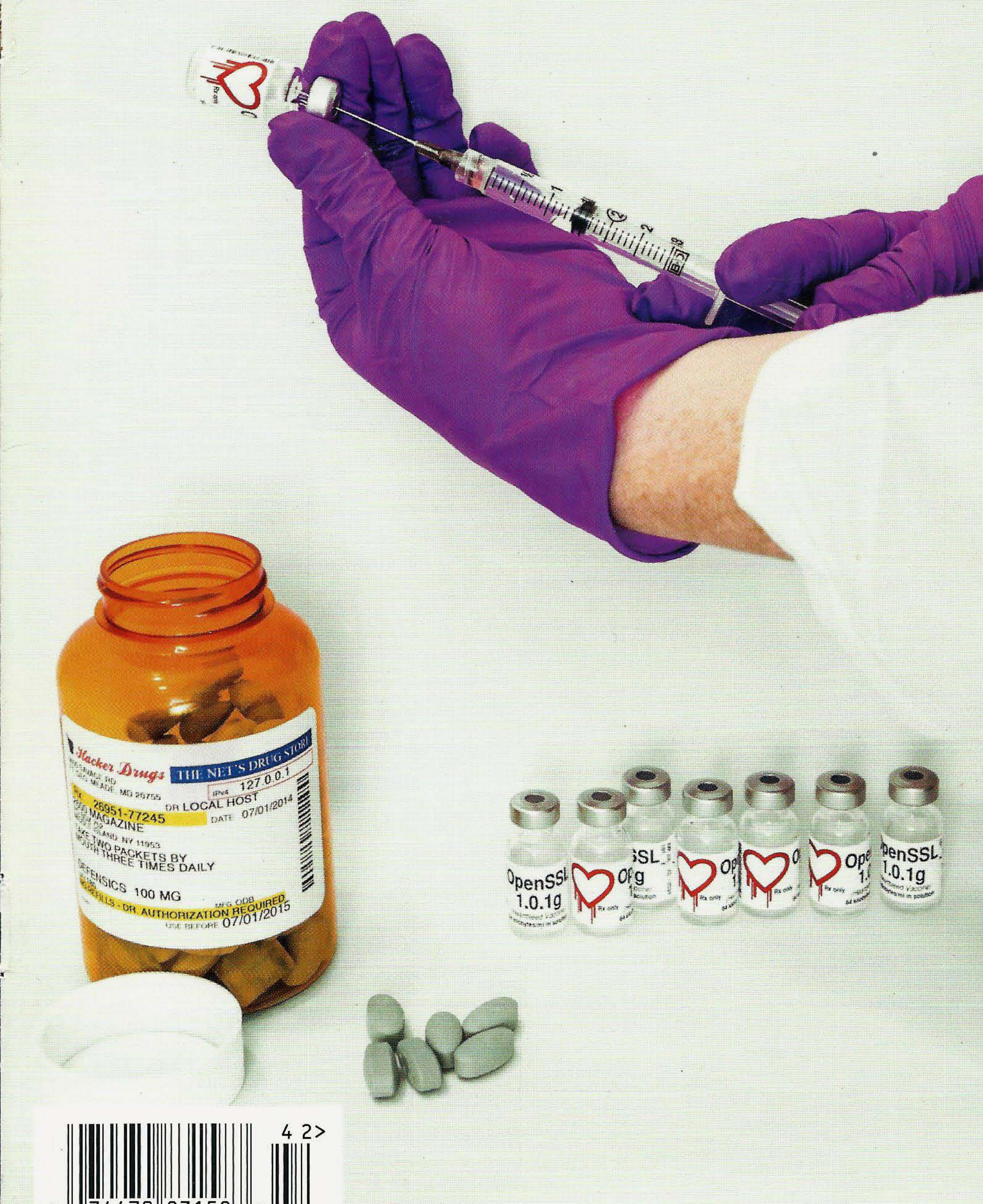
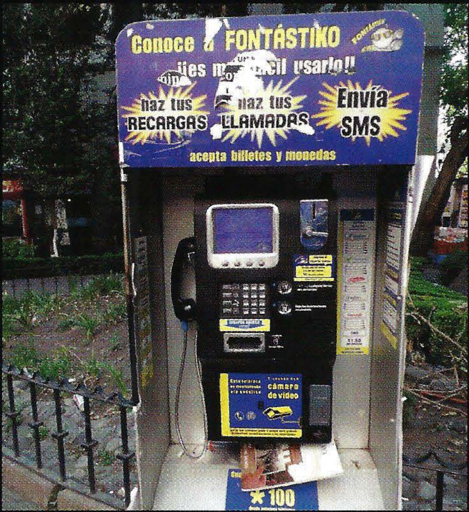
Volume Thirty-One, Number Two
Summer 2014, $6.95 US, $7.50 CAN

2600

The Hacker Quarterly

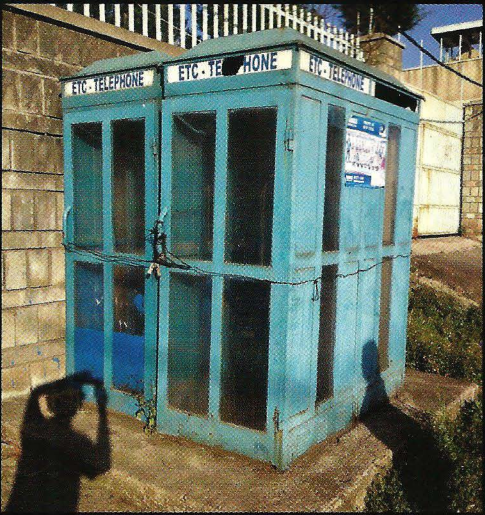


Payphones of the World



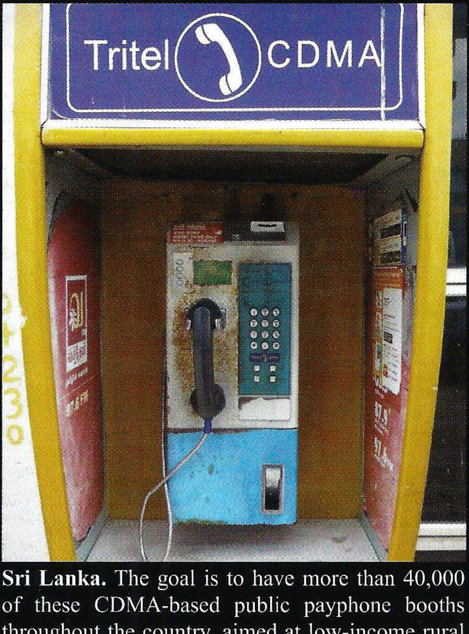
Mexico. This phone clearly sees itself as the center of the universe. Found in the Zona Rosa district of Mexico City, there's even a warning that you're being spied upon.

Photo by TProphet



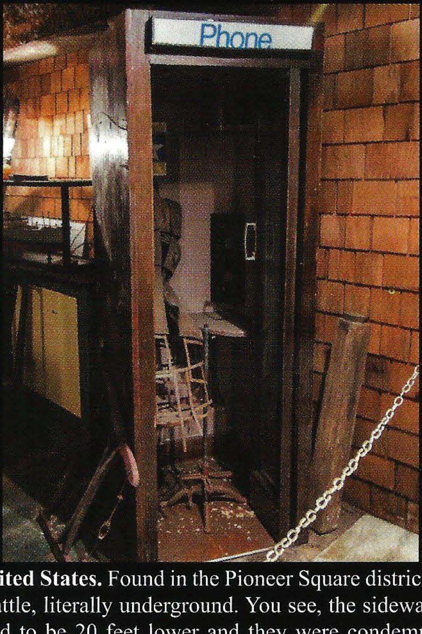
Ethiopia. We're not exactly sure what the fate of these phone booths in Addis Ababa is, but there is a certain irony in their being closed off by telephone cord.

Photo by Jon P



Sri Lanka. The goal is to have more than 40,000 of these CDMA-based public payphone booths throughout the country, aimed at low-income rural communities. They're far cheaper than landlines or mobile devices.

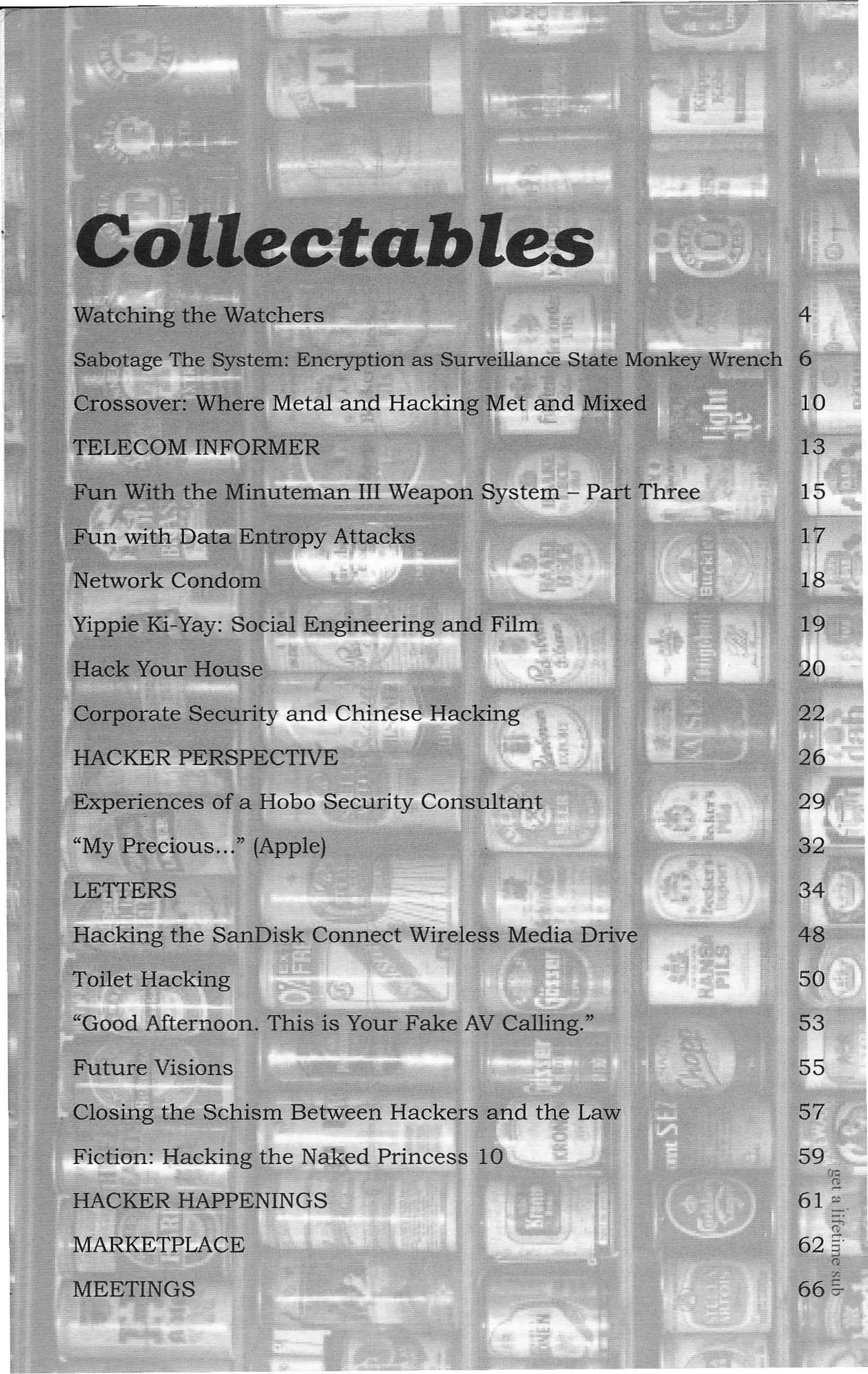
Photo by Matt



United States. Found in the Pioneer Square district of Seattle, literally underground. You see, the sidewalks used to be 20 feet lower and they were condemned altogether in 1907, but soon found a home for various illegal activities. Perhaps even phone phreaking.

Photo by Ryan Reggio

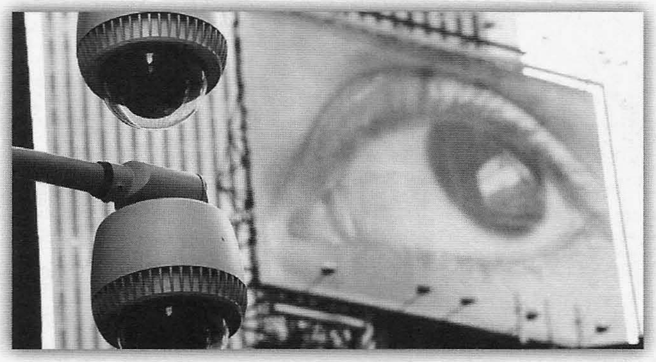
Got foreign payphone photos for us? Email them to **payphones@2600.com**. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (More photos on inside back cover)



Collectables

get a lifetime sub

Watching



the Watchers

If there's one thing we've learned, it's that those engaged in surveillance really hate to be observed themselves. This is why when you point a video camera at a cop, you'll likely get some push back or worse, even when the law is completely on your side. The same holds true for government officials who will stop at nothing to conceal their true actions and motivations. They have good reason - just look at how many times such revelations wind up hurting them. And let's not forget our friendly corporations, engaged in all kinds of privacy invasions hidden in services and the promise of convenience. They certainly don't want to be under the magnifying glass themselves.

This last year has been a tough one for those running the show. On a regular basis, the Edward Snowden leaks have revealed the extent of the massive surveillance taking place worldwide, invading the privacy of everyone from average citizens to world leaders. When this all began, many people in the States were willing to accept a little privacy invasion if it resulted in more security, which is the usual justification for removing a few liberties. That worked for a while, until the revelations kept coming and expanding the scope of the actual spying.

We heard about the metadata and the spying on diplomats. We then heard of the many secret partnerships between the NSA and various governments, allowing more spying on more people around the world. We learned of the massive amount of tapping into fiber optic cables around the world and how telecommunications companies were being forced to cooperate. Then we started hearing of attempts to weaken encryption in commercial software, the compromising of security on smartphones, even the planting of malware on target systems to help in the spying efforts. Social networks were being used to gather and analyze more data on individuals. An internal NSA presentation seemed to actually gloat over these efforts, saying in a slide show: "Who knew in *1984* that this would be Big Brother...." (showing an image of Steve Jobs holding an iPhone) "...and the zombies would be paying customers?" Whoever wrote this clearly didn't know that there are no zombies in *1984,* only pathetic people victimized by the all-seeing State. The irony is pretty staggering.

We could go on and on about the scores of revelations that have come out, making the NSA's intentions quite obvious and the technological potential more than a little frightening. The point is that throughout all of this, the conversation changed. People who were once willing to accept the government's defense are now questioning the necessity of this kind of surveillance. When former NSA employee and whistleblower William Binney came to HOPE Number

Nine in 2012 and claimed that "the NSA has put together over 20,000,000,000,000 (20 trillion) 'transactions' - phone calls, emails, and other forms of data - from Americans, including potentially almost all of the emails sent and received from most people who live in the United States," it was widely seen as an exaggeration, since the numbers seemed so incredible. Now we know that they're not so incredible after all.

When Snowden first came forward, there were many in positions of power who were calling for him to be tried for treason. An airliner was even forced down by United States and European Union authorities because of a rumor that Snowden was on board. Make no mistake - the authorities are not happy with this sort of thing and they will do whatever they can to get their hands on the people they blame. There are many individuals who have put themselves in harm's way by getting involved in this and other such stories of secret documents that expose betrayal and wrongdoing on the part of powerful governments. Once we might have called them paranoid for not wanting to return to their home country or for not agreeing to put themselves in the hands of the authorities for "fair treatment." We can call ourselves a "nation of laws" and delude ourselves into thinking that justice awaits those who go through the system. But that's rather hard to believe when we routinely see laws bypassed or broken outright by the same authorities we are expected to trust. The NSA was never supposed to spy on American citizens, but that little rule was sidestepped. Drone strikes on suspected terrorists in foreign countries are now routine, without regard to innocent casualties, due process, or even the wishes of the foreign countries' governments. We've seen how quickly those in charge are willing to throw civil rights down the drain, as they did with the Patriot Act, which has done more to harm this country than any terrorist act ever could. So we ask forgiveness for not immediately trusting that these people will do the right thing. Their track record speaks otherwise.

The question we must ask ourselves at this point is if we're better off knowing such things or not knowing them. As hackers, we have a very clear and simple approach to this: knowledge needs to be shared and information is by default free. That certainly doesn't mean that *all* knowledge and information should be revealed. There are indeed sensitive bits of data that would be detrimental in the wrong hands. But the same holds true for individuals. When *their* data falls into the wrong hands (i.e., snooping authorities and corporations), we need to do something about it. And, yes, telling the world that this is going on is appropriate and necessary. Those in power will always play the security hand and imply that thwarting that is tantamount to risking lives. We say that hand is vastly overplayed and that we face far greater risks if we allow these programs to continue unchallenged. A simple way to realize this is to theorize on what this kind of power could result in if it were in the hands of a truly evil government. If the ability to do this kind of thing is left in place, it *will* fall into such hands eventually. And then the *1984* scenario will become truer than most of us believed possible.

Another thing to consider is how the story will continue to be distorted. The mass media will inevitably make it about the individuals involved in leaking the information, rather than the actual issues. Character flaws and skeletons in the closet will be used to cover up the importance of the revelations themselves. This is an effective approach, because it gets people talking and fixated on something else, which is the best way to bury a story. You will also see this strategy every time our data is compromised due to improper security or lack of precautions. The companies involved will inevitably point to "hackers" as the culprits. We've seen this done even when there wasn't a security breach in the guise of "hackers *could have* gotten your data, but we prevented it." This form of distortion is something we've been battling for decades. Think carefully of where you actually get the information that those in power don't want you to get, such as how to protect yourself from being spied upon. Certainly not from those in power. Hackers are the ones who reveal the inconvenient truths, point out security holes, and offer solutions. And this is why hackers are the enemy in a world where surveillance and the status quo are the keys to power.

Sabotage The System: Encryption as Surveillance State Monkey Wrench

by D.B. LeConte-Spink

Since Snowden's 2013 disclosures confirmed longstanding assumptions that the NSA and other Western spy agencies have secretly constructed a massive global surveillance infrastructure - at a cost of well in excess of $50 billion - much focus has been brought to bear on techniques, technologies, and tactics capable of protecting individual citizens against this snoopware monstrosity. And, as a direct result of Snowden's heroic whistleblowing, we now have a generally good sense of what does - and does not - work when it comes to protecting data-in-transit from these spy regimes. Or, more formally, we know which tools are more and less successful in increasing the cost and difficulty of a successful surveillance attack: given the TAO and their near-bottomless arsenal of 0days, we don't look for *perfect security*, but rather tools robust against the widest range of automated attack vectors.

That's all well and good. Understanding which tools really "work," and which are simply ineffective - or backdoored (or both) - is necessary. However, we can also see clearly that this necessary work is not in itself sufficient to accomplish the goal of undermining the astonishingly apocalyptic capabilities that such global surveillance infrastructures represent. For, in the wrong hands (or even in the "right" hands seeking the wrong ends), the power of such systems that can spy secretly on any non-encrypted electronic communications anywhere in the world - and, worse yet, dig back into enormous archived troves of intercepted/stolen data to run historical queries against any desired "selectors" - is so great that eventual systematic abuse is all but inevitable. Human beings have not shown themselves to be very good, in historical terms, at making wise use of supremely powerful weapons designed specifically to be used against other human beings. And, as we all know, spy systems are designed to be used against targets: human beings who, for whatever reason, are defined as "enemies" of a given government. The hacker community knows all too well how easy it is to find ourselves labeled as "enemies" of this or that state entity - whether such label is justified or not. Fair warning, indeed.

What's required, in the words of Evgeny Morozov, is an approach to these illegal, secret spy regimes that promises to "sabotage the system" at the most fundamental level: something that will make the systems themselves inoperable, ineffective, inefficient, or some combination of all three. Without doing so - without sabotaging the system - the system will inevitably, in due course, come to be used for evil ends, by evil people... and, as William Binney and others have pointed out with forceful, well-founded warnings, once put in place such systems are nothing short of "turnkey totalitarian states." There is no undo button; by the time they're locked-in and fully functional, any resistance, any attempt at defiance, will prove too little, too late... and too easily squashed by the all-seeing eye of Sauron.

It is not enough to protect ourselves, individually, from this surveillance nightmare. Indeed, many readers of this article will already have the expertise, knowledge, and capability for self-protection to a high degree of success. Nevertheless, even if as individuals we can (and, I most certainly hope, do) protect ourselves, we must do more. We must also protect ourselves, collectively, as a society and a species. We must sabotage the system. But how?

The Surveillance Monkey Wrench

To begin, we can easily see how individual activists can use encryption and obfuscation technologies to protect data-in-transit. Such tools are inexpensive, well-established, and in many cases have been shown via Snowden's whistleblowing to be effective against automated NSA attack vectors. That's great: Alice can talk with Bob, and Snooping Uncle Sam can't see what they're saying. As Snowden has said, the maths work. He's correct. We all, by now, surely know and understand this.

Building up from there, is it enough for individual citizens - due to their technical capabilities and knowledge - to protect ourselves, one at a time? Metaphorically, is microeconomic theory enough to explain the great forces of global markets? In a word: no, it's not. Those of us with that capability are similar to winners of the "privacy lottery" - we have the luxury of privacy, but the vast majority of other players will lose. The collective result is that the global surveillance regimes sink deeper and deeper roots into our planet's collective future. The lucky winners do OK; the world overall goes down a bad path indeed.

To understand why that's so, it's useful to think on the problem from a slightly different angle....

The Econometrics of Spy Regimes

It is said that, at the apogee of the Stasi's reign of terror within the former East Germany, fully one in six citizens was acting as a Stasi informant on their friends, neighbors, and colleagues. This was in a time before cheap, fast computing technology - which required all those snitch reports to be filed manually, by hand. The paperwork burden was concomitantly enormous, and the efficiency of the system ground to a halt. It's literally impossible, in practice, for that big a chunk of a country's population to be effectively snitching on the rest: the swamp of paperwork becomes too much, and the result is a version of Kafka's impenetrable, dysfunctional, amoral bureaucracy made real.

Unfortunately, when we add in fast, cheap computing power, things change dramatically.

Yes, it's true that the NSA (and other spy cartels) spend billions like it's water through their fingers. With those billions, they get enormous bang for their (well, our) bucks: they're able to free-query datasets comprised of many trillions of data points. Fast, accurate, and above all else cheap on a per-query basis. Any analyst with a workstation - even an outside consultant working from an underground bunker in Hawaii - can hit the DB again, and again, and again with no technical constraint holding him back. Worse, the cost per query is infinitesimally small. Those data are accessible, cheap, and eternal. They never go away.

Make It Cost

This enormous drop in the cost of accessing and organizing data is what drives the frightening power of the modern surveillance regimes... but it's also their weak spot. Just as Achilles had his heel - the one place on his body vulnerable to damage - so it is that the cost metrics of spying are the most easily accessible point of attack for activists who work to ensure that these spy monstrosities don't blanket our planet with a future of monochrome, standardized, unchanging totalitarian horror.

In practical terms, the reason these costs are so low - and going lower every day - for spy regimes is *automation*. Data are collected automatically, collated automatically, and added to existing DBs automatically. Once a new "input program" is initiated - by stealing data illegally from companies, illegally tapping fiber optic channels, or illegally coercing companies into handing over data "voluntarily" - the process is automated. Without automation, it's utterly infeasible to add hundreds of billions of data points per day and, of course, impossible to query across them. Automation is the key.

That is precisely, exactly where Achilles is uniquely vulnerable.

Break the efficiency of automation, and we break the cost leverage of these spy machines. To do this - to break the machine - we need only increase the cost of automation. This, as we see below, is trivially easy to accomplish... not only for individual activists, but for vast swaths of the human population on the planet today. Automation thrives on certain assumptions, and certain regularities of structure within underlying data sets. Remove those regularities, complicate the data model, inject stochasticity and uncertainty into the pool of underlying information... and automation breaks down entirely. Cause and effect.

Decoupled Selectors

Jacob Appelbaum has forcefully - and wisely - argued that we don't need to make data-in-transit crypto "perfect" or "unbreakable" in order to have a devastatingly effective impact on illegal surveillance regimes. Even if encryption only makes the administration of those spy regimes *more expensive,* we will have success. The costs of running such systems don't rise linearly with increases in cost driven by data complexity - they accrete exponentially (perhaps even non-polynomially) as per-datum costs rise. Any systems architect is familiar with such a dynamic: systems complexity is rarely a linear metric.

When one studies the Snowden documents thus far available, in detail, the importance of "selectors" becomes clear. Selectors, in spy-speak, are variables used to mould queries (congruent with SQL nomenclature, in a sense). One selector that comes up over and over as a crucial cross-domain bridge - a join key, as it were - is physical IP address. Physical IP address can (and does) tie together webmail, IM chats, video streams, cloud-based storage access, website visits... one's physical IP can often be the skeleton-key fingerprint identifying a unique individual. Of course, there's all sorts of corner-states where such is not the case, but for an awfully large percentage of folks using the interwebs, their IP address is their unique identifier as they go about their online lives (in this, we speak of short-term durations, *pace* DHCP et al).

So, we must break that selector. Fortunately, we know exactly how to do that.

There's an endless list of tools that serve to decouple one's physical access IP address from one's online activities. Beginning with the most feebly secure "free" proxies and adware-based "VPN services," and continuing all the way up through Tor's robust architecture and cryptostorm's token-based model, these tools are widely available and generally dirt cheap if not outright free to use. For automated spy systems, the use of these tools introduces a frustratingly opaque layer of uncertainty in cross-domain selector searches: IP addresses are decoupled from individual activities in a way that's variable and unpredictable over time. The spies' data warehouses fill up with oceans of data... but one of the crucial connectors amongst all those tidbits of intel is lost. IP address becomes a broken key.

Encrypt All The Datas

Taken a step further, cryptographically-secured methods of decoupling IP addresses from online activity add vastly more leverage to our efforts to make global spy systems cost-prohibitive to administer. This is trivially easy to see, in fact: imagine all those encrypted packets, flowing into Bluffdale's rows and rows of SAN'd hard disks... each packet a bitter little pill for data administrators. Perhaps vulnerable to eventual brute-force decryption (or quantum-based attacks, someday), but in the meantime those packets cost money to store and yield zero benefit for the spies (assuming competent header data obfuscation and/or encryption, to mask protocol details and so on). Sure, the cost-per-packet for storage is infinitesimally small... but add up a few hundreds of trillions of 'em and things get interesting.

Better yet, the cost of *encrypting* those packets is so small as to be essentially zero. A bit more electricity burned on the client-side machines, perhaps... and a bit more wear and tear on the logic gates of CPUs and swap memory. For each of us, those costs won't ever add up to a cup of coffee or a packet of ramen over an entire lifetime of crypto-caution... but for the spy cartels, an ever-expanding bolus of indigestible encrypted packets is a bad (read: costly) thing indeed.

Yes, of course, the TAO can attack individual packets, or packet streams, or targeted individuals. But TAO doesn't scale, and never will. If even 0.01 percent of the global human population were to be TAO'd - subjected to manual, TAO-level attack - the TAO itself would need to include hundreds of thousands of warm bodies. That's impossible, as TAO relies on unique skills, not to mention a total contempt for "the rule of law" - neither of which can be boosted up to entire cities' worth of human beings doing the work. The entire model breaks down at scale.

Ned Ludd's Lessons

One need not have any particular attraction to the philosophical underpinnings of Ned Ludd's campaigns against the automation of cotton milling in Industrial Revolution-era England in order to benefit from a study of its tactical underpinnings. The core lesson of the Luddites (in tactical terms) is something different, perhaps even universally applicable: if we want to effectively attack a complex technological system, we seek a way to do so which requires minimal complexity and cost, in order to wreak maximum long-term damage. In other words, the monkey wrench.

Throwing a monkey wrench into a complex, delicate, interconnected system of gears and levers working at high RPMs causes spectacular, massive, permanent damage to the mechanism. The damage expands, building on itself: a gear breaks, and the broken pieces in turn smash other gears. An axle shears, its shattered components tearing out control mechanisms in their death throes. All from one small, cheap, anonymous monkey wrench.

Encryption is the systematic monkey wrench for modern surveillance machines. Not just any encryption, but widespread data-in-transit encryption coupled with IP-decoupling technologies and techniques. Together, these two joined approaches to network data security are deadly for highly-automated, top-heavy, billion-dollar global spy architectures. They serve to break the key conditions for such spy systems to work, making the systems vastly more expensive and unwieldy to manage and scale. They make such systems brittle, unworkable white elephants... too costly to run continuously, too ponderous to upgrade in the face of agile, crypto-based sabotage.

For The Win

It is easy enough to become despondent in the face of spy cartels demonstrating sneering, hypocritical contempt for civilian laws - and for democracy itself. How can a ragged band of data activists ever hope to face off against surveillance machines built with tens of billions of dollars, sheltered in military secrecy, spanning the entire globe? Isn't it hopeless from the start? And shouldn't we just keep writing letters to our congressdrones, begging them to "regulate" these un-regulatable spy cancers with laws they'll then contemptuously use (yet again) as mere toilet paper?

No, it's not hopeless. In fact, beating the power-mad spy-voyeurs is both easy and free of any need to break laws along the way. By viewing these systems as fundamentally economic (hat tip to Appelbaum again), we can see right away where they're most vulnerable. Change their cost dynamic - make automation difficult/expensive - and they become useless relics of a bygone era. Sure, they'll keep eating tens of billions of dollars per year - they'll keep growing and chowing through data - but the *output* they provide will become increasingly brittle, imprecise, uncertain, and useless. They can keep throwing queries at the DBs, but if we feed the DBs garbage, then we all know what comes out....

Despite the obvious, inescapable logic of such an analysis - I'm hardly the first to propose it, nor I hope the last - one rarely, if ever, sees these perspectives discussed outside of specialized, anti-surveillance technology circles. Why is that? Because, in a word, this analysis *works*. It provides a tangible, actionable, risk-free path towards our goal: viz, to "sabotage the system." As such, this approach brings fear to the hearts of military spy cartel kingpins and their enablers worldwide. Those of us who promote, publicize, and enable the deployment of solutions based on such approaches face harassment, persecution, and extralegal attacks for doing so. That, too, rather elegantly demonstrates just how effective these approaches are. Indeed, when our enemies ignore us, we're not perceived as a threat. But, when our enemies react to our efforts wildly, violently, and with panicked overreach... when this happens, we know we're doing something right. We know that we're bringing to them the fear of their own defeat. Just so.

Spread the word. Spread the technology. Spread awareness of how it works. Put your grandfather up on a secure network service of your choice. Set up your aunt's router with a good, open source OS and Torify its connection. Stick some solid SOCKS proxy addys in your buddy's browser settings. Spread the love, *compa!* The more we encrypt (and IP decouple) comms traffic online, the more we throw a nice, chunky, proud monkey wrench into the sick dreams of spymasters worldwide. Sabotage the system... so we can have a future that's free, open, diverse, and, above all else, healthy for our planet.

crossover : where metal and hacking met and mixed

by Brett Stevens
http://www.deathmetal.org/

Underground movements are by definition networks of people doing what is not officially approved of. This usually has a scent of some truthful or realistic activity that society refuses to endorse. Hacking during its formative era formed an underground, as did a related movement: heavy metal.

Born from a frustrated generic blues-rock band amongst a sea of similar bands, heavy metal arose when Black Sabbath began combining horror movie music with the heavy guitar rock of Jethro Tull, King Crimson, and Cream. The result displeased parents and the music industry alike by refusing to get on board with songs of love and peace. Heavy metal is the music of the brutal truth hidden right beneath the shared illusion of consensual reality.

As one early textfile writer said:

"One might call a headbanger 'dumb,' but nine times out of ten, the guy will survive the onslaught of political mindgames better than the smartest 'normal' person would. It is much harder for a 'headbanger' to be brainwashed by politicians because of the music he or she has listened to for years.... It is the true reason heavy metal, acid rock or whatever you call it, came around. To make people aware and to keep people from being brainwashed into mindless cyborgs that revolve around one who can afford the company."[1]

While this seems like an extreme statement, it is a parallel statement to the fundamental idea of hacking, which is that "information wants to be free." Free means an absence of unnecessary control. Early computational and network resources were controlled through software and social limits that hackers quickly obliterated.

In the same way, most of our society is kept under control. We are told that there are hard limits to reality where no such limits exist in actuality. However, it is perceived that these limits are necessary to keep society from falling apart. Back in the 1980s, one limit was a fear of heavy metal's grim and startling realism: sex, drugs, occultism, and distrust of authority.

Not surprisingly, hackers and heavy metal found each other. Not only were many hackers inspired by heavy metal nomenclature and its spirit, but others used the early network of bulletin boards and AE lines to transmit information about the music and to help each other find new music. The result was a fertile cross-influence between the two undergrounds, heavy metal and hacking.

"My primary exposure to music through BBSs in the 80s was through two AEs. On the west coast there was Dark Side of the Moon (408-245-SPAM). On the east coast there was the Metal AE (201-879-6668 PW:KILL). Until then, my only music exposure was via early MTV (A Flock of Seagulls) or Houston classic rock (Beatles). Dark Side exposed me to industrial and EBM bands such as Throbbing Gristle and Ministry (and its offshoots). The Metal AE was pure metal. The Neon Knights text file group also released most of their files there first so you would occasionally find files like 'How to Fuck the Dead' among Metallica S.O.D. lyrics," said Reflexive_Arc, a third coast hacker known for penning anarchy files and deep penetrating of academic networks during the late 1980s.

Hackers named their groups after metal themes. Groups were how hackers associated to share information that was not for general public consumption, but which could aid them in pursuing individual learning and accomplishments. Two hacker groups who openly displayed their influences from heavy metal were the Neon Knights, named after a Black Sabbath song, and the Cult of the Dead Cow, who use the slogan "Bang the Head That Doesn't Bang," which was borrowed from the back of Metallica's 1983 debut, *Kill 'Em All*.

Hackers also wrote about heavy metal in textfiles. Textfiles were both the newspapers and the research libraries of hackerdom, often including high-density material like technical instructions on equipment or software, but also containing lighter fare. Designed to be transmitted quickly, they were often short and written in an information-heavy and effective style. To a textfile writer of the past, blogs today would be both wordy and low in content. Both the Neon Knights and Cult of the Dead Cow published both metal-themed textfiles, such as lyrics files, and textfiles on other topics which would frequently use metal lyrics and imagery, although they were not the only two groups to do so.

Some hackers named their boards after heavy metal. The Metal AE was an Ascii Express line, or a board with no usernames and a single password for access. These types of "remote" systems were basically file servers, allowing users to anonymously upload or download files. To send a message, you typed it into a text file and uploaded it with a filename created from the name of the person you wanted to receive it and the subject of the message. Hackers from all over the world popped into the Metal AE for its plausible deniability, active user base, and steady stream of fresh textfiles[2]. The hacker named The Mentor, whose lengthy screed "The Hacker's Manifesto" was used in the movie *Hackers,* mentioned the BBS "Metal Shop Private" as having "a metalhead or two" on its staff. As Erik Bloodaxe of Legion of Doom and later *Phrack* e-zine pointed out, the name of the board was derived from a radio show, "Metal Shop," hosted by DJ Charlie Kendall from 1984-1995.

In addition, many hackers enjoyed metal. Bloodaxe said, "My life's ongoing soundtrack back then was Metallica, Queensryche, Iron Maiden, Judas Priest, etc."

Grandmaster Ratte', a longstanding member of the Cult of the Dead Cow (cDc), said his group was very influenced by metal. "I'd say within cDc, appreciating metal aesthetics is almost universal. Though we draw from other wells too," he added.

It's hard for us to remember then how hard it was to find information about music. The average city had two chains of record stores, a Sound Warehouse or Hastings and Sam Goody or Tower. These stocked releases from major labels, of which there were many, but these formed pyramids of ownership which tracked back to a handful of big media conglomerates. Thus, for all the variety that was available, there was no music that was not under their control and, as a result, some genres got excluded, notably metal, some Gothic music, industrial, and hardcore punk.

A dearth of music information made it hard to know what to even ask for, and even at one of the rare specialty record stores that ordered from smaller labels, if you did not know the name of an artist to request, it would never come your way. The major music magazines like *Rolling Stone* and *Spin* covered almost anything but metal for most of the 80s, and when they did cover metal, it was with scorn and bemusement. Academia and news media viewed metal as some sort of million moron march, and in popular entertainment, liking heavy metal was a signal for a character's clueless rebelliousness.

"Most of this music was beyond the scope of mainstream media at the time. Even MTV wasn't playing metal (other than hair metal) until years later," said Reflexive_Arc.

With the rise of the home computer, the affordable 1200 baud modem, and the bulletin board (or AE line), the average computer-savvy hobbyist could access information that others could not. At a time when CDs from Europe were tagged "imports" and sold for 40 percent more, and long distance calls across the ocean were prohibitively expensive, finding information on international music was difficult. Bulletin boards, however, had an international audience, even if many of that audience borrowed other people's long distance codes to get there. And unlike news magazines or music media, bulletin boards had no financial incentive to do anything but tell the narrow truth and leave the hype and deception outside.

Bloodaxe explained why the BBS was central to hacker culture. "In the 80s, BBSes were the most important thing to the hacker world. They were where people met, talked, exchanged information. They were the central meeting places where you could find those people who actually cared about the same things you cared about," he said.

The world created by hackers allowed users to find new music and spread it to friends through copies. "[I]n the early days before thinking about copyright infringement, we'd type up lyrics and upload them to the metal-themed BBSes. It was a common practice, because a lot of kids were trading tapes and didn't have access to album covers to read," said Ratte.

"We swapped video and audio tape-trading lists and traded a lot within our small community," said the hacker known as Mightypeniz. He referred to a bulletin board he had joined where he and the sysop found musical taste in common. He later founded his own BBS, "Blood Fire Death," named after the album of the same name by Swedish death/black metal pioneers Bathory.

"Most of the people in my peer group would be calling bulletin boards daily and were phone phreaks, so their long-distance calls were free. It was basically like being a regular on 4chan or Reddit, but 30 years ago. So we would talk about niche topics like metal that were very hard to find out about unless you, say, lived in a big city or college town and knew the right people/right places to go. Instead, you had access to people from all over the world, many of whom were very knowledgeable," added Ratte.

Even more importantly, there were parallels between hacking and the mental process of enjoying the more complex forms of heavy metal. Both were undergrounds, isolated from a society that feared and rejected them, which then required their users to find ways around the methods of control. However, as the hackers spoken to for this article revealed, there were internal parallels as well, both in the realm of similar spirit and similar types of complexity between the two.

"[F]or some of the more complex and extreme forms [of metal], there are a few parallels that could be drawn. Both require concentration and attention to detail, both rely on near blind devotion to achieve something interesting or truly worthwhile," said Simple Nomad, an Apple // hacker who specializes in forensics. "Both are about an underground person bending the rules, in some cases fairly severely from what society says is normal or acceptable behavior. Thing is there is large push for conformity in numbers even while rejecting societal standards," he added.

Ratte took more of a Nietzschean perspective. "I'd say they do have a similar spirit, but it's more nuanced. A lot of hacking is about solving tough problems, mostly by yourself, requiring intense effort and isolation. The metal that resonates the most with me has a similar vibe, where you feel the visceral impact of a difficult problem and the struggle to triumph over it. Eventually leading to victory or failure. The mindset of a hacker is inundated with this cycle day-after-day, so I think both hacking and metal are a natural fit," he said.

"To me that was one of the most interesting aspects of the music at the time - a source of inspiration for writing philes," said Reflexive_Arc. "I liked to picture someone in a dark room, in front of a black screen with 80 columns of green text, an intense song blasting in the background as the soundtrack for a phile on how to blow up the world. Within hours the phile snakes its way from AE to AE."

"Maybe it was just the 'in your face' teenage rebellion thing. Your parents hate it, so it must be cool. Also, young hackers tend to imagine themselves as renegades living outside the law, so the music associated with that at the time was certainly heavy metal," said Bloodaxe. Some time later, he elaborated: "I think there was just a natural cultural overlap as 'outliers' (like young computer hackers) went about finding ways to fit in with new people and make new friends. In my case, mix typical hormonal teenage rage against parents, teachers (or any authority), rules and laws perceived as arbitrary and stupid, groups like the PMRC saying 'this is bad,' etc., so once someone handed me a copy of Metallica's *Ride the Lightning,* it just sounded right to me in ways that nothing else at the time did."

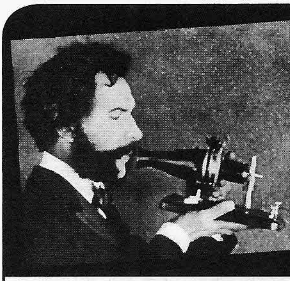
In a time when all music is a quick search away, and we wear more computing power on our wrists than those old big mainframes could pump out on a good day, we are drowning in an abundance of information. It is perhaps why this age is less friendly to any but the professional hacker, since any information that wants to get free has found a way and then been commercialized as a method of control, instead of using prohibition-based rules. Media has diversified and will gladly sell you any form of metal you desire.

And yet, the same problem remains. Sale is control. Popularity is control. And public opinion is control. As the next generation of hackers rebels against that tendency, they may find inspiration in the past, where hackers escaped control by setting up their own information network and using it to spread the word of heavy metal.

The author of "The Heavy Metal FAQ," Brett Stevens writes about underground death metal and black metal in addition to computer-mediated communication and information security. He began writing about music on the Metal AE and others BBSs, including his own "Apocalyptic Funhouse," uploading textfiles in the dead of night extolling the virtues of Slayer, and later branched out to the web, editing the oldest and longest-running metal site at the Death Metal Underground in addition to freelance writing.

[1] Starmaster, "Heavy Metal: The Untold Truth," January 25, 1990 (retrieved from `http://www.textfiles.com/music/➥metaltru.mus` on April 1, 2014) (as quoted in "Defending Metal Before the Internet", retrieved from `http://www.deathmetal➥.org/news/defending-metal-➥before-the-internet/` on April 1, 2014).

[2] Author's personal experience. I began writing about metal when I was uploading message files, lyrics, and reviews to The Metal AE. In many ways, it was one of the best audiences a writer could ask for: already primed for the subject matter and concise writing, they were heavily involved as readers.



TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! I am in sunny Southern California after several months of traveling around the world. I have enjoyed fine hotels and luxury travel from London to Los Angeles while researching some of my favorite topics, all on the company dime and never in economy class. The management lifestyle is definitely a cut above the union rate. I'm never going back!

I love the smell of a 4ESS tandem in the morning, but today, I'm standing in a new style of central office. It is what is known as a carrier hotel. Much like the Central Office tandems that remain as part of the old Bell System, it is a hub and interconnection point. However, this facility is for Internet carriers, many of which are also long distance phone companies. They all pay to exchange traffic here, and there are efficiencies to be achieved.

Bell facilities were built to exacting standards and maintained nationwide according to detailed and consistent Bell System Practices. Bell System employees were generally unionized (some still are) and received extensive and exacting training. Most traffic between telephone companies is exchanged at specialized offices called access tandems. These are carefully managed and run by dedicated staff, most of which have extensive telecommunications experience.

Carrier hotels are a much different type of facility than a traditional Central Office. These are operated by private Internet companies, and while *some* operational aspects are consistent, there isn't anything approaching the management rigor of Bell System Practices. The three largest companies, who operate most Internet interexchange points, are Equinix, TelX, and Coresite. These facilities can be very large. For example, One Wilshire in Los Angeles, one of the densest carrier hotels, hosts more than 260 different Internet service providers exchanging traffic within the facility.

My employer recently acquired a carrier hotel and assigned me to a project to achieve additional efficiencies. All of my usual management tricks didn't apply. I like to streamline processes wherever possible (leaving a paper trail could be bad for my bonus in the future), but I found out that the engineers who manage peering often turn up circuits based on just a few email messages. Sure, security procedures are theoretically in place, but the guys all know one another, so what's the harm? In 2010, a single routing error (using the Internet equivalent of SS7, which is called BGP) routed 15 percent of the world's Internet traffic through China until it was corrected 18 minutes later. These sorts of errors happen all the time, but I correctly recognized that there is no real harm to the business, so I have streamlined security procedures even more. For the most part, security is an unnecessary cost. After all, for Internet service providers with more than one connection, TCP/IP is largely a self-healing protocol. Even if traffic is routed through China, it still gets there eventually and it doesn't really cost any more, even if you misroute traffic halfway around the world. This is much different than a similar SS7 error, which would inevitably result in a flurry of debit memos (assuming the unwitting recipient of the erroneous traffic has configured their system to complete the call, which is usually the case). There is an exception for smaller providers, who are often connected to only one "upstream provider." A single routing error could put them out of business, so more testing is done before "flipping the switch" to ensure that changes are accurate.

I next looked at HR to find out whether I could save money by firing better paid older workers or breaking a union. Unfortunately for me, I discovered the average age of the staff in the facility is 21, they are all non-union, and the average wage is about $10.50 per hour. It's hard to wring many cost savings from this, but I still found some. As it turns out, management brings in new hires from the local technical school. A grizzled old hand complained bitterly, and told me they don't really know what they are doing. Customers complain of constant issues with people unplugging the wrong things or damaging things while trying to work with them. And the company had to pay compensation! I had been tuning him out until I heard this, but the word "compensation" definitely got my attention. I had found something to streamline! As it turned out, our contracts promised a particular service level that implied our staff was competent and even provided compensation for errors and omissions on our part. I instructed the legal department to update our contracts to promise that we would provide service "in good faith" and based on "best efforts." They also helped me with new compensation clauses. I opted not to entirely eliminate promises of any particular service level or response time, because customers demand these clauses in the contract and competitors would gain an advantage if they didn't exist. Instead, I just watered down the clauses to the point where they are effectively meaningless. I love "new" and "updated" contracts - they always mean a bigger bonus! I laid off the grizzled old hand. He was a great engineer, but he was twice as expensive as the kids, spent most of his time posting on the NANOG mailing list, and our new contracts meant we didn't need anyone competent anymore. I then boosted sales by updating our sales program to promise expert 24x7x365 service while also raising our rates. Our customers have no idea they are paying more and getting less.

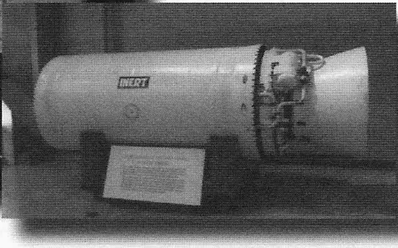
Finally, I helped the company with a very successful "green initiative." The carrier hotel was hot and uncomfortable, with temperatures reaching up to 100 degrees in the "hot rows." However, I observed that July temperatures in Phoenix are as hot as 130 degrees so there was room for our facility to be even hotter! Obviously, if a major city in the United States can be 130 degrees in the shade outside, so could our carrier hotel; I believe this is a fully justifiable position to OSHA. I immediately instructed that the air conditioning be turned down, raising indoor temperatures to 130 degrees. A couple of the kids turned green and threw up, so I saw immediate green results. We are saving a fortune in electricity costs and the environment along with it! I will hopefully receive a larger bonus for my environmental stewardship. Sure, it's bad for the equipment hosted in our facility, but it's not *our* equipment and there is nothing in the contract guaranteeing any particular temperature.

And with that, I declare our newly acquired carrier hotel streamlined! I have improved profitability by seven percent with a few simple changes. If you complain about warm weather this summer, think of our employees toiling away in 130 degree temperatures and consider that if I were your manager it could be you! I will be at Defcon and HOPE this summer, and will look forward to meeting all of you and exchanging ideas about success. For now, I will enjoy the ice cold air conditioning in my brand new car. Management life is the best!

References

- `http://bellsystempractices.org/` - Complete text of Bell System Practices.
- `https://www.youtube.com/watch?v=8Rs0n97qC_w` - Video of the fourth floor "meet me" room at One Wilshire in Los Angeles.
- `http://www.nanog.org/` - NANOG, an organization of grizzled old hands who work at Internet providers and carrier hotels. Without these folks, there would be no Internet.

Fun With the Minuteman III Weapon System – Part Three "AHC Chicken"



by Bad Bobby's Basement Bandits

Welcome to Part Three of fun with an active Minuteman III nuclear weapon system. In Part Two, we examined how to intercept basic nuclear missile communications, and how different trips communicate with the transportation center and the missile flight security controller using the VHF radio. Finally, we examined the various radio communication scripts and learned how we may begin to put together our VHF radio hacking library.

As usual, I have received feedback from Part Two. I was able to speak with active and retired Minuteman III nuclear missile officers (otherwise known as "Crewdogs"). Some Crewdogs thought that I should have discussed the concept of frequency hopping as it relates to VHF radio transmissions. We all agreed that having a properly tuned trunked scanner would be the best way to intercept the VHF radio transmissions today.

A lot has happened in the Minuteman III community since Part Two was published. It appears to this author that a great portion of the ICBM community is attempting to self-destruct. A two star general, who was an active commander of the Minuteman III nuclear force, has been fired because of his unusual behavior while performing temporary duty in Russia (excessive drinking, beautiful Russian girls aka spies, etc.). Eleven Crewdogs were found to be involved with illegal drugs. Initially, 34 Crewdogs were caught cheating on a Top-Secret Emergency War Order (EWO) test. The Air Force investigations continue and, as of today, the number of crew dogs caught cheating on the top secret EWO test is closer to 100. The drug investigation has gone dark with no further information being released.

Today I'm going to put on my white hat. We will be discussing how any civilian can establish a communication link to be able to hack into any Minuteman III ICBM nuclear missile computer. This will be accomplished by completely bypassing the Launch Control Center - the place that usually controls all communications having to deal with Minuteman III missiles. The main purpose for discussing this information is to show that even the most secure, unattached to the Internet system can be hacked as a result of owner/operator carelessness. The secondary purpose for exposing this information is so someone else in authority with the Air Force or government will read this and take the necessary steps to stop Crewdog buffoonery with the Airborne Launch Control System Holdoff Command (AHC).

Usual disclaimer: All of this information is unclassified. Standard disclaimer: For information purposes only. Do not do any of this.

First, some brief background information. Both the Minuteman III missile and its associated Launch Control Center (LCC) each have their own computer. These computers handle the bulk of the communications back and forth between the missile and the Launch Control Center. Every six hours, Crewdogs in the LCC must initiate the Airborne Launch Control System Holdoff Command. This command is intended to be sent from every LCC to every Minuteman III nuclear missile, no exceptions.

The AHC command was built into the Minuteman III system during the dark days of the Cold War. The idea was if any launch control center was destroyed by an enemy missile, there needed to be a way for United States forces to launch any remaining Minuteman III nuclear missiles. At the end of a certain amount of time, if the Minuteman III missile does not receive an AHC command, the missile computer switches on its UHF radio so that the missile can receive communications through its UHF radio. Sooner or later, an E-6B from the 624th Strategic Operations Squadron (containing the airborne launch control system) will fly by and Crewdogs in the aircraft will begin to communicate with any Minuteman III missiles that are in the UHF mode. Of course, in a time of nuclear war, they will be sending UHF commands that will cause the missile to launch.

There's something about pulling a lot of alerts in an underground nuclear Launch Control Center that eventually makes some Crewdogs do crazy (and dangerous) things. One of the crazy things that some Crewdogs do is play the "AHC Chicken" game. The goal of the AHC Chicken game is to see who can get the AHC command sent out to the missile as close as possible to the six hour timer without having it expire. Since the AHC timer clock does not report fractions of a second, then the winner of AHC Chicken would send the AHC command to the missile at one second before the six hour timer expires. There are five launch control centers in each squadron. To play AHC Chicken, two or more launch control centers will get a chance to run the AHC command. This game takes twelve or more hours to play. At the end of twelve (or more) hours, the launch control center with the close0 st time to zero on the AHC timer is the winner. If a mistake is going to happen, it is usually going to be at the 18-hour point (usually at about three or four in the morning). A mistake is made when the AHC command is not sent out and all the missiles go into the UHF mode (or RADMO).

A wild guess is that the 0 AHC Chicken game is played about two times a year in any given nuclear missile wing. Generally, Crewdogs are quick enough to catch the mistake and run the AHC command within a few seconds. On other occasions, Crewdogs have left nuclear missiles in the AHC mode for nearly four hours. Of course, Crewdogs get in big trouble for having done this.

The materials we will need for this hack will be a tuned 40+ watt UHF transceiver and a DTMF0 tone generator. The purpose of this hack is to demonstrate that a civilian with no nuclear missile knowledge or experience can obtain electronic access and communicate directly with a Minuteman III nuclear missile computer by way of its UHF receiver. There is no danger of launching the nuclear missile since only the President and National Command Authorities actually have access to the real nuclear missile codes. This hack just feeds electronic gibberish to the nuclear missile computer. This hack demonstrates electronic access to a nuclear missile, nothing more.

We all remember from our "Radio 101" course that the UHF band operates in the line-of-sight mode. This means that our UHF transceiver must have a fairly clear line of sight between the operator and the nuclear missile site. We want to get close enough to the nuclear missile so that our UHF transceiver is able to make contact with the missile, but not so close that we can be picked up on the missile site security cameras. Once we are set up, all we need to do is set our UHF transceiver to the frequency of the Minuteman III nuclear missile computer's UHF receiver. The frequency of the Minuteman III nuclear missile's UHF receiver is set at.... Okay, I can't tell you the actual frequency(s) because they are classified. However, a communications link can be established by stepping through UHF frequencies while transmitting random DTMF tones. We really only need to have a couple of random tones register on the missile's computer for proof of concept. And there you have it! A. very. cool. hack.

I don't know why nuclear missile wing commanders do not take steps to completely stop the Crewdogs' ability to play the "AHC Chicken" game. It has been going on for more than 30 years. By highlighting this hack, it is my hope that nuclear missile wing commanders and politicians will take the necessary steps to shut down the Crewdogs' ability to play "AHC Chicken" immediately. This will also ensure that no hackers/civilians will be able to communicate with a nuclear missile.

(Bad Bobby has spent more than 6,500 hours on alert in the Minuteman III Nuclear Weapon System. Next time, Bad Bobby will wear his White Hat (again) as we examine the Enable codes for the Minuteman III nuclear warhead!)

FUN WITH DATA ENTROPY ATTACKS

by Spacedawg

<insert standard disclaimer here>

Today compression is used everywhere. Most modern file formats, networks, and computing systems are optimized to reduce waste of space in buffers, memory, and storage. The level of sophistication of this compression varies, as does the value of that compression in certain situations. In this article I will explain how one can use knowledge of these variances to gain advantage over a target system by bending and breaking the rules.

high entropy = bad time for compression

In general, data entropy is simply a measurement of order in a block of data, so to say data has a high order of entropy is to say the data is in a low ordered state such as a block of truly random generated data. Conversely a block of raw ASCII alphanumeric text would be said to be in a low entropy state, and is suitable for compression by an appropriate algorithm. This is true for all types of *raw* representations of data, sound, video images, all of which have vast ordered, yet repeatable data patterns in their structure. So what about encrypted data? It appears random externally, yet has a high order of structure - only to the parent cypher algorithm when accompanied with the correct keys. To any compression algorithm encrypted data is indistinguishable from random data and is high entropy. As a result, it is a common rule to do all compression steps on a data block before encryption, in order to reap the benefits of size reduction and security from both algorithms.

The order of data entropy is measured against the process it is being run through.

How is This Useful for Hacking?

With this in mind, if we create a large, low entropy data block with highly structured layout suited to a high compression ratio, and inject it into a system that uses even the most simple compression, we can transport a huge amount of data to the target in a short time that, on reaching its destination, will expand to rapidly fill buffers, memory, and even petabytes of hard drive space on an unsuspecting target. This is similar in method to the recent DNS vulnerability where exploited code was used to flood the buffer of the target until the network failed - except we are using the system's own compression to transport our generated data. So what is the lowest entropy data structure we can fit into 10TB that almost any compression algorithm can reduce to almost nothing? It's simple, how about 10TB of 0s!

Real world example 1 - Practical example: Free stuff on FTP.

Disclaimer: I'm not proud of this, but at the time it had to be done. Back in the day, before file sharing programs like BitTorrent and Napster, people mainly shared files by setting up local FTP servers. Users would connect to these FTP sites, upload media files requested by the server owner, and an automated script would keep count of the files uploaded and then offer the user download privileges based on a ratio of the data uploaded, usually 2:1. So me living in the back end of nowhere with a dial-up 56k modem and an ISP dial-up rate of 10c per minute (no free local ISP calls in my country) and no files to trade could not really play by the rules. So....

Step 1: Open mspaint.exe.

Step 2: Make new image, increase canvas size to several times the screen size.

Step 3: Save as 24 bit uncompressed bitmap file (lots of 0s).

Step 4: Check file size, increase canvas, and re-save until file size approached 5MB.

Step 5: Write "sorry" on the bitmap (it doesn't affect the entropy much).

Step 6: Rename the file from "untitled.bmp" to "Britney Spears - Hit Me Baby One More Time.mp3".

Step 7: Upload the file to the FTP server over the 56k modem at >300KBPS (!!!!).

Step 8: Quickly download files (at normal speed) from FTP before the owner finds your corrupted mp3 and boots you.

I learned the modem's simple compression was able to take packets of 0s and say "30 0s" instead of "000000000000000000000000000000" and upload my payload at a fantastic speed. If you were the owner of any of these FTPs, I hope you found the BMP header data and my embedded apology. I'm sure this type of entropy attack could be adapted to be used effectively in modern DDOS, network exploit, and fuzzing attacks.

Real world example 2 -
Hypothetical example:
Utilizing high data entropy to protect Internet privacy.

We now live in a world of almost total surveillance. As individuals, most of the gigabytes of data that typically travels in and out of our broadband routers (streaming videos, music, app downloads, etc.) is quickly indexed and the redundant data is discarded by the man in the middle. The bulk of the data that we send and receive that is personal, unique, or creative is relatively small, unencrypted, and easily stored for processing. Smaller still is the average user's encrypted traffic that can, and is, collected, sorted, filtered, and stored indefinitely. Encrypted traffic is difficult to identify specifically using deep packet inspection methods. Instead *all* unknown, high entropy traffic is interpreted as being encrypted data and is *all* collected and saved for processing and decoding at a later time. This is something we can work with....

Raising the Signal to Noise Ratio

If there were a peer to peer network that did nothing but send a stream of meaningless high entropy data to participating nodes on the Internet, the storage capacity requirements of those who would hold all of our private communications would need to be dramatically increased. This also breaks the web of association that those watching us like to draw between individuals as it appears that we are all always connecting to one another through small intermittent encrypted channels. The data could not be simply ignored or discarded, because some users can still embed real encrypted messages in the data stream amid the overwhelming noise. While these encrypted communications might still be deciphered, the job of identifying encrypted traffic interlaced within a high entropy data stream just became a painstaking, manual process, prone to false positives and wasted resources, perhaps to the point of mass surveillance becoming a financially inviable endeavor.

Shoutout to Crunchman, Dublin 2600, and the TOG Hackerspace crew.

Network Condom

by Sh0kwave

The Internet is full of STDs - make that malware: exploit kits, drive-by downloads, redirects, cross-site scripting, malnet nodes. (Try nmap on 221.130.179.36.) If you want to do a little exploration of the seedier side of the Internet, it makes sense to take precautions. Use a little protection, as it were.

This little Python script lets you explore safely. You won't be using a risky web browser - you'll be making raw network socket connections. Honestly, you can do something similar with netcat, but if you want to dip your toe into Python, and you don't want to enter a bunch of long command lines, give this a try.

Create a file called "NetCondom.py" and enter the following:

```
import socket

ip = raw_input("IP: ")
port = int(raw_input("Port: "))

try:
    s = socket.socket()
    s.settimeout(5)
    s.connect((ip, port))
    s.send("HEAD / HTTP/1.0
➥\r\n\r\n")
    result = s.recv(1024)
    s.close()
    print str(result)
except Exception, e:
    print str(e) import socket
```

Save it, then run it with: `$>python ➥ NetCondom.py`

When prompted, enter the IP address and port you want to explore, and see what you get back. Whatever it is, you won't infect yourself with malware because it is just going to be a string.

How do you know what to explore? Try some scans with nmap: "nmap -sV {ip-range}".

How do you find an IP address from a URL? Use nslookup, or dig: "nslookup www.google.com" or "dig www.google.com".

Happy, safe, exploring!

Yippie Ki-Yay: Social Engineering and Film

by Gregory Porter
http://backfromthemovies.blogspot.com

Social-engineer.org defines social engineering "as the act of influencing a person to accomplish goals that may or may not be in the 'target's' best interest." [1] Convincing a user to divulge his or her password is a commonly cited example that illustrates the definition but also brings to light the relationship between social engineering and computer security. Social engineering is, at its core, persuasion, but the term emphasizes a relationship between an individual (the engineer, if you will) and a target, be it a system, an individual, or a situation. Although elements of social engineering exist in every facet of life, there is a tendency to relegate the practice to computer security and, in doing so, one may fall victim to the practice. This article will discuss the presence and implications of social engineering in film.

Overt examples of social engineering fall under the term of "propaganda." Consider the Nazi film *Triumph des Willens* (*Triumph of the Will*). The message is as clear as someone commanding, "give me your password." Bugs Bunny also participated in this practice, though with a different audience in mind. [2] The idea, of course, is to persuade the audience to support the Nazi party or "buy a little bit of Freedom (on sale at this theater)."

Although propaganda doesn't often reach WWII levels, there are still elements of social engineering throughout modern films. Consider the classic action movie *Die Hard*. Although it came out in 1988, its characteristics are indicative of mainstream, blockbuster action movies. Although it might not be persuading the audience to do something, it is subtly reinforcing social assumptions held by the audience.

First, the idea of "normalcy" must be defined. In a blockbuster movie, there is a general story arc. A family unit (a white, heterosexual, middle class couple with maybe a child) is disrupted by some outside force. By the end of the movie, the male protagonist triumphs and brings us back to normalcy. That is, he preserves the family unit. Each of these qualities, white, heterosexual, male (for the protagonist) serves to connect with the audience, the majority of whom are white, middle class, and, as this is an action movie, male. This very concept of normalcy is an element of social engineering. The movie is taking the majority's definition of "normal" and replicating it to draw you into the movie and, more importantly, into the movie theater.

John McClane is a detective from New York. He and his wife, Holly, separated six months prior to the start of the movie. He explains what happened to Argyle, his African American limo driver: "she had a good job that turned into a great career." He had a six month backlog of criminals he was trying to arrest, so it wasn't "easy to just pick up and go." "In other words," says Argyle, "you didn't think she would make it here, so she'd come crawling back to you, right?" "Like I said, Arygle, you're very fast," responds McClane.

The limo arrives outside Nakatomi Plaza, a name that highlights the economic climate in the late eighties/early nineties, namely that Japanese corporations were moving to America. This notion of the Japanese corporation links to the McClane couple through the gift Holly receives for being the best employee: a gold Rolex watch. Before long, Hans Gruber, a former West German radical, and his other "Eastern European terrorist" cohorts take over the plaza and, not long after that, McClane defeats them.

Given that *Die Hard* premiered a year before the fall of the Berlin wall, the decision to make the villains German is not a coincidence. It's a common theme throughout movies. Who was "the enemy" during WWII? Nazis. Who was "the enemy" during the Cold War? Communists. Who is "the enemy" now? The umbrella term "terrorists," though it is often specified "Middle Eastern Terrorists."

In the climax, Gruber is holding Holly hostage. McClane quickly pulls out a gun and shoots Gruber, who begins to fall out an open window. He holds onto Holly's wrist. McClane hangs onto his wife and unlatches her Rolex causing Gruber to fall to his death.

What is going on in this scene? The white male saves the damsel in distress but how? He takes the watch off her wrist. This symbolizes her removal from the professional world. The couple is reunited and we return to normalcy; the couple is back together, the woman is at home with the kids while the man earns a living.

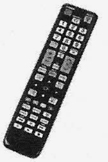
To what end is this social engineering? When we consider the subject in computer security, it is an inherently disruptive act. As the example of *Die Hard* demonstrates, there is actually an effort to maintain the status quo. A computer engineer may say "give me your password," a blockbuster film seems to say "keep your password." This analogy, however, is false.

Consider the previous discussion of normalcy. Films, especially blockbuster films, create a fictional world based on the preconceived notions held by the audience to, then, draw in the audience. If the majority of the audience saw that world as black and white, the movie's world would probably be black and white as well. Movies are often considered an escape, but from what? They are often considered an escape from trouble, confusion, or complexity. *Die Hard* may seem to be a simple action movie about the good guy fighting the bad guys, but its success must attest to its ability to address the audience's attitude about social and political issues. This can be considered social engineering because the film is presenting a fantasy as something rooted in reality. This fantasy reaffirms potentially false notions held by the audience, thereby propagating another level of fantasy.

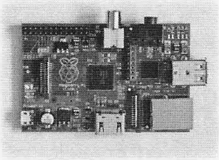
Consider the images projected before you the next time you watch a movie. What ideas about the world are presented with a matter of fact tone? What assumptions are being made for the sake of the story and are those assumptions significant?

Sources:

- `http://www.social-engineer.org/`
- `http://www.youtube.com/watch?v=_TUPUbvO0eU`



HACK YOUR HOUSE MAKING THE MOST OF RASPBERRY PI



by Michael Post

After recently moving, it was soon realized that my home that has been abandoned for approximately 15 years was going to need some serious TLC - first and foremost being water and power. Water was a breeze: run some pipe, call the city. A few days later, voila - water. Power, on the other hand, was a bit different, replacing fabric wrapped wire with proper wire, replacing fuse boxes with a breaker box, a new meter box just so the power company would come out to turn it on. Once that was done, I felt pretty comfortable dealing with AC power.

So I decided to introduce my house to the Raspberry Pi. First was to decide on an OS for the Pi. After a little consideration, I decided on Raspbmc - main reasons being, first, I was already running MediaTomb on my laptop and, although the Pi is a little light on processing and RAM, it thus far has made an excellent head unit. Second was hardware - what would I have to buy, what could I fabricate myself, and how much would it cost? Lastly, and quite possibly most importantly, what would be the best way to communicate with the GPIO pins on Pi?

Raspbmc requires very little to no configuration to get up and running and plays all matter of file format streams. Plus there is pre-built smartphone apps for iOS and Android, very convenient for couch sitting, or armchair, if that is your thing.

On to the hardware. First, the Pi was going to need power. I figured probably the more the better, so I chose an LM2596S. It can take from 36v in and step it down to 1.5v and is rated up to 2A. It seemed to be a pretty good choice at the time and I haven't been disappointed. Any old power supply will do. I have a 12 volt, 2.67 amp power supply and it works fine with the converter and the Pi. It will power all nine pins I'm currently using plus the Pi and USB keyboard at 5.5 volts input, so that is a great thing. (I'm not sure if a regular cell phone charger can power the above without a voltage drop.) Second, I needed switches. The first set of solid state relays I bought was from SainSmart on Amazon for about $16. The next two I bought were knockoffs at $8 apiece, but, as far as I can tell, they're just about identical. All three have four inputs, four outputs, and run on 5 volts. Lastly was wire and connectors. I used 14/2 wire (left over from wiring my house) for the lights to relays and some Plain Jane CAT5e for the GPIO pins to the input pins on the relays. I used female to female jumper wires cut in half and soldered to the CAT5e to complete the connection from Pi to relay, and I found some lever nuts to use between the lights, relay, and breaker box.

HTTP, the sweet jelly filling. After kicking a few ideas around my laboratory, I decided that for me, controlling the Pi via web page was the most ideal. Mostly, because writing separate apps for Droid and iOS seems time consuming and a little daunting. Now, with a little HTML and JavaScript, you can execute the commands needed to turn your GPIO pins from any device connected to your network that has a web browser via CGI scripting. My Pi was running Raspbmc which already has a web site used to remotely control XBMC. I added another step. I host my website on my laptop and execute the CGI scripts via SSH. My reasoning for this was to keep as much heavy lifting on the server side. Running cron to automate and run the full blown web server just seemed more reasonable. I didn't want my movies or music or whatnot to deteriorate because of programs running in the background on my Pi. So, to achieve this, first you need to create an RSA key for your laptop to your Pi, then write your scripts on your Pi end. There are a lot of ways to activate the GPIO pins on the Pi. I chose to just use bash scripting - it's quick and efficient. I also used shell scripting on the server end for the same reason. The Pi has three scripts: one to activate the GPIO pin, one to turn it on, and one to turn it off. The script to activate the pin is in `/etc/init.d` and looks like so.

```
#!/bin/bash

echo 24 > /sys/class/gpio/export
echo out > direction
echo 0 > value
echo 1 > value
```

The other two are in ~/ and are as follows. To turn the lights on:

```
#!/bin/bash

cd /sys/class/gpio/gpio24
echo 1 > value
```

And to turn them off:

```
#!/bin/bash
cd /sys/class/gpio/gpio24
echo 0 > value
```

On the server side, I have a lot of scripts, but there are four basic ones. The first two are in ~/.

```
#!/bin/bash

ssh root@<ip number of Pi> "
➥ /etc/init.d/<gpio activate
➥ script>
ssh root@<ip number of Pi> "
➥ ./<script for on or off> >
➥ /dev/null
```

The next two are the CGI scripts to execute the on/off scripts. I could have streamlined this and just written the whole script with the CGI scripts. I used the first two for testing purposes though, so I just left it as is. Most of the CGI scripts look as so. They are in **/usr/lib/cgi-bin**.

```
#!/bin/bash

# This first part keeps your
➥ browser from switching pages
➥ except on my iPhone still
➥ looking for a work around
➥ there.

echo " No content"
echo " text/plain"
echo ""

~/<script for on or off>

# this next part is here to edit
➥ my website that lets me know
➥ what lights are currently off
➥ or on
sed -i '5s/offbutton/onbutton/'
➥ /var/www/index3.html
```

That was the best way I could figure to get accurate feedback on what was currently on or running or not. In my opinion, sed is probably one of the greatest tools in any shell scripter's tool bag.

So what I ended up with was a PC that can run my lights, play streaming media on my TV, and, with a little creativity, run just about anything in my home. It cost me a little over $150 for the Pi, DC to DC power converter, 250' 14/2 electrical wire, female to female jumper wires, and lever nuts. The CAT5e and everything else I used I had available. To control every ceiling light in my house, I think it's a pretty cheap route.

CORPORATE SECURITY AND CHINESE HACKING
LESSONS FROM THE MANDIANT REPORT ON CHINESE ESPIONAGE

by Jim L

Last year a report was published that shines a light on sophisticated hacker techniques and how they have been successfully used in the real world. I'm referring to the Mandiant report called "APT1: Exposing One of China's Cyber Espionage Units." It can be found at `http://intelreport.mandiant.com` ➥`/Mandiant_APT1_Report.pdf`. It's a great report that shows how a foreign government used common and advanced techniques to pillage corporate databases. Given that corporate espionage costs billions of dollars every year, this report got my attention. When a threat is as well funded, planned, and executed as this one was, it gets labeled as an "Advanced Persistent Threat" (APT). This report looks at one particularly aggressive group affiliated with the Chinese military that it calls "APT1." Even when one excludes the political and diplomatic implications of such a sensitive topic, the report is still a great read for its detailed examination of how all the dirty work gets done. I think hackers and curious minds everywhere should read it over and see what can be learned from it. In this article, I'll summarize the findings of the report and offer some suggestions companies (and individuals too) can take to improve their security.

First, a little overview of how Chinese hacking has impacted U.S. companies, particularly companies in the defense industry. In the age of the Internet, cyber spying stands out as a gold mine of information acquisition, and this report shows why. The volume of attacks attributed to China has reached such a high level that the U.S. government considers it a threat to economic competitiveness. Industries hacked include those involved in energy, finance, aerospace, information technology, and automobiles. Intellectual property theft targets a variety of technological areas including defense and military technology. In 2009, it is believed that Chinese hackers stole token related technology from security company RSA which was later used to hack into Lockheed Martin's computer network. Indeed, Lockheed Martin may have lost information related to the newest stealth fighter, which could jeopardize lives and cost millions of dollars. One defense contractor, QinetiQ, was reportedly infiltrated and took little action to stop it even after repeated warnings from NASA and the NCIS. The network was compromised at every level for almost a year. As a result, investigators said that terabytes of data, including classified information relating to military robotics, drones, and the Army's helicopter fleet, including PIN codes that could now be used to identify helicopters' deployment and combat-readiness, were stolen. (Schwartz, 2013)

It is more than a little disturbing that the national security of the United States could be at risk from such security breaches. Many of the security breaches are downplayed by companies worried about their public image. However, the more such security breaches are kept hidden, the harder it will be to force companies to take security more seriously. Due to the persistent nature and broad scope of such attacks, one former Bush administration official feared we could find that some of America's most critical and expensive weapons technologies will fail to perform in a military conflict with China. While the Chinese government denies engaging in computer hacking, evidence to the contrary is mounting. The report by Mandiant stands out as one of the most well documented reports to date linking economic cyber espionage directly to the Chinese military. While the amount of public information related to IP theft and hacking could literally fill volumes of books, the Mandiant report deserves special attention because it consolidates the hacking problem into one coherent and well documented report.

The actor known as APT1 is believed to be the Second Bureau of the People's Liberation Army, Unit 61398. This elite unit recruits those with the background necessary to conduct hacking operations against English speaking countries. In addition to English language proficiency, the recruits for this group are also skilled in highly technical areas of information technology, including computer security. The unit receives large scale fiber optic infrastructure support from China Telecom, which cites its importance in protecting national security. The data stolen by this unit since 2006 is measured in terabytes and over 140 companies are known to have been targeted. The attacks are continuous and widespread over a range of industries. Once a target was successfully attacked, the unit would maintain a continued presence on the network for almost a year on average. The information targeted is highly technical and confidential - system designs, test results, business plans, manufacturing procedures, management emails, network architecture information, and user credentials. (Mandiant, 2013)

Anatomy of an Attack

This kind of cyber espionage requires the exploitation of vulnerabilities in existing computer systems and networks. Vulnerabilities can range from unpatched software to zero day exploits to social engineering. Not surprisingly, people appear to be the weak link that the Chinese are exploiting the most. Spear phishing is APT1's most commonly used technique. Why spear phish? Because spear phishing works! The methods used to perpetuate these attacks are a textbook lesson in computer security and hacking. Unlike many spear phishing emails, their emails use proper English to the point that it can fool well-educated targets. They even incorporate American slang to an extent. The emails originate from free webmail accounts and contain infected attachments or hyperlinks to infected sites. When someone clicks on the attachment or link, the malicious spyware is loaded onto their computer. Many of the malicious attachments used by APT1 have been zip files. This shows the importance of not randomly opening executable files from unknown sources. Once the zip file is opened, a user may see what appears to be an Adobe PDF file. However, the file is actually malware complete with an Adobe PDF icon. Most users won't look carefully enough at the file extension to see the .exe at the end.

Once the malware is opened, it installs a backdoor on the victim's machine. The backdoor is very useful to the attacker because it allows an outbound communication back to the malware's command and control (C2) server. These outbound communications are easier to get past a firewall than an inbound connection. The malware can send data back to the command and control servers or download additional malware. Multiple kinds of malware were used in the APT1 attacks. In fact, Appendix C of the Mandiant report (which details the malware used) is 153 pages long. Another indicator of the sophistication of the attacks (and likely government involvement) is that most of the malware was custom made to conduct these cyber-exploitation attacks.

Mandiant actually categorizes the malware into sections: reconnaissance prior to the attack, establish foothold and maintain presence, and complete the mission. A beachhead backdoor will establish a presence on the compromised system, gather system information, and lay the groundwork for additional malware. For example, it might open a Windows command shell, download and execute a file, and then sleep until it's time to be used again. This type of backdoor would likely be hidden in one of the initial spear phishing emails sent to a target computer. Once an attacker is in the system, other backdoors will be created and kept hidden - ready to be used if others are found and eliminated. This can make the network compromise persistent. One variant of this malware called WEBC2 can download HTML pages from a C2 server and look for special commands hidden between special HTML tags. After installation, the standard backdoors will begin doing most of the cyber espionage. The methods of exploitation include uploading and downloading files, taking screen shots of the victim's computer, logging keystrokes, creating or modifying programs, altering the registry, stealing passwords, identifying users, and even establishing remote desktop interfaces. (Mandiant, 2013) These backdoors will try to mimic routine network traffic in order to avoid detection. They may use names like "MACROMAIL" and "CALENDAR" to blend in.

As part of a standard hacking methodology, the APT1 attackers will employ privilege escalation to gain access to sensitive files and directories. They will dump hashed password files from the victim's network using such publicly available tools as cachedump, fgdump, mimikatz, pass-the-hash toolkit, and pwdump7. Once they have the passwords, they can use software to crack them. With cracked passwords, they can log on as privileged users and access even more data. As the attackers gain greater access rights, they can run basic Windows commands to explore the target systems. The commands can be manually typed or run all at once as batch files. These basic commands can yield important information about who is logged in, network configuration, domain information, accounts that exist on the network, which accounts have administrator privileges, and currently running systems services. At this point, the attackers can move laterally around the system gathering and stealing information.

They will also install multiple backdoors so that if one is discovered and removed, there will be another waiting to be used. Once these attackers have stolen a user's account name and password, they can impersonate that user over the company's VPN or webmail connections. The group would also steal email using GETMAIL and MAPIGET. These utilities allowed them to steal email from PST archives as well as directly off the MS Exchange servers. As they mined the data, APT1 would archive it using the proprietary RAR format. The archived files would be broken down into manageable 200 MB portions, encrypted, and sent back to the C2 servers. By encrypting the data that is sent back, they make it impossible for companies to know exactly what was stolen.

How can one be certain these attacks really originated in China? Fortunately, Mandiant also provides documentation of the worldwide Internet infrastructure used by APT1. Mandiant could observe APT1 activity after it hit U.S. servers and then trace it back to servers originating in China. Although APT1 used various server hops in countries all over the world, the attacks could be traced back to four major networks in Shanghai. These hop points can make it appear that the attacks originate in countries other than China. APT1 will create these hop points by compromising networks in various countries and then using them as launch pads for attacks against their ultimate objectives. Incredibly, Mandiant was able to observe APT1 as it logged into some of its compromised hop points. It captured 1,905 instances of these logins that utilized 832 different IP addresses of which 98.2 percent originated in China. (Mandiant, 2013) By capturing the IP address ranges from which the attacks originated, Mandiant could see that most of them were registered to China Unicom Shanghai Network. The registration information even included contact information. Because APT1 utilized Remote Desktop protocol, they inadvertently disclosed details about themselves. For instance, the keyboard layout was observed to be "Chinese (Simplified) - U.S. Keyboard." The IP address originations and the keyboard layouts are good indications that the attacks originated in China by Chinese speakers.

APT1 also utilized C2 servers and DNS servers to facilitate the espionage. Some of these C2 servers utilized by APT1 were examined. 709 of them were in China and 109 were found to be in the U.S. These C2 servers used various protocols to facilitate the hacking: FTP for file transfer, web, RDP for remote control of a system, and HTran for proxy. The DNS servers allowed APT1 to use Fully Qualified Domain Names (FQDNs) instead of hard coded IP addresses. An IP address could be blocked or shut down, but by using a FQDN and reconfiguring the DNS servers, APT1 could maintain their connections to compromised networks. All that was necessary was for APT1 to point the FQDN to a new IP address. Some of the registration addresses have been found to be fraudulent. Others had been hijacked. In either case, APT1 has used the TCP/IP based Internet infrastructure to establish a cyber-espionage architecture that is vast and persistent.

Common Sense Security

A strong corporate security policy cannot prevent all attacks, but it can make them much more difficult to conduct. In fact, common sense security policies that are already standard practice in the IT community today could have prevented much of the theft that has occurred. There is simply no reason for a business entity not to address the methods employed by APT1 when developing a security policy.

Business and government entities (especially those working on sensitive technologies) should conduct periodic reviews of their security landscape with an eye toward spotting vulnerabilities and unsecured access points. These reviews should also look at employee training programs, current backup and disaster recovery procedures, change management policies, network architecture, firewall policies and rules, wireless access points, use of encryption, remote access, and other areas of vulnerability. These reviews will help develop and maintain a comprehensive security policy that is implemented through strict corporate procedures.

The case of APT1 shows that poor decisions made by employees can open the door to cyber intrusion. One of the simplest things a company can do to protect itself is to train employees in the basics of information security. If you work in corporate security, train your employees not to click on unverified hyperlinks, to be suspicious of emails from outside the company, and not to open documents in emails that they are not expecting and from people they do not know. They need to understand that email addresses can be spoofed and that some attachments can be dangerous. If employees had been more vigilant about opening email and clicking on links, many of the attempts by APT1 to gain network access could have been prevented. It is also fairly simple and inexpensive for a company to adopt strong password policies. The stronger the password, the less likely it is that it can be cracked using brute force attacks. Also, by forcing employees to change their passwords every 90 days and preventing the reuse of old passwords, hackers who have stolen a password will be kicked out of the system after the password expires. Make sure employees know whom to contact if they do notice suspicious activity. That way, security has a chance to stop an attack before it can succeed.

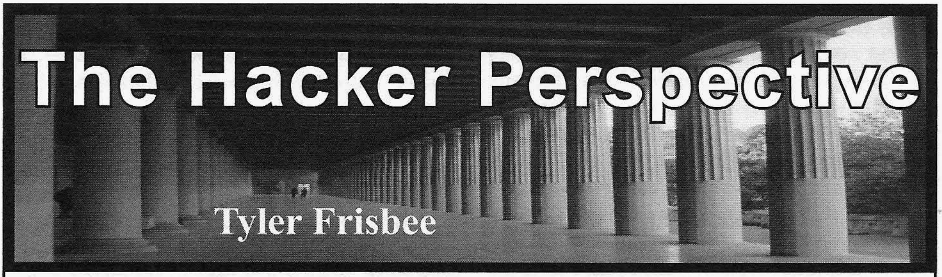
Strong email and spam filtering protocols should be implemented to prevent phishing emails from arriving in the first place. It would also make sense to initiate polices that prevent employees from sending company files and data through unencrypted private email accounts, especially free ones. Corporate data should stay on the corporate network. With good training, an employee should immediately be suspicious if a manager is sending attachments or links from a non-work-related email account. Companies and government entities should also implement multi-factor authentication through the use of security tokens. The tokens generate random numbers that are synchronized with a remote server and change at regular intervals (such as every 50 to 60 seconds). When the employee attempts to log on he must type the randomly generated numbers into the logon screen. If the numbers match what is on the remote server at that time, he is allowed access. In addition to the token generated numbers, the employee should also have to provide a PIN number that only the employee knows. That way, a hacker who steals the token will still not be able to log in even if the logon ID and password are known. In order to log on remotely, the employee must have a user ID, password, PIN, and token generated random number. This type of multi-factor authentication should be used for remote VPN access as well as webmail access.

Other standard security precautions all companies and individuals should take include maintaining up to date and effective patch management policies. It should be assumed that all known software vulnerabilities will eventually be exploited, so all software patches for both operating systems and applications should be applied regularly. Antivirus definitions should be up to date and scans should be run regularly on the network and against all files downloaded from the Internet. Firms should use IDS and IPS systems both on the network and on individual hosts. They should develop and enforce strong authentication protocols for VPNs and remote access. To help prevent data loss, laptops should have full disk encryption. Companies should practice good wireless security by scanning for and shutting down rogue access points. The latest wireless security protocols, such as WPA2, should be mandatory. The most sensitive parts of the network should be inaccessible to Wi-Fi devices. They should also conduct frequent penetration tests against the network to highlight vulnerabilities.

I learned a lot about hacking and security from this report. It should be of interest to hackers, security professionals, and anyone else interested in keeping information safe in a cyber-world.

Bibliography

- Elgin, M. R. (2013, May 02). China's Cyberspies Outwit Model for Bond's Q. Retrieved from *Bloomberg*: `http://www.bloom` ➥`berg.com/news/2013-05-01/` ➥`china-cyberspies-outwit-u-s` ➥`-stealing-military-secrets` ➥`.html`
- Huntsman Jr, J. M., Blair, D. C., Barrett, C. R., Lynn III, W. J., Gorton, S., Wince-Smith, D., et al. (2013). The Commission on the Theft of American Intellectual Property. United States of America: The National Bureau of Asian Research.
- Mandiant. (2013). APT1 Exposing One of China's Cyber Espionage Units. Alexandria, VA: Mandiant.
- Nakashima, E. (2013, February 10). U.S. said to be target of massive cyber-espionage campaign. Retrieved from *Washington Post*: `http://articles.washington` ➥`post.com/2013-02-10/world/` ➥`37026024_1_cyber-espionage-` ➥`national-counterintelli` ➥`gence-executive-trade-` ➥`secrets`
- Schwartz, M. J. (2013, May 02). China Tied To 3-Year Hack Of Defense Contractor. Retrieved from *Information Week Security*: `http://www.informationweek` ➥`.com/security/government/` ➥`china-tied-to-3-year-hack-` ➥`of-defense-con/240154064`



The Hacker Perspective

Tyler Frisbee

Contrary to the norm of my generation, I had a late start to my hacking career at the elderly age of 13. My inspiration was that of many bored adolescent malcontents: Hollywood and television. I was what you could probably call a computer addict back then, but I still didn't know a whole lot about my pitiful HP G60 Notebook running Vista, nor did I understand *why* that setup was pitiful. Nevertheless, I had the drive, and the naivety, to believe I could hack with the best of them.

With the aid of a little bit of math, you have probably deduced that I am not much older than I was at the inception of my "career." You would be correct. At 16, I am now taking a look back at the past three years, both critically and humorously. I do not by any means condone my early transgressions described in this text, and I only now write about them to entertain and educate experienced hackers and to dissuade aspiring hackers from following a path of misconceptions and destruction. That being said, I would also like to provide my insight on the beginner hacking subculture and the hacker mentality.

Following in the footsteps of all the pernicious script kiddies before me, the most obvious plan of action to kick-start my hacking adventures was to Google search "how to hack." After sifting through the first ten of several thousand results, I had collected enough regurgitated information to begin breaking cyber-laws.

I'm sure many aspiring hackers can relate to the next "hack" that is almost a rite of passage into the role of being a script kiddie. I learned about a now scarce flaw in some websites based on outdated SQL databases which allows you to easily gain some limited administrative privileges by entering simple strands of code into the login field. You don't have to go through any of the steps that are necessary in hacking modern or maintained SQL databases. Not much by our standards, especially since wikiHow largely contributed to my success, but to a 13-year-old computer-illiterate, I was now a self-proclaimed hacking genius.

I relished every exciting moment of my shady SQL escapades, yet there was one aspect of my saga which cannot be ignored. Most of the databases I had targeted were outdated and often abandoned, making the difficulty level equivalent to shooting fish in a barrel and adding to the ease of implementing stolen techniques. My mistake, however, was when I began targeting up-to-date SQL sites that didn't tolerate such behavior. After a successful night of breaking and entering, I was horrified when one website kindly presented me with a notice stating that my activity on their site, along with my IP address and other identifying information, had been reported to the police. Needless to say, whenever I saw a cop car for the next several months, I nearly vomited.

Obviously, nothing ever came of this supposed reporting of my activities, so my fear subdued and I happily returned to my misadventures. It is quite apparent that not much rattles the spirit of a heretical script kiddie, an eternal testament to their catastrophic potential.

As time wore on, I inevitably found my way to much more malicious software as my few SQL tricks grew increasingly boring. Many clear net hacking forums were not pleased after multiple DDoS attacks brought down their websites. I was fortunate that I never saw repercussions for this behavior and, while I am not particularly proud of my rocky start, my malevolent acts as a script kiddie did lead to something far greater than reading the Wikipedia page on hacking.

After months of indulging in my newfound juvenile pastime, I began to develop a strong curiosity for what was *really* happening behind the scenes with these hacks. I soon found myself staying up late researching HTML and SQL code and several web applications. Without even realizing it, I was slowly evolving from a script kiddie into something somewhat more respectable.

During the process of learning about how important technology worked, I grew to become borderline obsessed on the topic of Internet security and how to break it. I've always seemed to have a talent for breaking things, why not security?

The day I began exploring the deep web and reading some hacker forums may have been the true turning point in my morality. I read a lot of posts from well-established hackers scolding the kind of behavior I had been participating in. At first I was confused - why did they consider hacking to be scandalous? Aren't they hackers themselves? It took a great deal of time to understand their thoughts and to be able to distinguish between a script kiddie and a true hacker.

It is now clear to me that, yet again, Hollywood had portrayed something inaccurately. Shocking, right? With overzealous media, gross misconception, and modern entertainment, most young hackers begin their escapades out of sheer ignorance, complete disregard for the potential consequences of their endeavors and, in many cases, just to appear cool or to show off. The birth of many hackers today is in substantial contradiction with the early phone phreaks and hackers that hacked either for the fun of the game or to overcome obstacles.

While the playing field may have changed over the years, there is still an abundance of highly skilled professionals out there contributing to the community, and it was my goal to be a part of that. I wanted to break away from the derogatory category of "script kiddie" and graduate to the venerated status of what is widely considered a "true hacker."

Subsequent to my revelation, I quickly ditched the ruinous inspiration of Hollywood and adopted something much more authentic to that of a hacker. However cliché, as it has seeped through to the mainstream, "The Conscience of a Hacker," more commonly referred to as "The Hacker Manifesto," by Loyd Blankenship (also known as The Mentor), provided something relatable which many hackers can most likely sympathize with.

Empowered with my latest reading material, I was determined to begin to actually learn the proper way to hack, but in the words of many Sean Bean memes, "one does not simply learn how to hack." Becoming a skilled hacker is a long process, one that takes years of gathering knowledge about pretty much everything. This is a difficult concept for many beginners to understand. To do so, you must already have followed the aforementioned concept throughout life. Hacking isn't something you can simply learn with a Google search or by reading a "for dummies" book. It takes a collection of many skill sets such as knowledge of multiple programming languages, computers, circuitry, social engineering, the Internet, and maybe even the phone network!

Earlier, I listed the reasons for script kiddies becoming involved in hacking. The most important point of that list was the idea of self-proclaimed "coolness" through destructive attacks derived from software that can be easily downloaded from the Internet. I understand this desire as much as any script kiddie as I was indiscriminately one myself. If you are inspired to hack just out of the desire to appear as though you're an Internet badass, then I recommend revaluating some life decisions. Hacking isn't about being the coolest guy out there; it's about having fun and overcoming obstacles. Sometimes it's about supporting a cause or advocating against an injustice. Can you be considered cool if you hack? In my opinion, of course you can! You have the skills and the ability to do something that many would never dream of doing. That being said, hacking isn't a popularity contest. If you're hacking to be cool, then it's time to find a new hobby.

As with any hobby or profession, there is always a substantial supporting community. For me, and I'm sure I'm not alone, hacking became about the social aspect just as much as the hack itself. Feeling like you belong to something great, like the hacking community, can be a powerful thing. With only a few clicks, you can instantly connect with thousands of like-minded supporters of your campaign for greatness. This has been a significant driving force for many aspiring hackers to sharpen their skills.

Not only does hacking give one a sense of belonging, but through my experience they can also develop a certain level of self-confidence. For years, I was "that shy kid" who didn't say much in public unless surrounded by friends or family. Even my friends proved to be of little comfort as I have a knack for befriending arrogant narcissists that enjoy nothing more than pointing out everyone's perceived flaws. When you become immersed in the world of hacking and have the opportunity do something that many people can't, and know you have the ability to solve difficult puzzles and outsmart some of the best, you begin to feel very good about yourself.

Aside from the social curiosities of hacking, as backwards as this may seem, possessing an interest in hacking can improve the outlook of your future. I had struggled throughout elementary and middle school. When I developed an appetite for learning about technology, I quickly gravitated towards the idea of being a programmer. Knowing that my dream depended on doing much better in school, my grades began to skyrocket and have launched me into several advanced classes, most notably Advanced Placement Computer Science. Hacking is what essentially sparked my interest in computers and, while I certainly do not promote attempting to DDoS the NSA home page, I do believe that a little recreational hacking can be good for one's future and curiosity.

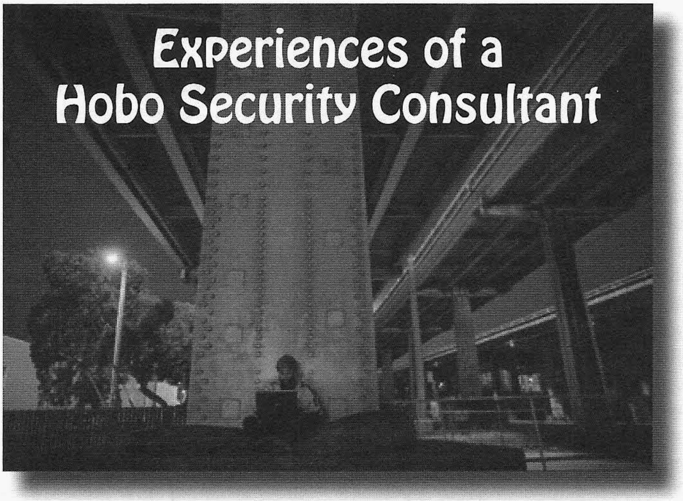
You have all heard the story of how that famous pair of geniuses, Steve Jobs and Steve Wozniak, had their first experience in design, development, and marketing in their original shady business of manufacturing and selling homemade blue boxes which allowed you to make free long distance phone calls. This background in entrepreneurial activities undoubtedly aided the future sale of Apple I computers, and the procreation of Apple itself. Not only did they have their first experience in business through the sale of the controversial... phone accessories, the experiences they shared brought them closer together as friends and made them very popular amongst their soon to be loyal customers. While the career of vending blue boxes proved to be ephemeral, hacking, or phreaking, with these seemingly magical devices, was a kick-start to one of the most influential technology companies in the world. and not because of a will to cause destruction to or steal from Ma Bell, but to entertain and explore.

I have referenced hacking to be a "hobby" on countless occasions throughout this text. This shortcoming is a mere derivative for lack of a better word. Hacking isn't just some pastime you participate in on the weekends; hacking is a way of life. Hacking is seeing the world differently and longing for something you currently do not possess or cannot do. Hacking is the freedom of information and knowledge. Hacking is about the thrill of solving puzzles in the name of exploration. Hacking is about understanding what is really going on in the world and having your eyes wide open when so many others are blind. Most of all, hacking is about curiosity, ingenuity, and problem solving.

The term "hacker" is an elusive one. One that is seemingly impossible to develop a clear definition for as raging debates are often the result of any attempt to apply a formal treatise to the word. The hacker perspective itself is also a matter of controversy, yet it is indicative of the very force within hackers of all forms. White hats, black hats, grey hats, crackers, pirates, carders, penetration testers, programmers, activists, phone phreaks, noobs, script kiddies, or bored teenagers. No matter the name or title, they all possess the unique characteristic for challenging the status quo. You may call them nerds, geeks, misfits, or criminals, but no matter what label is applied to us, we will continue to succeed at what we do best. We are hackers. And that is a powerful thing.

Tyler Frisbee is a 16-year-old in his junior year at Shenendehowa High School in New York who has a tenacious interest in technology and writing. While he doesn't know which career he wishes to pursue, it is his dream to work with technology and he believes that he will one day change the world.

Experiences of a Hobo Security Consultant



by eyenot

Sometimes, when your life lacks direction or purpose, it's good to take a break. In my case, it was good to take a nearly 12 year break from things like a job, bills, responsibilities, or a home. I was getting allergic to mold anyway.

There's a lot you can do to survive without any income or any home. Almost any city you find yourself in has one of two kinds of homeless shelters: notorious or secretive. The secretive kind are usually reserved for battered women or sensitive families in emergency situations. The notorious kind are usually crawling with people who receive some form of fixed income, but aren't spending it toward a living situation, but rather a lifestyle.

The worst case scenario I ever found myself in was when I visited the northwest to study the anarcho-primitivist enclave there. I arrived too late - they had been arrested for burning several SUVs and a postal truck, and were among the first U.S. citizens to enjoy the new laws against "terrorism." So I got to sleep under a perfectly nice bridge with perfectly fine intellectual hippy types instead of in a shelter. Nothing I hadn't done for years by that time - but in a strange town, it's a bit unnerving. Luckily, some hippy had filled their rather copious medical marijuana prescription.

Myself, with no mental or physical ailments, disabilities, or disorders - and having no felonious or serious criminal history, and being entirely able-bodied and well-minded - I faced a lot more challenges on the streets than most people. Most of the homeless people you meet are collecting some kind of money for something being off about them; they just don't know what to really do with the money.

It was unusual just 12 years ago to see a homeless person with a smartphone or a computer of any kind. Such items realistically offer a destitute person little more than a potential crosshair on their back. And when cell phones of the lost, found, and stolen variety are easily sold on the street for as little as $5 to $20, you can be sure that being seen with an expensive gadget makes you look like a quick fix to your fellow destitute hustlers.

Then, about six years ago, laptops started showing up in the hands of some homeless people in the United States and, most surprising of all, started staying in the hands of their owners. Maybe this has to do with computers being seen as more of a burden than smartphones, on the heels of smartphones becoming ubiquitous instead of frivolous. A laptop is a magnitude more difficult to prize, to run away with, to pawn, to sell, or to ditch than a smartphone is. And, of course, it's more a burden from the owner's perspective as well. Especially if you don't know how to use a computer.

And, as luck would seem to have it for anyone who can repair computers but finds him or herself down and out, most fellow bums and hobos don't understand how to operate computers. At least you would think that this fact coupled with the increasing appearance of expensive gadgets around the campfires and "day room" tables would spell lucky money for risky entrepreneurs. As it turns out, it's just a huge headache.

Even if you aren't homeless, doing computer repair work on a walk-up, on-the-street basis is hell. The major nuisance is competition. The Hollywood imagery of "hacking" is prevalent within the imaginations of the United States populace. Even among my new college peers, the "Holly-hack" image supersedes anything else you try to say to them about topics like programming or security, so just imagine the uneducated masses. Easily nine out of ten people on the street who "can fix your computer for you" are going to beset you with a nightmarish conflagration entailing two or more actively scanning anti-virus/malware programs, a handful of "cleaner," "doctor," and "speed up" software, as well as some trojan or spyware of their own sly choosing.

So, being the street equivalent of "white hat" isn't that hard. Just genuinely clean a person's computer, install half-decent free anti-virus and anti-malware software in a configuration that the softwares find conducive, and then test the defenses legitimately.

The great thing is that there are numerous free end-user titles to choose from to help you out. Smart tools available from Sysinternals go a long way towards fixing Windows XP, Vista, and 7 systems. Your client may or may not especially enjoy if you replace their regular "task manager" with "Process Explorer," though if you have to walk them through something on the phone you can have Process Explorer already set up with your preference of columns. Some Gibson Research tools are still very useful. If your client is trying to micromanage their "friends'" use of the laptop, Steady State is still a workable solution. WinPatrol is helpful for long-term clients. Baseline Security Analyzer is a must-have for its ability to fix the "windows update" scheduler when it hits a hiccup - clients with frequent signal interruptions over slow Wi-Fi will be grateful if you manage to rescue them from an update loop.

However, the various free anti-malware utilities always leave me scratching my head. The most popular virus scanners are for-pay but are notorious resource hogs with morally objectionable definitions of "uninstall." Then we find the free scanners and again the most popular ones (or at least, the ones that computers brought to me typically have installed) are also clingy and suspicious-acting. Then when you think you've found a nice product, they go and change on you, so you're always looking for the best combination of things. I've found one active scanner and also one passive scanner activated by a time-triggered event is the best combination. But a client's computer isn't a good ballroom to discover which crippled free active scanner is a suitable dance partner for your favorite heuristic defense engine. Most street business entails one thing and one thing only, and that's getting their computer running "fast" "again."

As an aside, another nice "white hat" thing to do is walk onto the scene at one of the local second stores operated by a charity nonprofit organization, and offer to create and maintain a computer department for them. I was successful with this as a means of earning my keep at a homeless shelter that demanded an hour of verified volunteer work in exchange for every night I slept under their roof. I managed to pump computers out at a pretty fast rate, especially since they were all mostly built for XP and their cases still had valid product keys on them. Of course, the product keys are useful even when you are parting a machine out and throwing the case in the scrap heap. There are other fringe benefits of such a position. And just because you haven't seen such an operation, don't imagine it can't be done. Trust me, the rural, semi-rural, and suburban areas around you are chock full of computers that somewhat intelligent people detect are too valuable to just be "thrown away." "Maybe some poor people can make good use of the computer. I will donate it to the second hand store owned and operated by a nonprofit charity." Try to convince the management to take any old or new computer, indiscriminately. If anything, busted-up old hard drives still yield those amazing rare earth magnets, which are great for hanging tools from in the amazing, magical workshop you've set up. But I digress.

To continue on, you then explain to your street client the trouble with browsing, downloading, and running things as Administrator, and set them up with the "user" account. Oh, now we're getting somewhere. And get them to learn and stick to a regimen of not doing things to directly attack their own computer. Ah, exactly: now we've arrived squarely back at "work" but you're only going to get between $5-$20 for it. And it's work you'll be doing with them over your shoulder, and in one spot, for upwards of a few hours.

And we all know the education can't stop there. I once sat down with the ostentatious ambition of writing "ten things you *have* to know about computers," which quickly became "25 things," and when I hit a weird number like 34, I decided to just make a thorough list. I concluded with 80 things I wished every one of my clients already knew about computers (or else would learn). Who has the time when your clients don't listen because they don't truly care, even to the same one single item at a time for weeks and weeks?

Sure, there are things that you can do to make the "work" easier on you. You can give the client a bulleted list of finishing-up tasks they can complete on their own. Or can they? Maybe they'll be capable of using the "uninstall a program" panel to remove an annoying or potentially unwanted toolbar. Or maybe they'll just say they will - while secretly they covet their precious little browser doodad that they successfully installed all on their own. And they'll become silent for a few weeks while they enjoy their precious, forbidden little spyware you insisted was malicious. "Grandma's recipe organizer." *Sniff*

And maybe they'll be capable of updating the newly installed scanner and performing a full scan. Or maybe they'll attempt the update without making an Internet connection first because McDonalds shooed them out, and maybe they'll feel like the scanner is taking too long and hit abort because the police were pulling up to the park bench. In which case, when you try to follow up with them, they'll tell you "it didn't find anything!" (Ting!) They have other things to do and can't always make it to a hotspot or find time to sit in one place for an hour or two while not being entertained.

And when you get tired of them bringing the same computer to you with the same problem, and you smell something fishy and ask them if they let anybody else use the Administrator account, they will spill the beans and admit they let their nephew (or their fellow addict) "fix some problems" with it. Oh, here we go, again.

"What kind of problems? It was fine when you left me."

"Well, you know. It started running slow. A-gain."

"When did it start doing that?"

"Right after I let my 'nephew' use it to chat online."

"The same nephew who then offered to fix it for you? Can you remember if you typed *anything* sensitive after he started using it? It's kind of important."

So, eventually, you start to add a bulleted item at the bottom of the list: *No Outside Consultancy*. But that doesn't work, because now you're insulting the person by what appears to be an ultimatum. It's one thing to really represent a lifeline to a company who has no option but to honor such an agreement. But on the street, to America's special and sensitive population, you're just another computer person. They have no idea what the hell you're doing and have no reason to trust you any more or any less than the next "computer guy." Frankly, you'll eventually lose the respect of people whose respect you can't afford to lose, just because you're the only "uptight" computer guy out of all the rest of the pretenders, and the rest are schmoozing while you're accomplishing nothing but to make your clientele grow increasingly uncomfortable with you. Especially when that enemy you're warning them about is one of their closest friends, or worse, their family.

There are, of course, some pieces you could play to win the game against those who are attacking your client's computer. But they're extreme moves. You could lock your client entirely out of administrative privileges, for example. I tried this. "You sure this is all you want installed and you're completely content? Here we go. Now only I, your consultant, knows the Admin password." But they will eventually forget why you said that was important, or they will want another piece of software installed, and they will take it to another consultant, and that consultant will either just Ophcrack the account password or else wipe and install with a compromised copy of Windows they torrented. The client won't come to you to change the setup, because they don't want to supersede your presumptuous appearance of authority, but they don't exactly like your genuinely necessary position of authority, either.

Or you could rootkit your client's computer. But then you're not strictly white-hat (depending on your philosophy) or, at the very least, you're just overcomplicating the matter. What else are you going to do? Set up a honeypot and a LoJack? If you had a server to dedicate to the cause, you could even maintain your own level-headed, nigh-impenetrable dragnet over all the computers of the gentle salt of [your city here]. Yes, to the tune of decreasing amounts of money (wow, $5/3 per hour!) while people on the street gripe to each other of what a stick you have up your ass.

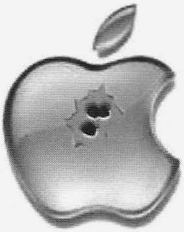
When it comes down to it, there isn't

anything to gain from street level computer security consultation. The money isn't there, the respect isn't there, and even the experience of educating people and doing a good deed goes unfulfilled. That warehouse I worked in? They kept taking up all my time, insisting I should try to repair and resell used and discarded printers. They didn't want to listen to the hobo ranting and rave madly about how he worked for several years in new and used computers and electronics and that if there's anything you don't do, then you don't do used printers. I tried to tell them that they couldn't keep installing XP forever, but they weren't eligible for Microsoft's free OEM offers to charities because they discriminated against sexual orientations. Because God.

The department was eventually deemed unprofitable and was shut down. I managed to decently train three novice repairmen and to successfully bring a formerly knowledgeable ex-con up to snuff and make him into a fully-fledged secure end user and modern-day computer repair person. But the "e-bay" department, which consisted of an insane hoarder who didn't understand the real meaning of "mint condition," was deemed more important. She told everybody she was a "computer hacker" and a "computer expert," but when she infected her own computer with a virus and I pointed out her incompetence to the management, she rallied every day to have my section shut down and spent every hour trying to get on my nerves. Eventually, I gave up my only means of keeping shelter, and quit. The "Holly-hack" is like the Nothing of *The Neverending Story.*

Hobo security consultant? Depending on if the economy is worsening or improving, (consecutively) your time would be better spent trying to write the next *Steal This Book* or *The Joy of* [insert some thing that gives you joy but is outdated, here.]

(In my personal story, I eventually shook my head sadly and decided to go to college in pursuit of a Ph.D. in computer engineering. In retrospect, if I had made that decision sooner in life, it would only have been for the better. However, there is no other lifestyle to rival homelessness in offering instant gratification of the need to feel carefree, to relax, and to take it easy for a while. As long as you can handle the street environment and relish being a literal bum.)



"My Precious..." (Apple)

by lg0p89

For full disclosure, I do drive an iPhone. There are absolutely no complaints regarding the iOS or the hardware from myself. This is recommended for any users. Back to the story.

One thing we could depend on day after day, month after month, up until one or so years ago, was Apple products being relatively safe from malware and the other bugs that can haunt PCs and Android OS devices. One could sleep soundly at night knowing with a reasonable certainty that everything was safe.

RGE (Resume Generating Event)

Well, all was not well in Mudville, Cupertino. In July of 2013, the Apple developer site went down. The message provided was that the site was being maintained for a longer than expected period. The site stated "We'll be back soon." (Osborne, 2013) This was on a fateful Thursday.

There was an update from Apple stating the maintenance was still in process as of that Friday. Given Apple's attentiveness and proactive nature, this was an odd effect of something. Finally on Sunday, the actuality of the situation was released to the public, aka the truth. The updated message on the Apple website was that there was a breach of their system. A portion of the data that was accessed was not encrypted. Based on the potential for issues by non-authorized persons accessing the compromised accounts, Apple sent out password resets. (Zorz, 2013)

On a positive note, the Apple customer information was not in the same location. This was a blessing, as it turns out. It was also caught in a very timely manner and managed.

The point, however, is that this is not the standard operating procedure. Apple, with its closed source, was the bastion against intrusion and malicious penetration. The system segment that was breached was where the developers would visit for downloads, documentation, and discussion forums. This was a black eye and bad news for Apple's info sec team.

Twist

Up until this point, it appeared there was a malicious attack and successful breach. This clearly would have been bad news. A few days later, a security researcher (Ibrahim Balic) claimed responsibility for this. He even went so far as to post a video on YouTube showing the methods used for the breach. This was on his Twitter account. (Osborne, 2013) It was also posted on *Tech Crunch* that he found 13 bugs and had reported these with `http://bug➡report.apple.com`. (Zorz, 2013) Thus it is clear to a reasonably prudent person that Balic did this, due to his own admission published by at least three sources.

Ethics

For penetration testing, generally the contractor speaks with the client, reviews the parameters for the project, prepares a contract, both parties read and understand the ground rules, and the testing starts at the opportune time.

In this case, he allegedly completed the penetration test successfully. However, he did not secure permission from Apple to do any of the work. None. Apple had no idea this activity was inbound. Granted, he had the best intentions, however, these do pave the road to Hell. His intent was, as it appears, for a friendly to explore the vulnerabilities. His comments show there was no malicious intent. The vulnerabilities were reported to Apple so they could be closed and also to lower the attack surface. Although his intent and subsequent actions show no malice, the breach may be actionable by Apple.

It is hoped Apple will see the light and not pursue any legal action against Balic. He should not have done this without permissions and a contract, however, it was done solely to benefit Apple.

Lesson Learned

The professional e-security researcher does not conduct a penetration test or active measures in an attempt to breach another's system without express permission, generally in the form of a contract so there are no misunderstandings later, aka lawsuit. The security researcher may only want to help the company out by letting them know about their vulnerabilities or that they need to push patches now.

As an analogy, think of your neighbor's home. As you drive home late one evening, you notice their floodlight has burned out. Wanting to be a good neighbor, you walk onto their property, prop up their ladder against the barn, and exchange the light. Think of your neighbor's physical property as Apple's digital playground.

Some people on the Federal level may call this trespassing or a breach of several Federal computer laws. As a security researcher, you don't want the criminal or civil issues that could be pursued because of this. Being a good Samaritan at times does not pay. No good deed goes unpunished.

Remember, always have express permission to do a penetration test unless you enjoy a rather large bulls-eye on you or your smart phone being tracked via its GPS by government employees wearing black suits.

References

- Infosecurity. (2013, July 22). *Apple developer site breached.* Retrieved from `http://www.infosecurity-mag➡azine.com/view/33555/apple-➡developer-site-breached`.
- Zorz, Z. (2013, July 22). *Apple developer center hacked by security researcher?* Retrieved from `http://www.net-sec➡urity.org/secworld.php?id=➡15259`.
- Isidore, C. (2013, July 22). *Apple's developer site shut down by hack attack.* Retrieved from `http://money.cnn.com/2013/➡07/22/technology/apple-➡hacked/index.html`.
- Osborne, C. (2013, July 24). *Apple hack conducted for the greater good of research.* Retrieved from `http://www.zdnet.➡com/apple-hack-conducted-➡for-the-greater-good-of-re➡search-7000018492`.

Public Address

Further Questions

Dear *2600:*

I have a few articles ready for submission. Would like to send them to you, but first could you please point me in the direction you would like to see? Have a few ready about how to hire pen testers, how to conduct safe pen tests, exploit development (basic stack overflow, basic malware analysis), behavioral analysis, and a few more. Is there anything in particular you would like to publish about?

Yuval Nativ

We want you to write about what you know and tie it into the hacker perspective as best you can. We don't want to steer you into a specific topic or theme since you may have a great deal to say on something we know little about. The best articles come from the passion you feel about the subject matter, not from an assignment by us or anyone else. We look forward to seeing what you have to say.

Dear *2600:*

The below mentioned things I used to do regarding penetration testing and currently working with the penetration testing (article writing and book publishing) firms from the U.K., Poland, and Russia. Let me know if I can submit an article and work along with you guys.

RP

In the interests of time and space, we left out your extended resume, which was pretty impressive, but completely unnecessary. We're not about titles and achievements, but rather ideas and theories written by curious and adventurous types who aren't afraid to try new things and risk getting into a little trouble in the process of learning and sharing information. That's what we define as the hacker perspective. So please send us an article (articles@2600.com) and tell us what you've been up to and what sorts of havoc you might be able to wreak, given the opportunity. You can be nine or 90, as long as you can write and have something interesting to say.

Dear *2600:*

I'm going to be purchasing a lifetime subscription in the coming weeks and had a small (and fairly trivial) question.

I've been reading your magazine since the mid 90s, and have always purchased it from a store. For subscriptions, do you ship the issues in an envelope or is it loose? I ask because I live in the frozen wastelands of Canada, and loose magazines from other publications tend to get torn up by the time they reach me.

I'm definitely getting the lifetime hook-up, so your response won't alter my decision. I'm just curious about what I can look forward to, that's all.

Thanks for your time.

Daniel

We thank you for your support. Lifetime subs help us pay the bills. Your issues will arrive in plain brown envelopes. For those who are really concerned about such things, our name doesn't appear in the return address.

Dear *2600:*

I have been published a substantial amount and I have just completed an interview with an individual that by anyone's definition is a cyber spy. I thought of your magazine as a good place for such a piece.

As background, I was working on a piece about a cyber attack and this just sort of evolved out of that. My guess is that it would be about 1000 words.

So, are you interested? If so, when would you need the piece by?

Kevin

As our auto-responder should have told you, articles are continually processed, so deadlines aren't really an issue. Please just send us what you have and we'll hopefully find a place for it in a future issue.

Dear *2600:*

If I digitally subscribe to *2600* through Google Play, would I be able to participate in the many perks that regular dead-tree version subscribers have?

A curious person

If by perks you mean being able to submit a free Marketplace ad, yes, this is now possible if you send us some sort of proof of purchase in place of the subscriber label coding. The perk of being able to smell the ink or fan yourself with our pages just isn't available to digital subscribers, sorry.

Article Feedback

Dear *2600:*

In 30:4, the article titled "Black and White: The Growing Schism between Hackers and the Law" is a great example of our universities, lawmakers, and law enforcement not working together to explain how to properly report a vulnerability to an affected organization. I think it is high time we all start contacting our politicians to encourage them to begin writing better laws and enacting better policies to allow white hats to report problems they find to site owners. When I say white hat, I literally mean someone following the letter of the law. Going into a network, especially areas that require authentication, and snooping around without written consent from the owner and without doing damage, is equivalent to breaking the Computer Fraud and Abuse Act of 1986 (CFAA). The CFAA should be your ultimate guide to determine what you are wearing - enough said.

Not to knock the original writer, but it seems he must not have known or tried to use a whois lookup to find the contact information of the site owner. He should have also tried to contact one of the Infragard members listed on the site, assuming they had their email addresses posted. The reason for the feds' overreaction is that Infragard is a forum between federal, state, and local governments, along with critical infrastructure organizations, to discuss critical security issues. Posting a vulnerability all over the place was not the brightest idea, but it was noble for the writer to try to get their attention. I hope this incident does not cost him his future job prospects.

I would suggest that we all try to use some discretion in bringing to attention critical security issues that were accidentally discovered, by using anonymous forms of communication to report the problem to site owners. That means using whois.sc, looking for the webmaster's email address (which the author did try), and using Google to try to look up the owner's contact information. It is vital that you document all of the time and work you did (e.g. right clicking and looking at the source code of the site). This is your get out of jail free card. It proves what actions you performed and when. Assuming the site owner has logging enabled, the logs should clear you from any wrongdoing - this assuming you didn't go into any protected areas on purpose or try anything to exploit the vulnerability. Overall, you need to treat this with due diligence. If you can't find the site owner, then contact the hosting company as a last resort. If that does not work, then just let the site owner find out the hard way. I am sorry to say that, but if you covered all your bases, then the onus is on the owner and you should pride yourself on doing a good job.

Never cease trying to do good - it will be rewarded one day. I understand the author's frustration and belief that no good deed goes unpunished, but I believe in the end the good will always outweigh the bad. Keep trying and never give up helping those around you.

The Professor

And don't forget to send us the details whether or not you were successful in getting any attention. It's what we're here for.

Dear *2600:*

I enjoyed "Telecom Informer," as always, in 30:4. In the article, TProphet bemoaned the lack of responsible schools of thought for American businesses. I'm writing to mention that there is now a new breed of business school, where "sustainability" is the key theme. Bainbridge Graduate Institute, near one of TP's prior haunts, Seattle, is one of the earliest. Presidio College has a sustainable MBA, too. One of the binding notions is 3BL, or Triple Bottom Line, which emphasizes "people, planet, and prophet."

Estragon

Seems like a natural fit with a slogan like that. The spelling is a little off, though.

Dear *2600:*

I was just reading Clutching Jester's "Hacker Perspective" column in the Spring 2014 issue and the "encrypted" message at the end of the article is "Happy hacking, everyone!"

It is shifted two characters to the right in relation to the typical American keyboard. I'm sure you have figured it out already, but I just thought I would send a message to spoil the secret!

Wolf Bronski

Random Thoughts

Dear *2600:*

When thinking of privacy statements such as those found on the bottom of websites or pertaining to other services used, consumers believe this means their information will be kept from prying eyes. The complete opposite is true when it comes to privacy statements that individuals agree to. Instead, these statements give many loopholes for any type of organization to give out personal information on consumers. Privacy statements give the organizations providing a particular service terms that only benefit them, not the consumer, clients, etc. Privacy statements are legal contracts that have loopholes to benefit only the service provider, not the individual users, unfortunately. My advice to all consumers like myself is to read those terms carefully.

Bill Miller

This is good advice, but we also need to know what exactly to do when these terms fall short of our expectations. Many of them contain pages and pages of legalese and it's almost impossible for any but the most dedicated to wade through all of that. We believe that helping to spread the word on which of these agreements actually offer a raw deal to the consumer is a very valuable service. Often, the resulting bad publicity results in a quick change to the policy in question.

Dear *2600:*

With the rise of password cracking tools using dictionary, brute force, and algorithmic methods, why haven't system administrators and programmers universally adopted a simple method of thwarting such attempts?

These attempts rely on the fast computing power of both the target system and the attacking machine or network. Password crack attempt speed is currently measured in millions or billions of attempts per second. Why not simply set up the target systems to require a delay of, for example, one second per password attempt on each username? I admit to not being a developer, so I don't know if it's easy or possible for a system to lock out each particular username for one second after each failed attempt at that username. Many systems will lock you out after a specified number of failed attempts, so my proposal seems reasonable. Developing and implementing this ability would essentially end password cracking by slowing the cracking tools down to glacial speed. Authorized automated systems which contain the correct password and human users would not be inconvenienced at all.

Food for thought....

Sol

The extremely fast password attempt speed you refer to applies to offline attempts, where a list of encrypted passwords has been obtained and the cracking is done at whatever speed is available through the hardware and program being used. Actual attempts using a login prompt do indeed slow down on some systems, such as Linux, in almost exactly the way you propose. The real trick is to keep the actual password file secure, as there is no way to control the speed with which someone attempts to crack it once it's in their hands.

Dear *2600:*

So instead of a rally in D.C., how about one at Ft. Meade, Maryland? It is public domain... think about that... why can we not see what is inside the software? I am very interested to see this magical coding that eludes all perimeter security. Furthermore, I would argue that it is in the public interest to see the source code to this software that they call PRISM. We all know that it take a lot of processing speed to convert binary to assembly language, so in that there is the real possibility of a physical or metaphysical layer such as EMP, or electromagnetic impulse. The utilization of this bandwidth is the most efficient way to collect metadata since the invention of transistors and is one of the most untapped resources, being that it is a physical reaction on the atmosphere that is being collected. These new devices that are visible in the magnetic spectrum are the hole in the window or the reason you keep being robbed.

There are a number of factors, now. Going backwards from metaphysical, we get into physical or actually visible in the known measurable range. We have a large amount of data being hexadecimally rearranged into variables that seem inconsistent or rearranged and then that data is stored. Without an outer shield/condom for computers, the infrastructure will always be vulnerable to an outer perimeter attack on information. SIGINT is nothing new. It is a shame that this technology is not available to consumers; to detect and reuse such an energy source is vital to power consumption capabilities in the sense that it allows more power to be stored in one AA battery. Theoretically, you could turn one AA battery into the largest supercomputer in the world if enough resources were applied to it.

J Thompson

That's one battery we could really use.

Communications

Dear *2600:*

I'm writing a book about what society can learn from the work, motivations, and methods of hackers. And I'm hoping you'll consider allowing me to include you. Obviously, your work across *2600* and HOPE makes your perspectives essential and I'd love to talk to you about it in person.

My working premise is that the rest of us (i.e., not hackers) have a lot to learn from the way hackers (white hats) go about things. I'm exploring how we might become better in life, business, art, etc. if we can adopt some hacker traits ourselves. And I'm wondering whether a world of driven, questioning hackers might be able to solve some of the world's problems, and how we do that.

Dave

We get a lot of letters like this and it's simply not possible to give each of them individual attention, let alone do in person things. That's why we encourage people to attend (and start) our meetings, as these are the places where all sorts of conversations are possible with people who really do get it. Sure, they may not be official representatives of the magazine, but that really isn't important in describing what hackers are all about, relating some of the history, etc. People who come to the meetings are usually quite well versed in what we're all about and they deserve the opportunity to give their perspective. We're also able to provide feedback at our conferences and through our weekly radio program, in case you really want something specific from us. Finally, we're not big fans of the whole white hat/black hat thing as such designations are meaningless and ultimately harmful. People, especially hackers, cannot be categorized in such a simplistic manner, unless it's to sell a product or scare someone into buying or doing something you want. You will find generally good people doing evil things and vice versa. That's the nature of humanity and it's no different with hackers. We're just a bit more interesting.

Dear *2600:*

I have been inspecting some of our cable equipment and i haven't read up on the magazines in a long time. However, my dad's phone hasn't worked right since 2009 and it's our business phone also. I went out to inspect some of the cable stuff.... I found four red tags on the cable lines, one blue tag, and one white tag. None of our services have worked properly and a lot of times we don't even get our phone calls. What are the technical codes of these tags?

Robert

To the best of our knowledge, those tags simply indicate the last time that particular piece of equipment was looked at or serviced. It would be very helpful to know what was written on them, if anything. For your dad's business phone to not have worked properly for the past five years is inexcusable. We're not sure what kinds of problems you've been having, but it's been our experience that when dealing with the phone and/or cable companies, aggressive hounding is sometimes the only way to get something done. Obviously, it helps to be specific and direct with them. The problems you're having need to be documented and, if nothing is fixed after all of that, your next stop should be your region's Public Service Commission or equivalent.

Dear *2600:*

Have you heard about the proposed new rules on net neutrality the FCC just announced? They plan to allow a "fast lane" at higher pricing. What do you think about this? It was just announced today, April 23rd.

Jerry listening on WBAI

The net neutrality issue is moving too fast for us to be able to say definitively where it stands at the time we make it to newsstands and subscribers. Suffice to say, it's in dire shape at the moment, due to the recent actions by the FCC. If that is allowed to go unchallenged, it will change a great deal about the way we get access to the Internet. We believe individuals won't benefit from this and that large corporations and parties interested in control of traffic will be the ones who gain. But the battle is not lost. This recent turn of events only serves to demonstrate how quickly things can change and how we should never let our guard down. We suggest keeping updated online, particularly through sites such as eff.org, so more negative changes don't go through without our being witness to them.

Information

Dear *2600:*

For those who missed their chance at phone phreaking in the 80s and 90s, the Phone Losers of America have developed a Telephone Network Interface which is connected to seven answering machines. This interface allows people an opportunity to hack into the connected machines, thereby experiencing some of the thrill enjoyed by enthusiasts back in the glory days of phreaking. The list of answering machines currently includes an ITT 9910, AT&T 1722, GE 29875GE1-B, Vtech 9152, AT&T 1738, GE 2-98768, and a Panasonic KX-TC1743W. Hacking answering machines is easier nowadays thanks to the advent of Google to locate their respective instruction manuals, but some can prove to be more challenging. In addition to the answering machines, the network also offers a conference room that nobody is ever on and a "choose-your-own-adventure" game that can be played over the phone. The system also recognizes Autovon military tones to access extra "features." This isn't the first network to be developed in hopes of capturing the nostalgia of old-school phreaking. Project MF exists to give younger phreaks a taste of what blue-boxing was like and it appears that HackThisSite.org is working on a similar project. If anybody wants to give old-school phreaking a try, you can find information at ProjectMF.org and PhoneLosers.org/TNI. The Phone Losers of America TNI can be reached at 206-424-8422.

Tyler Frisbee

This is truly some amazing stuff and we're thrilled that the history is being preserved in this manner. We had all kinds of fun with answering machines over the years and had even more fun watching others try to hack ours. Incidentally, we printed an article on brute forcing PIN code keypads in our Spring issue which contained a list of the shortest possible sequence for entering anything up to a four digit code, which would pretty much cover any answering machine of the era.

Dear *2600:*

I read that some of your readers had lost the back issues (and probably some other items as well) when their credit card expired from Amazon.

Myself being a veteran of the IT industry with a long period of my career spent doing backups (and restores) for a living, and generally being cautious about trusting Big Corporations with my stuff, I "solved" this very problem a while back.

I use an application called Calibre (http://calibre-ebook.com). With that you will be able to manage your Kindle (and other e-book readers) and synchronize the content to and from your device and computer, aka backup!

Keep up the good work!

//j

We've heard very good things about this application and hope our readers use this to protect the content they've purchased. With luck, we'll be able to help make this the norm, so that nobody loses back issues of any publication.

Dear *2600:*

I enjoy reading your articles and love the variety included in each edition. Thank you *2600*, and thank you to all contributors.

I know you've already mentioned Grace Hopper in the past, but I think she's worth reintroducing on a regular basis. Newcomers will benefit by learning about someone who greatly influenced our current understanding of technology and leadership - and old hacks occasionally need a reminder of such things. Grace is not with us anymore, but she was incredibly influential when she was; her ideas are still relevant and applied to this day. You can learn more at http://en.wikiquote.org/wiki/Grace_Hopper.

Oliver

Dear *2600:*

I was rummaging around the insides of my XP PC and learned that Microsoft decided on an interesting name for the OS's final build number.

I'm pretty sure someone must have sent this to you already, but just in case... screen grab attached.

Chris

We didn't even have to look. Build 2600, right? We've gotten so many emails on this over the years, we've completely lost count. What's most surprising about it all is that it's lasted so long.

Meetings

Dear *2600:*

The New York City *2600* meeting was an important thing in getting me to where I am in the world today. However, over the past ten years or so, I haven't attended any. I was thinking about attending the next meeting and giving a hacking presentation, something relatively low key (I remember how the Citigroup people were). I was wondering if I should just show up, develop a quorum, and make it happen, or if there is someone specific I should speak with who "runs" the meeting. If it goes well, maybe I'll make it a regular thing.

Brad

If you attended the meetings in the past, you should remember that they are extremely informal and that "presentations" aren't really given. Some meetings are able to incorporate such things, but to the best of our knowledge, *New York didn't really do this. Also, there is no one person who "runs" the meetings in any location. It's a group effort and there's no rank to pull. We hope you show up and get reacquainted with attendees.*

Dear *2600:*

I am here at the Krystal's Hamburgers in Titusville, Florida, the stated meeting location for *2600* readers in this part of East Central Florida. Once again, I feel like The Maytag Repairman as I sit with the empty boxes that once held my Krystal hamburgers, and I wander back to the counter to refill my small Coke every once in a while. The free refills and free wi-fi is what made the location my venue of choice since the Stonefire Art Gallery closed down.

Please consider asking meeting hosts to list their Foursquare short code for inclusion in their meeting listing. This way, people looking for the meeting can find a standardized format (Google Maps) for finding the meeting venue. Example:

Titusville: Krystal Hamburgers, 2914 S Washington Ave (US-1). http://4sq.com/bpM6DY

The use of the Foursquare short code allows a user to not only find our venue, but use the directions section of the site as well without the host having to deal with geocoding the place. Meeting hosts just look for their venue on foursquare.com, and the short code is available on the page.

Richard Cheshire, Phreak & Hacker

Again, as we don't actually have hosts for the meetings, it's tough to say who would take on the responsibility for doing this and making sure it was accurate. While this can be convenient, we don't think people aren't showing up because they can't find one of our venues, especially when an address is given. If there still isn't anyone else showing up after the promotion this meeting has received through the magazine and website, not to mention this letter, we'll have to conclude that it's just not a viable location.

Dear *2600:*

I am disappointed at the turnout of the meetings, especially since it is already official on the website. Is there anyone that you know in Minnesota who would like to take over and will show up every month? Thank you.

Scott

We urge you not to give up so quickly. It can take many months to get responses and attendance and we know it can be frustrating to not see results right away. If you continue to get the word out, we believe people will respond. Getting a website going can definitely help, as can social media. If there is a problem with the location for potential attendees, you will likely hear about it there.

Dear *2600:*

I have a friend who was looking for the local *2600* meeting. He said he checked out Barnes and Noble downtown and was unable to locate it at the typical time and that the website for the local chapter seems to have dissolved/disbanded. I would like to start a new *2600* local meeting in Maryland. I can create a website with times and information about topics. Is this acceptable? Supposing I set up the details and get it running, what is necessary for my group to be listed as a meeting in the official list? Is there a code of ethics for local meetings that I could found the group on to attempt to keep it professional and out of legal trouble? Let me know any information you can provide. Thank you.

David

All of the info you're looking for can be found in our guidelines section on our meetings page (www.2600.com/meetings). We do suggest keeping the meeting in the same place if you're planning on reviving an existing meeting, as you don't want people going to different locations based on old listings or memories. Meetings should only be moved if there's a problem with the venue, such as it going out of business or being extremely hard to find or inconvenient to get to. Read on for someone else with a similar objective.

Dear *2600:*

I'm going to give a shot at reviving the Maryland *2600* meetings. If you're interested, meet us at the Barnes and Noble in the harbor. You can be anonymous and avoid the linkedinesque environment that has largely taken over the local hacker scene. Don't worry about expensive meals and alcohol, or offending a potential employer, because there will be neither.

zenlunatic

Sounds like there's some history here which may be worth exploring as a lesson to the rest of us. Please share these experiences if you can. We wish you luck getting things going again.

Dear *2600:*

I would like to know how I can be a part of your next meeting?

Stacy

We have the easiest meetings in the world to be a part of. Just show up and you become part of them. If you don't have one nearby, you can *start them and become a part of them that way. Our meeting guidelines are at http://www.2600.com/meetings/guidelines.html. It's really that simple.*

Dear *2600:*

What can I do about an incorrect *2600* meeting location in the Dallas area? I am aware that there is both a "Dallas *2600* meeting" and a "North Dallas *2600"* meeting, but I only see the listing for "Dallas (Plano)."

What can I do?

Mike

You did the right thing coming to us. And you weren't the only one. Read on.

Dear *2600:*

It has recently come to my attention that the Dallas *2600* meeting has been removed from your 2600.com/meetings/mtg.html page. The Dallas meeting has been at the same location for over six years.

We have had meeting information up at http://tx2600.org and http://tx2600.info for several years and run an active mailing list on tx2600.info.

Please correct your information. I'm also available in the irc.2600.net #tx2600 channel if you have any questions.

Will (NameBrand)

The situation has been rectified. This mixup happened when we received an update for a meeting that seemed to be representing Dallas and, having not seen any recent reports from the old Dallas location, we assumed it was the same one that had moved. We've renamed the new one as Plano and restored Dallas to its rightful place. We're happy as always to see people paying attention.

Dear *2600:*

Hi I am looking to participate in meetings with HaxOrs

LONDON STYLE PLS

DANKE

Budo

We don't really know what this means, but if you're asking where the London meetings are, they're listed in the back of the issue and on the website. The location is the same as always. We will phone ahead so the London regulars know what's coming.

Dear *2600:*

Well, that was fun! I put on a clean shirt, my best jeans, even clean socks and underwear and headed out to my very first *2600* meeting at the Lakeshore Mall in Sebring, Florida. I arrived at the appointed place at 5:15pm for the 6:00 meeting. I stayed till 6:30. Not a soul showed up. There were a few possibilities... folks who looked like they might be the types interested in a *2600* meeting. I walked up to each and asked, "Are you here for a meeting?" One dude gave me the deer-in-the-headlights look before saying, "No." The others just shook their heads, afraid to make eye contact with me. I might give it another try next month, in which case I'll report back on my adventure.

Frankly, I was rather surprised to see Sebring in the meetings listing. We are a fairly rural county in central Florida where there are more orange trees than people. In fact, I think there are probably more cattle in our county than people. I'm curious: when was the last time you received confirmation of a meeting actually taking place in Sebring?

I've enjoyed reading your magazine every quarter for the past two years or so. Keep up the good work.

Seymour

Technically, your showing up made it somewhat official, but clearly a meeting with only one person isn't much of a meeting at all. We haven't seen another update in a year or two, so if you can confirm that nobody else is showing up to subsequent meetings, we'll have to pull it from the listings. This kind of thing happens as people move out of the area or wind up doing other things. It's always possible for others to pick it up again, but it's pointless to list meetings that aren't happening. Our typeface in the issue really can't get any tinier, so deleting a few entries isn't necessarily a bad thing.

Dear *2600:*

As required by the *2600* meeting guidelines, I would like to inform *2600* that I am transitioning the duties of coordinator and primary contact for the XXX *2600* group in ZZZ to YYY. If you have any questions please contact YYY. Thank you!

Name Deleted
ex-XXX *2600* coordinator (Aug 2006 - Apr 2014)

We deleted your name and all identifying info because we didn't want to bring undue attention to your meeting through our response. We don't know where you got the idea that you had to have a coordinator, let alone that we had to be updated on who that was. It's fine to have someone who takes on responsibility, but it's important to not let that turn into any sort of authority, as that's not what the meetings are all about. Everyone at the meeting should be *considered equal and as much a part of things as anyone else, regardless of how much or how little they actually contribute. Our only stipulation is that attendees follow our guidelines in order to remain a welcome part of the gatherings. And we thank you for your service.*

Dear *2600:*

I'm curious about how up to date the list of meetings is. I live in Seattle and was wanting to attend meetings, but didn't see any groups or mailing lists about it, and was wondering how active the Seattle group is. Thanks in advance!

Jared

We update the meeting list for every issue and you can see the most recent date on the top of the meeting pages on our website. We know that the Seattle meeting is pretty active.

Dear *2600:*

I, with some friends, am attempting to start a *2600* chapter operating out of Wilmington, North Carolina. We have held one "meeting," though it was mostly just us hanging out. I put up a page at portcityhackers.org to try attracting some attention, and was hoping that y'all would list us with your aggregate list of sites/meetings for some extra exposure since our bookstores don't sell *2600*.

P.S. I love the product that y'all put together.

John

You're off to a good start, and hopefully this letter will help more people find out about your meetings. If we keep getting updates sent to meetings@2600.com, we will add you to our official listing. Good luck!

Letters on Letters

Dear *2600:*

Reading Issue 30:4 prompts me to write this letter. The first thing I do when I get my *2600 Magazine* is read the letters section. Perhaps I was in a bad mood or something but some items in the "Critical Observations" section really annoyed me. Reading the first two letters, I am reminded that some people don't understand the spirit of hacking and what *2600* is trying to preserve. Common topics of letter submissions include: complaints of political motivations of *2600*, outright asking for someone to "do" something for them, implications of *2600* being hypocritical, and general misunderstanding of what *2600* wants to preserve. This might kinda seem like a rant and I may be talking in abstract terms, so I apologize in advance.

I'll start with my thoughts on the spirit of hacking. I believe the spirit of hacking includes thinking outside of the box. This means doing things that others don't do, finding ways of having things work differently than intended, making things work for how you need them to be instead of how they are, thinking of things that others have not thought of, and making things better than they are. Going further, the spirit of hacking is sharing this information with friends (and everyone else), recognizing that everyone has something to contribute (even if they have less or more technical knowledge), and holding onto the freedom to do all of the above. To some extent, this knowledge can be (and has been) used to help maintain personal freedoms that other people may want to take away.

Moving onto the political aspect, I would say that pretty much anything can be said to be (or twisted to be) a political topic. Isn't politics pretty much a difference of opinions as to what the freedoms and restrictions of the citizens of a country should be? Sure, it is a struggle for power for those involved, but to what end? It's to get power to enable the freedoms and restrictions that they want to have in place. Sure, I would say that makes the spirit of hacking as political (and non-political) as any other topic. That is not necessarily a bad thing. Instead of immediately discounting someone's view because it is "political," it should be responded to with reason and consideration.

My second item refers to requests for people to do things for them. It's hardly worth talking about since no one takes these people seriously (and why should they?), but I can say that I never really cared for people who don't at least try to do things themselves. Perhaps these people have tried and failed - no one really knows. The spirit of hacking is perpetuated by people who walk up to a task and start tinkering with it. Maybe they are tinkering for fun or they have a real need to do something. Everyone needs help sometimes, but I think it is often better to try to make the effort yourself (unless it is not feasible to do so).

The third item was the hypocrisy of *2600*. I don't really see it, myself. Keeping in mind that there is not only one person working and contributing to the magazine, I don't really know how you can expect to never see conflicting opinions/statements. Also, knowing that there are different people contributing, would you really want to not see conflicting opinions? The answer should be no. Imagine that you are in a meeting and you are designing some new [whatever]. The first person makes a statement as to what you should do and the other dozen people say "sounds good to me." That's not good at all. This idea kinda moves me into my last topic.

My final thought was about what *2600* is trying to preserve. The following items are what I have inferred from reading *2600* for about ten years now. They seem to try to preserve the integrity of the hacker spirit (through the changing times) as well as the integrity of their publication. They want a sharing of knowledge, opinions, and new finds. They want people with different experiences and conflicting beliefs to work together to better things. Unproductive and ineffectual things are not desired, and sometimes mocked ("Hey, can you hack my ex-girlfriend's email account, bro?"). As one might expect, they want to maintain the integrity of their publication. This is why they require articles that are not published elsewhere.

To close my letter, I am not trying to persuade you to change your opinions. I am trying to help make people realize that their letters might be able to contain more rational thoughts which, in turn, may offer more effective deliberation on the topics that are discussed in this magazine.

Shocked998

We have to admit that it wouldn't be nearly as much fun if those people who wanted us to do things for them didn't write in. Regarding the political angle, we agree that so many things in everyday life are political in nature. By avoiding that reality, we basically give up any say in the outcome, a contribution that could be considerable given the intelligence level of this community. We've seen that avoidance lessen over the years and the organizational abilities amongst hackers have improved substantially. That is a very good thing. How else will we not become victims of bad laws and oppression in the future? And how else will we be able to help share information, reveal leaks, and protect individuals from prying eyes? Politics, combined with our curiosity, mischief, and sense of justice have brought us to a very interesting place.

Dear *2600:*

I:m a bit late reading *2600* this time around, and the "Horror Story from Hell" in 30:4 really intrigued me. I study malware in my spare time, and have never heard of anything so completely devastating as the thing described by Morgan.

If I'm not too late, could you please pass off my email to Morgan? I'd like to try to help combat this malware. If everything in the letter is accurate, this discovery might be more important than the discovery of Stuxnet, and with many worse implications.

If Morgan isn't interested in my help, then I wish him/her luck, and would love to hear how everything turns out in the form of an article. This is definitely article worthy.

Thanks for the great magazine.

Hunter

We're not in the habit of passing messages between readers, but if the original writer expresses an interest, we will convey your info.

Dear *2600:*

I have read your website since the mid 1990s (after I started programming) and the magazine since the 2000s. Since then, it has been my favorite science/philosophy magazine (meaning also the philosophical/sociopolitical/ etc. focus of many editorials and some articles). Though I would have never expected to (with social attitudes about curiosity/hacking when I was growing up), I turned several people on to the magazine - both a hacker who inspired me, and those who do not consider themselves hackers, but liked the editorials, articles, and letters I advised they read. I found a local *2600* group, which exceeded my expectations, then I submitted my first article to you, and have ideas for others.

Though *2600* possibly always criticized large, inefficient, and corrupt organizations (government or private), after my first few years of reading *2600,* when so-called "free speech zones" became common at political events (after some being invitation-only), and various computer technology steadily became more integral to people's lives, it seems there has always been more to criticize... with companies creating more "walled garden" and insecure technology, and always more insidious stuff, such as Apple making a technology to sell to police to disable people's Apple devices in a specific area when the police want. Though various major restrictive net laws (often renamed and attempted again) did not always pass because of outcry, the U.S. and other governments did not hesitate to just start censoring whatever parts of the net they felt like (supposedly criminal sites) and punishing sites' owners even just for doing hyperlinks to average web homepages, blogs, posts, etc. It was good to see others from the whole political spectrum involved in outcry, part of which was begun by the late and great Aaron Swartz, who started the Demand Progress organization and "hacking politics." Since then, not only does Demand Progress report CISPA is back, but EFF reports that secret TPP negotiations (by politicians and who knows who else) are continuing, which would have many unjust effects, including a net more heavily controlled by governments and large companies, with an interest mostly in their "rights" and few/none of common citizens/netizens' rights. Good news on a smaller amount of legislation due to outcry is Congress' consideration of the USA Freedom Act to scale back NSA monitoring... but some hackers think if that passes, it would just be circumvented, as governments already circumvent laws when they can.

Some would argue it is not enough to "hack politics" in specific cases, but that political norms/processes must be hacked - at least to make politics more egalitarian and meritocratic (not special interest-controlled) and to restore freedom, civil/human rights, etc., to how they were intended for free societies. It is good to contact your representatives if they will listen, but it is important to spread the word to as many people as you can, like Aaron Swartz and the people he inspired to rally did, or like Mohandas Gandhi and Martin Luther King. History shows freedom erodes unless people take a stand sufficiently.

The larger good news this year was the growth of hacker conventions (of various focus), hackathons (including in mainstream companies), and the increased condoning of hacking, with even the U.S. president proclaiming a National Day of Civic Hacking - hacking is becoming more socially acceptable! It remains to be seen if this is just about what large organizations can get from hackers, or if organizations are starting to like hacker culture/ideals.

I continue to enjoy reading *2600* for technical aspects that interest me, and even for finding out about some hacker-related social issues that may not be widely known at the time. Thanks again for decades of *2600* and keep up the good work!

Happy Hacking.

darwin

The Digests

Dear *2600:*

First of all, thanks for the great mag, and thanks for making it available via Nook/Kindle. Any plans to make more of the annual digests available as DRM-free EPUBs? I would much prefer to buy them directly from you guys in that format rather than going through Barnes and Noble. I bought Volume 29, but it appears to be the only one available in that format. Thanks!

J

We do indeed plan on continuing with the release of more volumes. In fact, we're going ahead with a plan suggested by a reader in our last issue to hopefully speed up the process significantly. Look for the details in one of our house ads. In addition, Volume 30 should already be available at the time of this printing. As for the EPUB format, we'd like to continue with this. Surprisingly, not very many readers chose this format, apparently opting instead for PDFs.

Dear *2600:*

On page 41 of issue 31:1, sol mentions an idea regarding lifetime subscriptions for the yearly digests.

You mention that it is a great idea, but would most likely be applicable to the PDF version, as you do not have access to the Kindle customer data.

How is this a problem?

While Amazon would most likely not have a system to offer a lifetime subscription to a magazine, surely *2600* could come up with a system to disperse Kindle (and even Nook and EPUB files) to those who have such a subscription, perhaps with a website the subscribers have access to and a mailing list so that the lifetimers can be updated when new issues are available.

As for the editing and creation of these annual digests, I have done a lot of work in the field of converting physical books to digital books... even ones where I had to manually copy down the words from the source.

Let me know.

Variable Rush

We intend to look into every possible way of doing this, but the main problem with formats like Kindle is that we need to do a crazy amount of proofing to make sure the OCR scans are completely accurate. Much of this requires knowledge of what was in the original articles, and the entire process takes substantially longer than formatting pages into PDF form. The plan here is to get at least part of this done quickly, and the idea presented is the best one so far. It also will help us ascertain the interest level, so we can figure out just how much time is worthwhile to devote to future development of the archives.

Critique

Dear *2600:*

I have been an on and off reader of *2600* for some time. It depends on if I can find the magazine in the store. As I have gotten older, I have noticed that the magazine has not. Today I logged on to your website for the first time and realized why. It seems so juvenile.

Lock picking: How many times has this been covered in *2600* the magazine?

Phone Phreaking: Did we not cover that back when we actually had land lines?

Why have you not moved onto something more glamorous like:

1. "how to disassemble an iPhone."
2. "how to root an iPhone."
3. "how to remove the glass from an Android phone."
4. "lock penetration of the HID electronic locking systems."
5. "how and why Bitcoin works."
6. "how to hack a CISCO router."

Just some thoughts as I sit here at 5:30 in the morning.

Chris

Well, hopefully by the time the sun came up, you came to the realization that we have, in fact, covered a number of those stories over the years. There's nothing stopping us from covering even more of them if people write the articles and submit them. But your main problem seems to be in what we've actually spent time on in our issues. First off, we're not sure how you reached these conclusions when you "logged on" to our website, as you won't find articles from the magazine there. You seem to be under the impression that we've printed a lot of lockpicking articles when we're constantly hearing about how we don't print enough. (Again, this reflects the number of submissions on the topic that we get.) As for phone phreaking or anything else you consider outdated, there is a lot to be said about history and how systems of the past and present tie together. Again, we haven't printed that much recently on phone phreaking and would like to have more, both focusing on present day technology and the systems of the past. This is how we learn about features, possibilities of new developments, and weaknesses. Not to mention it's a hell of a lot of fun. So we'd like to advise you to lighten up a bit and see if there's anything you actually like in a current issue. Maybe there isn't. But we like to think that we still encompass the spirit of hacking in our pages and reflect what some of the more creative voices in our community are saying.

Dear *2600:*

Your code repository on 2600.com is woefully out of date. The last update is from 25:3. Is this because you now expect people to buy digital versions of the magazine if they want the code?

This forced me to type in blerbl's very nice "worlistgenerator.py" from 31:1. I could find no explanation for this code, as it does not go with either of the articles around it, or, really with the "Automated Target Acquisition" article on page 58 where blerbl is mentioned. OK, it sort of goes with that article, but not directly.

For readers who might be wondering, "wordlistgenerator.py" is a nice little text scraper. Point it at one or more "targets" (websites, files), pick a regex wordlist rule from the menu, and collect some interesting strings. Thanks, blerbl!

Sh0kwave

We're sorry about not updating our code repository in such a while. We're definitely going to get on top of that. As for the code you saw in the last issue, that was meant to be used in conjunction with our article on "Robbing the Rich Using Bitcoin," which immediately preceded the code.

Experiences

Dear *2600:*

I have been experiencing something very usual for the last two weeks. I have been hearing things in my head asking me for a website that I own. I registered this domain on Christmas Day and since then I have been working on developing it. I read that it is possible to make people hear things though V2K, virtual telepathy, using a microwave auditory effect. Have you ever discussed this on *Off The Hook* or *Off The Wall?* Has anything pertaining to this been published in *2600 Magazine?* I'm not sure who to turn to regarding this matter. I'm a big fan of *2600* and your radio shows. I was hoping you could give me some information about this or possibly discuss this on one of your future radio shows. Someone is abusing this technology and trying to extort me. Thank you for your time.

David

We've had obnoxious registrars hound us for renewals long before the expiration date, we've been bothered by annoying people who insist on trying to buy our domains from us, but we haven't encountered anything quite as intrusive as this. The "V2K" technology you allude to is a popular topic on the net and it's alleged that it's defined by the military as such: "Voice to skull device is a non-lethal weapon *which includes (1) a neuro-electromagnetic device that uses microwave transmission of sound into the skull of persons or animals by way of pulse-modulated microwave radiation; and (2) a silent sound device which can transmit sound into the skull of persons or animals... the sound modulation may be voice or audio subliminal messages." We should point out that none of this is verified, but we're certain the military would love to get their hands on this kind of technology if it were at all possible. However, whenever hearing voices inside one's head, it's always good to be open to the possibility that something else is going on, hard as that may be to accept.*

Dear *2600:*

I should really thank Anonymous for writing what could have been my own letter back in 31:1, since I have recently re-entered the world of IT employment after years of manual labor. The difference being, I actually enjoyed being away from IT the past four years! After graduating from a tech school (one that I loved, I might add, as their focus was on actual learning, not money), I was thrust into the world of corporate IT bullshit. A world of stress, tension, and all around ugliness. Money was the bottom line, which meant working 16-hour days without added compensation, and occasionally getting death threats. To get away from all of that, to actually have a job doing "grunt work," was a treat. I could enjoy computers again, since I was only playing around with them in my free time, and not struggling to make them work to keep from being yelled at. Hell, I'll be honest, I worked on a boat all those years! I was breaking ice, shoveling snow, and taking green water up to my knees on the bow... and I loved it. I thought I would never again return to the horrors of IT.

Yet, as Anonymous pointed out, there's always the issue of money. I couldn't survive on ten bucks an hour, no matter how much I loved my job. But I was lucky. An IT job opened up at a school and I was fortunate enough to land the position. Now I work at a place that encourages learning, a place that understands the true definition of "hacker," a place that prides itself on technology. So, finally, at 33, I'm a married man who gets to play with computers all day and teach kids about technology, and to watch as their eyes light up when they take a computer apart and put it back together. No, I'll never get rich working there, but you really can love something *and* make it your career. How's that for a happy ending?

To reiterate what Anonymous said, thanks to *2600* for keeping the hacker spirit alive, and I'll see you at HOPE X.

Screamer Chaotix

You raise some excellent points regarding employment. We find that the people who really excel at things have had a variety of experiences, often seemingly unrelated to each other, but all of which form a part of their overall story. This is an extension of the experimentation we are always encouraging within the hacker world. It's often necessary to experiment in life itself in order to figure out a direction. It can be risky and scary, but if you maintain a healthy dialogue with yourself, you can benefit greatly from this approach.

Dear *2600:*

Re: "Relax, We Bought Security," Wananapaoa Uncle wrote an amazing article on SMB (small-medium business) security. I walked out of my last job for exactly these written reasons. Third party security contractors have no idea how daily business operations and production up-time work. The contractors get the security audits because the company can point to them if there is a security breach, while not being personally responsible.

In my case, a security audit was being done by the same company that installed previous systems. One of my roles was managing and properly configuring these systems, which typically deployed with default passwords and configurations. Yes, these same folks were the "security professionals" running the audit. Said company's name has a dictionary definition of "spread throughout." I let a sad chuckle out reading that and applying it to their business model.

Pic0o

Dear *2600:*

This is getting really old. I'm not normally one to complain about how retail shops display their wares, but this is the third time I've done so in *2600*... about the exact same issue. After my last such letter was published, the local Barnes and Noble store (#2832) actually corrected how *2600* was displayed and it could be seen easily without needing to search behind other magazines for it. It seemed like a logical way to display a magazine, although I'm not a professional magazine rack manager. Once again however, it's back to the normal "keep it hidden" method. I recommend *2600* to everyone I know, and recently a friend actually went to purchase it but could not find it (even though they had numerous copies - if you weren't already aware of where it generally gets stashed, then you could be searching for a while).

This is getting old, and I'm tired of complaining about it. You often talk about having to pay for lost or stolen issues. I'm curious how many are reported as losses that are actually just scattered throughout the display shelves that even the employees can't seem to find. I always fix them, but they always seem to lose their way again. Perhaps the 20 plus brands of men's magazines with hot women in bikinis on the covers are causing them to wander.

Do you have any recommendations that might help with this? I would really like for people to be able to find *2600* when I suggest it. Not everyone is comfortable asking for employee help to find a hacking publication.

Thanks for all the great brain candy.

ghostguard

This is a difficult problem to solve, since it really only takes one person with a grudge to create this situation. In many cases, we can't even be sure it's someone working for the store in question. We have many enemies and powerful ones at that. So it's not too unreasonable to assume they would stoop to the level of actually hiding our issues to keep people from seeing them. We need people like you to counter this. Every time it happens, it needs to be brought to the attention of management. If they're the ones doing it (which doesn't make a lot of sense for them), they will want to stop being questioned constantly and will likely cease the practice. If it's somebody from outside who's doing this, perhaps the store will manage to catch them in the act. The important thing is to get it on their radar. Silencing people/publications is never the way to make a point and that needs to be made crystal clear.

Dear *2600:*

Here's the story of how I inadvertently got my cell phone into eavesdropping mode:

On my way to the airport, I left my cell phone on the airport shuttle bus. The next morning, not being able to find my phone, I dialed it in order to locate it by hearing the ringtone.

Instead, I did not hear my phone ring, I heard someone talking! It was like when you pick up your phone at the exact same time someone is dialing you. But the other person was in the middle of a conversation, and I could only hear one side of it. She was talking about intersections and addresses, and stuff like that. Totally confusing to me. After listening for a few minutes, trying to figure out what was going on, I hung up and redialed.

This time, the shuttle operator answered normally, and informed me that I had left my phone in the shuttle. I made arrangements to pick it up when I returned.

That's when I realized that I had been eavesdropping on her phone call to her dispatcher from my cell phone that had been somehow switched to transmit mode. I don't know if it was my newly-purchased prepaid cell phone that did it, or what.

Here's the part that I found so interesting: the quality of the transmission while my cell phone was in eavesdropping mode was outstanding. Normally, cell phones break up, the sound quality is poor, you almost have to yell sometimes. This was like I was in the car with her. Perfect transmission, like a professional sound stage.

Just thought I would let people know that your cell phones make Very Good eavesdroppers.

Margaret

New Stuff

Dear *2600:*

I'm contacting you from a local start up called notrace.im. We have been working on this product for a while now. We just launched not too long ago. We were wondering how to get an article published with you guys. What we launched is a private messaging app. We were called the Snapchat of texts but better because you don't need an app in order to receive text messages. Some of our features include self destructing messages, ability to send messages to email or most U.S. phones, ability to unsend messages, ability to send anonymous messages, and the security of knowing nothing is stored on your device but a dead link. Please give us a look and let us know what we can do. We are at website notrace.im and available as an app on Android and at the Google Play store.

nico

It's more likely that someone will review your service and write an article about that from a hacker perspective. You're welcome to send us an article describing what it is you do, but it's probable we'd prefer to print something written from the view of someone not affiliated with the company. But please send us something anyway, and if it's interesting and doesn't read like a PR piece, we'll certainly consider it.

Dear *2600:*

Hello, I'd like to let you know about Privacy Eraser Free, a freeware tool to keep privacy on a computer well protected and secure. The software allows cleaning up browsing history, wiping disk data down to unrecoverable state, and removing traces left by applications.

Typical computers usually have a lot of hidden doorways a cyber-trespasser can use to access personal or protected information. Privacy Eraser Free helps maintaining the security of a PC by regapping those breaches. In particular, the app permanently deletes visited URLs, browsing history, saved authorization data, Windows run history, search history, open/save history, recent documents, and more. It offers secure file deletion and disk wiping mechanisms to ensure deleted files remain deleted. Moreover, it helps cleaning leftovers of many popular applications that often stay in the system and keep cluttering it even after the app itself is removed.

With the flexible, highly customizable, and open plug-in architecture of the tool, users can even customize their own exclusive Privacy Eraser! Scheduling capabilities and the built-in performance booster help users to speed up Internet surfing and browsing and boost their PC's performance and stability.

I hope this information could be a good topic for a post or article that will be of interest for your readers.

Let me know what you think! If you have any questions or need additional information, please let me know.

Julia Wunder
Cybertron Software

OK, we know this was a blatant product pitch, but thought it was interesting enough to share. The features sound noble enough, but are you sure you want to call your product "Privacy Eraser?" That sort of makes it sound like it's privacy you're getting rid of, rather than the opposite. Just our humble opinion.

Dear *2600:*

My name is Nick Grey, and I am a professional social media manager.

I have something to offer that might interest you.

I have a suggestion for your Twitter channel https://twitter.com/2600 I can add to you Twitter channel, with more than 2000 followers.

The high rating of your Twitter channel helps increase the credibility of the services which you offer.

The cost of the service is only $60. I work without pre-payment; payment is carried out after all the work is done. You pay only once and all Followers are added permanently. No Twitter password is required. No harm to your chanel. Please let me know if you are interested.

If this does not interest you, I'm sorry to have bothered you! To unsubscribe click here.

Have a good day!

Nick Grey

Rather than clicking there we decided to paste here and share this absurd pitch with the world. Does anyone actually fall for this nonsense? Are there really people and organizations so desperate to have followers that they will pay to collect fake ones? We know we should never be surprised by these things, but for future civilizations who stumble upon old copies of our magazine and use it to judge our society, let this be the defining point of just how stupid some of us actually were.

Dear *2600:*

We noticed that the HOPE X domain name on the cover of the latest *2600* was similar to a domain name we own. You have 62 X's, we have 63 X's.

We just wanted to let you know that if anyone types in 63 X's, they will be taken to this web page: http://xxx.xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.xxx/.

Unfortunately, HOPE X falls on the same days as QuakeCon, so we won't be able to attend it - maybe next time. Members of our local hackerspace (Makers Local 256) should be there, though.

Anyway, just wanted to inform you about this redirect. We don't know if it was needed or not, but we wanted to help out if it was. (We also have 63 C's (.cc), so hence the site name.)

Charlotte & Jesse
http://c63industries.com

This is the coolest thing ever and we're thrilled that you put in the redirect for HOPE X. We're also pretty amazed that you took the time to count the number of X's on the cover and that we happened to be just one X shy of your site. This has really been a fun year for domains.

Hacking the SanDisk Connect Wireless Media Drive

by ook

So I bought this cool little device called a SanDisk Connect Wireless Media Drive. It's a cute little thing, weighing in at 76g, and nicely palm-sized at 6.5cm square by 1.35cm deep. It's got solid construction and, depending on the configuration, can produce a 50m Wi-Fi field of up to 320 GB (the 64 GB model with a 256 GB SD card, which is the market maximum at time of writing), accessible to any Android or iOS phone or tablet. The device creates a Wi-Fi network of your desired configuration, and can even connect to an existing Wi-Fi network. You connect your phone to it, or to a common network, and you're good to go. Unfortunately, this little hockey-puck of awesome has a couple of major flaws: first, it's got no SMB server, nor any standard NAS protocol to speak of. Second, it doesn't support MTP - so if you've got it hardwired into a computer, you can't access it from your phone. This obviously won't do. Assuming this is a Linux embedded something, I decided to portscan the little beast. What was open:

```
* 21  (FTP)
* 23  (Telnet)
* 79  (Finger)
* 80  (HTTP)
* 113 (AUTH)
* 513 (LOGIN)
* 514 (CMD)
```

FTP responded immediately to the admin credentials from the Media Drive app for my phone - so it's easy to access that way. Telnet also worked, giving an option for doing other interesting stuff. Let's have a look at the system:

"uname -a":

```
Linux Media_Drive 2.6.35.3-899-
g9b1a262 #18 PREEMPT Tue May 28
14:14:33 CST 2013 armv7l GNU/Linux
```

"cat /proc/cpuinfo":

```
Processor : ARMv7
Processor rev 5 (v7l)
BogoMIPS: 799.53
Features: swp half thumb
➥ fastmult vfp edsp neon vfpv3
CPU implementer: 0x41
CPU architecture: 7
CPU variant: 0x2
CPU part: 0xc08
CPU revision: 5
Hardware: Freescale MX50
➥ Platform - Nimbus@QSI(WG7311-
➥2A) Ver: 1.1.8
Revision: 50011
Serial: 0000000000000000
```

"cat /proc/meminfo":

```
MemTotal: 125496 kB
MemFree: 12152 kB
Buffers: 1816 kB
Cached: 66120 kB
SwapCached: 604 kB
Active: 27196 kB
Inactive: 74268 kB
Active(anon): 14664 kB
Inactive(anon): 19140 kB
Active(file): 12532 kB
Inactive(file): 55128 kB
Unevictable: 0 kB
Mlocked: 0 kB
HighTotal: 0 kB
HighFree: 0 kB
LowTotal: 125496 kB
LowFree: 12152 kB
SwapTotal: 151720 kB
SwapFree: 150976 kB
Dirty: 0 kB
Writeback: 0 kB
AnonPages: 33096 kB
Mapped: 7324 kB
Shmem: 276 kB
Slab: 6592 kB
SReclaimable: 2168 kB
SUnreclaim: 4424 kB
KernelStack: 1376 kB
PageTables: 1008 kB
NFS_Unstable: 0 kB
Bounce: 0 kB
WritebackTmp: 0 kB
CommitLimit: 214468 kB
Committed_AS: 899888 kB
VmallocTotal: 1761280 kB
VmallocUsed: 1152 kB
VmallocChunk: 1756732 kB
```

"cat /proc/partitions":

```
major minor #blocks name
179 0 61071360 mmcblk0
179 1 4096 mmcblk0p1
179 2 262144 mmcblk0p2
179 3 204800 mmcblk0p3
179 4 60584960 mmcblk0p4
179 8 125058048 mmcblk1
179 9 125041664 mmcblk1p1
```

So it's based on an armv7l, specifically a Freescale MX50. That means a Cortex A8 running at up to 800 MHz.

Next step is to gain root. The shadow file actually contained a password hash for root, so I went ahead and brute forced it with about five minutes of good ol' John the Ripper's time: sqn1351. Telnetting in as root succeeded. Once I had root, I was able to fix the sshd configuration:

```
chmod go-r /etc/ssh/ssh_host_*
ln -s /etc/rc.d/init.d/services/
➡sshd /etc/rc.d/init.d/services/
➡S99sshd
```

I was also able to set up a little SSH/SCP love:

```
ssh-keygen -t rsa
mv .ssh/id_rsa.pub .ssh/authoriz
➡ed_keys
```

I then copied the key into the FTP area for use with PuTTY and WinSCP (removing it later):

```
cp .ssh/id_rsa /var/ftp
```

I wanted the device to have a host name on the network, too, so I added the appropriate section to /etc/dhclient.conf (wlan0 is the AP, wlan1 is the client):

```
interface "wlan0" {
  send host-name "puck";
  request subnet-mask, broadcast
➡-address, time-offset, routers,
➡  domain-name, domain-name-
➡servers, host-name, SIP;
require subnet-mask, domain-name
➡-servers;
}
interface "wlan1" {
  send host-name "puck";
  request subnet-mask, broadcast
➡-address, time-offset, routers,
➡ domain-name, domain-name-
➡servers, host-name, SIP;
require subnet-mask, domain-name
➡-servers;
}
```

Now that you have working SSH, you can use Dokan (Windows) or sshfs (Linux) to mount the Wireless Media Drive to your PC. However, neither of these stream well with the limited bandwidth of the device. Fortunately, XMBC handles all that nicely. I also keep a small array of btsync nodes, managing a gig or two of personal stuff... so I figured, hey, why not one more? I downloaded the latest ARM build of btsync (symlinking it to /sbin), and added the following init.d script:

```
#!/bin/sh
 if [ ! -x /sbin/btsync ]
then
if [ ! -f /sbin/btsync ]; then
echo "BTSync not found"
else
echo "BTSync permissions not set"
fi
exit 0
fi

if [ ! -f /root/.sync/config.json
➡ ]; then
echo "Please create a config.json
➡ in /root/.sync/config.json"
echo "See http://btsync.s3-web
➡site-us-east-1.amazonaws.com/
➡BitTorrentSyncUserGuide.pdf"

fi
 if [ "$1" = "stop" -o "$1" =
➡ "restart" ]
then
echo "Stopping the btsync server
..."
killall btsync
fi
 if [ "$1" = "start" -o "$1" =
➡ "restart" ]
then
echo "Starting the btsync server
➡..."
/sbin/btsync --config /
root/.sync/config.json
fi
```

In sum, the SanDisk Connect Wireless Media Drive is a neat little headless Linux box. If you could construct an ARM toolchain for yourself, you could use it for all sorts of personal server applications: Samba, household Bittorrent, household remote control. Since it has two 802.11n devices, you could probably make a relay out of it.

If you need a tiny mobile media server, this is certainly a good and flexible option for the time being. Now if you'll excuse me, I'm going to try and get a JRE running on it; I work as a programmer on a Java-based XML CMS for publishers, so obviously, I'd like to try to get it running on everything!

TOILET HACKING

by Toilet Fixer 555C

Most hacking is done on computers because that's where the technology is - we live in a digital age and so most technology has a chip in it somewhere. But some things stubbornly refuse to be computerized. Consider the lowly toilet. Now, I'm aware that in Japan they have remarkable "smart" toilets which do... things. I'm not that familiar with them but I'm very curious. Anyway, the old-fashioned dumb (i.e., American) toilet moves something we like to call "waste" from our proximity into a collective depository where all the "waste" from the neighborhood can be mingled and purified (hopefully). If that's not possible, it's hoped that the waste can be rendered harmless or, as a last resort, pumped so far away that it will become somebody else's problem.

To do this, we need water - lots of water, as any intelligent person who watches a toilet flush should be able to figure. It's this water issue that creates some problems and presents some opportunities, which in and of themselves aren't evil but certainly attract a particular type of person with evil intent.

I'm not going to go into all of the legal and technical issues associated with the invention of the "low-flow toilet." The animated television program *King of the Hill* had an episode (season 4, episode 22, "Flush with Power") that thoroughly outlined the challenges faced by anyone attempting to install and use a toilet designed to use less water. The TV show even explained how crooked politicians and crooked industrialists can work together to make everybody miserable. Unfortunately, the program did not go on to explain how to modify (hack) a low-flow toilet to get it to flush using more water. It implied that one might wish to just install a "high-flow" toilet, but the problem is that those things are just not so easy to find and can be expensive and/or illegal. And therein lies a tale....

My own personal journey to toilet outlawry began with the ceramic "tink" of an old, old toilet tank breaking cleanly in half due to my failing to comply with the instruction, printed clearly on the inside of the tank, warning me not to over-torque the nuts that hold the tank to the bowl.

But wait... before I go further, I think I'll briefly review toilet construction (this will apply to all known toilet types, keeping in mind that European toilets are vastly superior to American junk, and Japanese toilets are, apparently, using NASA technology, so they won't be mentioned here). The tank is a big ceramic, uh, tank that sits on top. The bowl is the thing you sit on. The tank fills with water, and a float causes a float valve to close when it's "full." Flushing opens another valve (the flapper valve), then all the water dumps into the bowl, and the laws of physics and basic rules of hydraulics cause the old, yucky water to be carried away into the pipe that goes to the sewer (or someplace) and new water replaces it. It's pretty clever.

The power of the flush depends upon the amount of water that moves from tank to bowl. This water is lost - it will not come back again except through rain that came from the ocean - I think you get the idea. In places (like the southwestern United States) where there are drought conditions most of the time, it seems reasonable to try to minimize the amount of water lost through flushing. If you live in a place with plenty of water, it's no problem. But water is like air; it's not a big deal until you don't have any. The issue of water management is very, very emotional wherever water is scarce - political, even. Laws are passed. Regulations are posted. I'm hoping that the reader will see a glimmer illuminating the resemblance between this phenomenon and numerous other issues relating to high technology. Water, in a way, is like bandwidth and government attempts to be "fair" in assigning ownership often end up assigning that ownership to whomever has the most influence with certain politicians.

One easy way to "spread the burden" of water conservation is to create a toilet that uses less water. But an even easier way to do this is to create a toilet that appears to use less water, but actually does not (as was described in the

King of the Hill episode mentioned above). Furthermore, it's really easy to simply strike the problem "at the root" by telling the people who make toilets to build them so that they use less water, and the easiest way to do that is to adjust the float so that less water collects in the tank, so that less water moves through the toilet with each flush.

In other words, government is attempting to solve a problem, not in a direct, possibly disruptive and probably expensive way, but in a cheap, dirty, easy way that does not work. This is where the hacking instinct begins to kick in - for some of us. Something that has been deliberately broken in order to create a phony fix for a problem presents no moral dilemma to a hacker. It needs to be "un-broken," period. While many problems involving computers are just too darn complex for most people to be able to grasp easily, I don't think that this toilet thing is difficult to understand. This is a good example of why hackers do work on somebody else's equipment, often using somebody else's tools, in somebody else's back yard. It's simply a question of what takes priority; random lines drawn on a map, or the notion that "functional" is better than "broken?"

When my toilet tank broke, I went to the Giant Building Supply Store to get a replacement. They had only one kind - low-flow. They had cheap low-flow and expensive low-flow. I have learned since then that special, power-flushing toilets do exist, but they have to be special ordered and installed, I assume, by a special technician from Japan. The hell with that.

I bought the cheap low-flow tank, since the expensive ones were expensive only because they had fancy shapes and colors. I took the tank home and installed it. It wasn't hard. You just plunk it on there and tighten (not too tight!) those pesky nuts. That is when I began to really appreciate the creative genius that gives us programs like *King of the Hill*. The toilet now acted in strange and unnatural ways. It simply could not flush away the "waste" without requiring a second flush, and sometimes a third one. The tank, for reasons that might be discovered on some government website, had the symbols "6 lpf" stenciled inside of it like an Egyptian tomb. It means that this so-called "low-flow" toilet consumes 6 liters of water per flush - which means that it consumes twelve liters in two flushes and a three-flush job will cost humanity the use of eighteen liters of water. There is something spookily official about that stencil, and like all spooky, official stencils it pissed me off.

Here is where we get into the actual "hacking." The problem with toilet hacking, you may be surprised to discover, is that there is a law prohibiting the alteration of low-flow toilets by plumbing professionals in order to allow them to consume more water. I don't know for sure if such a regulation could be used against "a private individual," but it seems logical. When I brought the low-flow tank home and mated it to a high-flow bowl, I may have invalidated my warranty right there and ran afoul of the government. No, seriously. If I didn't do any crime at that moment, then the question is what sort of thing did I do? I surely violated the spirit of something-or-other and, I assure you, I wasn't about to stop there. Show me any well informed adult who thinks that we will never see further toilet regulation in America and I'll show you an individual who has only limited experience with building codes and enforcement of those codes. As the "end consumer" (so to speak), I am the last bastion of "freedom" in toilet modification, but that bastion is under assault just like any other bastion of freedom to do anything. I honestly don't know what kind of legal lines I did cross or may have crossed in my attempt to get this toilet to work. It's easy to say "none" but I don't know. I've "worked with" government agencies and I don't trust them. Sometimes, you can't know what a "violation" is until you do it.

I now had a poorly functioning toilet, even though I had "repaired" it. It not only failed to flush properly, it also required me to hold down the flush handle while it flushed. This problem was partially solved by installing a self-closing replacement flapper valve that could be adjusted so that it allowed more water to pass. The kind I used is made by a company called Fluidmaster - the Flusher Fixer Model 555C. I also replaced the plastic flush handle with a metal one. Now, you're probably thinking that it may have been cheaper to buy the power-flush toilet rather than modify this one. Maybe so (I doubt it), but this is the same argument presented to all hackers, hot-rodders, and assorted hobbyists by various moms, girlfriends, wives, and big brothers throughout history, right? So it's not a good argument.

It leaves out the part where I take my toilet destiny into my own two hands.

As I installed the Flusher Fixer flapper valve, I notice that it actually came with a system (using holes and plugs) that looked like something from the notebooks of Leonardo and was designed to allow you to adjust the amount of time the valve stays open. Fantastic. As any hacker can tell you, for every well-meaning idiocy there is a practical tool to kick its ass. But even though I now had a flapper valve that would allow more water to pass and closed itself when needed, one (major) problem remained. No matter how much I tweaked the flapper valve, and no matter how much I tweaked the float valve (the valve that fills the tank - the flapper valve empties it), there was a real, solid limit on how much water would flush through the bowl per flush. This limit wasn't the size of the tank (thank God) but the height of an infernal "standpipe" that, uh, stood in the middle of the tank and simply drained away any water that entered the tank and rose above the top of the standpipe. In other words a simple drain, placed at the "correct" height, making "over-filling" impossible.

For some.

The real trick here would be to figure a way to extend the height of that pipe. I decided not to simply go shopping for a new pipe. You might wonder why, but I suppose it's just my mechanic's instinct. I guess I should disclose that I am an aircraft mechanic, among other things. So I know that to take something apart, especially something involving a liquid, is to invite trouble. Specifically, leakage. You may scoff, but while you are scoffing at my hesitancy to simply swap out the component, any attempt to remove the funky old screws from the base of the standpipe will cause the tank to move, and that motion alone may start a leak near those blasted nuts - the same ones that broke the first tank and started us all down this road to toilet hackery. So I'm going to make a good decision now and *not* mess with those screws. Instead, I'm going to extend the height of the existing standpipe. As a bonus, this will allow me to "undo" the work if the total weight of the water in the tank somehow causes leakage at those infernal nuts or some other problem.

My first effort at extending the standpipe involved using an epoxy putty (called "Mighty Putty"), which is labeled "waterproof" and is (supposedly) used for plumbing repair. This didn't work at all, as the stuff is almost impossible to form into a tube shape by hand while awkwardly working inside a toilet tank. After discarding the rapidly-hardening putty, I noticed that the plastic tube that had held the putty was about the same diameter as the standpipe. I measured it and, *begorra!*, 'twas the same diameter. Now the question was - "How to attach the tube to the standpipe and make it waterproof?"

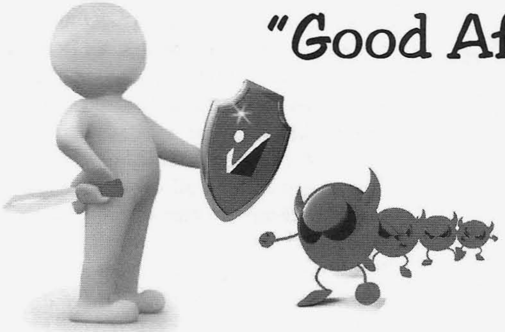
Ah, yes. Now, sometimes it is necessary *not* to give in to prejudice. My natural dis-affinity for duct tape made me wary, but a new kind of duct tape - a high adhesion variety from the people who make Gorilla Glue (called Gorilla Tape) gave me hope that this whole thing could be done without putting too much stress on those flimsy nuts at the bottom of the tank. Remember - I'm trying to avoid stressing those nuts and the surrounding seals (gaskets) and the surrounding porcelain. Any foul ups and I could a) break the tank, b) start a leak, c) break the bolts that the nuts thread onto. Any of these is an immediate "game over" - requiring a trip back to the Giant Building Supply Store.

I cut the plastic tube to the right length by "eyeball" measurement and carefully put *one* layer (with a quarter inch of overlap) of Gorilla Tape onto the "extension" and the standpipe, thereby joining them together with an outer "sleeve" of tape. One quick flush-and-fill later, I found that I needed to adjust the fill valve (it's adjustable with a simple screwdriver, since this is one thing that can cause a toilet to "run" and will get complaints from end-users), then I inserted one of the plastic pins into the Flush Fixer 555C (the flapper valve) in order to delay its closing long enough for all the water to be flushed. Once this was done, I not only had a tank that would fill with ten liters of water, it would flush all ten liters. Yeah baby. I hope you won't be shocked if I mention that this number is still low compared to "world averages" for flushing!

A simple ten-second countdown and the first flush of a new high-flow age had begun. My new and jazzy hot-rod toilet can now consume, on a good day, just about anything I usually put in a toilet - in one flush. It won't flush away apples or pineapples or watermelons or anything that Thomas Crapper's original Victorian toilet could flush, but it's all right for now. It also doesn't consume twenty liters per flush, as some very old systems did, nor does it consume twelve or eighteen liters per "incident" as this very same toilet did before I modified it. Please note that I did not want to create some kind of monster in my lab - I only wanted to restore what had been unfairly taken away.

So here's the take-away from this window, kids. Try this at home. But be warned - I don't know what, if any, laws you might be breaking (and neither does anybody else) doing this to your own toilet. But if you go into business modifying toilets, I have a feeling you will definitely feel the wrath of Big Brother (this would be a violation of federal law). But I do not believe that I did anything wrong. The water I use to flush my toilet is, I believe, less than when I had a "proper" low-flow toilet, since the "low-flow" requires multiple flushes. But that isn't really the point. The point is that some idiot, somewhere, dictated something and the result, incredibly, was that my toilet wouldn't flush properly. Not only did this have very little to do with sewage management or water management, it actually ended up using more water, as we all learned from *King of the Hill*. I do understand that water is something that we all share. Water can never be used, only borrowed. The same water that rained on Socrates flows in rivers today. I know that I have an obligation to "play nice" and not hog it, and I know that some people, if confronted by my modified toilet, might jump to the conclusion that I am, in fact, being a pig and using more than my share (especially if the word "hacker" is thrown around). But, in fact, I use less water - in the long run. Unfortunately, the phrase "in the long run" usually indicates that something is just beyond the grasp of the herd. Politicians know this and will provide a "short term" solution no matter what. So it goes.

I don't know what stupidity I may encounter tomorrow. But somehow I know that my first reaction to it will not be to write to a politician. I will want to do what a few hardy souls have always done. I will want to start hacking.



"Good Afternoon. This is Your Fake AV Calling."

by lg0p89

Background

Early in the summer of 2013, my wife's son called for his mother. He noted that the computer said there was a problem. Naturally, we went to see what the issue was. After heading downstairs, the laptop screen showed a rectangle with flashing lights in the lower right hand corner stating the app was running a scan. Also, there was an attention grabbing banner warning that the computer was infected and immediate action was required to fix the issue. All you had to do was just click on the yellow warning sign, which just happens to be next to the bar scrolling through all of the viruses allegedly found on the computer, along with the malware and porn. Oh, and by the way, yes, there was a fee involved to fix this. Nothing in life is free.

The young family member was a victim of ransomware. Of course, he denied clicking on anything he was not supposed to or visiting any adult-oriented websites. The computer was not chock full of malware, viruses, and porn. Somewhere along the way, the computer had been infected with ransomware. Prior to this, his mother elected to ignore my repeated requests to renew and update the anti-virus (AV) package as the expiration was quickly approaching. How does the quote go regarding a horse and water?

Definition

Ransomware is a form of malware. There are two primary types of ransomware. These involve either, once infected, locking the system up where the user is not able to access the files or programs, or encrypting the user's system, such that they need to have the password to open and access the system. This also has been known as scareware. (Russinovich, 2013)

General Operations

The bottom line of this attack is to force the user into believing their system is totally infected and has to be cleaned immediately. The user, for example, does an Internet search. There is a site listed that looks intriguing and "exciting." The user clicks on the site, not knowing it is not remotely what it appears to be. Immediately, the ransomware is installed as a register entry. Until cleaned, every time the user starts or restarts the system, the warning as described earlier comes up. This warning may be a pop-up window, a new website page, or another form that appears legitimate. The ransomware may lock up your system and/or files (Zorz, 2013) until you pay up. (Leyden, 2013) People generally are so stressed out that they just pay and hope they get their system back. That is a bad idea. Now they have your credit card number and your computer's accessibility. They may continue to demand money, much like a shark smelling blood in the water. Good times are going to follow. The better route is to have this fixed by a professional.

The warning may also state, in order to elicit a quicker response, that illegal activities have been detected coming from your system. This notice feeds into the person's worries and concerns.

Although technology has improved over the years by leaps and bounds (thank you Moore's Law), the method and look of ransomware have not changed much since 2006. The new improvement on the malware lately is with the lockout function. (Russinovich, 2013)

Specialty Add-On

Not all of these are the same. Granted, there is a generic framework that is common. As an example, a seemingly genuine, legitimate website or pop-up shows on your screen. This looks just like the MS or other AV service provider warning. This states you have to take immediate steps to fix the issue.

For fun and excitement (for them), the ransomware engineers have added a menacing voice to the application. Imagine the noob turning on their laptop. The warning pop-up appears listing all of the horrific things that can happen or have happened to the computer. To increase the user's anxiety and the probability they will pay, there is added the threat of imminent loss of the family's pictures and information that won't be able to be retrieved if they don't get this fixed immediately. Their firm will just happen to fix it right now for them for the reasonable price of $xx.xx. Now (here is the fun part), add in the deep, authoritarian voice (think Darth Vader) telling the user everything they have been reading.

Avoiding the Issue

When the user's system is infected, this is potentially a traumatic and stressful experience. There are ways to avoid most of the risk. The users should ensure the AV definitions are up to date. These should be updated frequently. For myself, every time the laptop is turned on the definitions are updated. This only takes two or three minutes at the most, and decreases the risk to the user. As this is being typed, the definition update took all of 45 seconds. The inconvenience to the user in this case is not significant.

The firewall should be left on at all times. This should not be turned off. There really is not a significant point to not having this on. This will provide an additional layer of protection, above the user's knowledge of what not to do to get in trouble in the first place.

If you are receiving emails from UPS or Fedex - along with 30 others in the same email - telling you to open an attachment to claim an undeliverable package, don't open it. The user should not open an email or attachment that looks to be suspicious. Too often at work, one of the users receives one of these emails and opens the attachment. If you do, you probably will have a bad day after IT is alerted to this. The sysadmin will not be happy four hours later after scanning your system and trying to fix it, only to later ghost the template image onto your system.

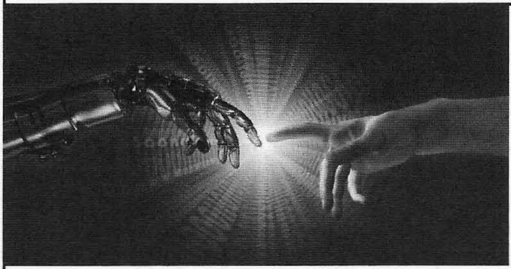
Also, scan your system regularly. This is not harmful and may slow down the system temporarily, but it will still be workable.

Conclusion

Ransomware can be a significant pain to everyone involved. Users need to understand not to click on anything suspicious. If something seems too good to be true or does not make sense, this it is and it probably does not. If the user does slip up, don't pay the deviants who infected your system. It will only lead to more fruitless payments, stress, pain, and yet more data loss. There are ways to lessen the risk to the users from this.

References

- Zorz, Z. (2013, August 8). *Reveton changes tack, relies on fake AV*. Retrieved from `http://www.net-security.org/➥malware_news.php?id=2557`.
- Russinovich, M. (2013, January 7). *Hunting Down and Killing Ransomware*. Retrieved from `http://blogs.technet.com/➥b/markrussinovich/archive➥/2013/01/07/3543763.aspx`.
- Leyden, J. (2013, August 8). *Child abuse ransomware tweaked to tout bogus antivirus saviors: Crass, fiendish and no doubt a good money-spinner*. Retrieved from `http://www.theregister.co.uk/➥Print/2013/08/08/ransomware➥_scareware_hybrid_scam/`.



Future Visions

by Jason Sherman

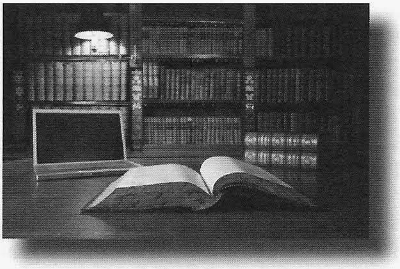
In 1984, I was but eight years old, but I can vividly recollect playing games on a Commodore 64 computer, or creating simple programs, as well as my parents using it for more important functions. Then my father sold this amazing machine to buy a revolutionary new computer called the Apple IIe. My parents, who are retired schoolteachers, loved to teach my brother and me new things, and I was always interested in computers at an early age, either tinkering, programming, playing games, or simply interacting with an interface. When my father introduced me to the Apple IIe, I was bewildered at the things I could do, and as I got older in my teens, I grew more engrossed in what technology had to offer. Being a sci-fi fan, and always enjoying the best movies, TV shows, and books that showed the promise of a technologically futuristic society, I've always been fascinated with the gadgets and software that entrepreneurs have developed over the years.

When the Internet surfaced, I was in college and learning how to build web pages. Again, I was intrigued by the notion that all of our information can be stored in ones and zeroes or a coded language somewhere on a server to share it with the world. Like most techies, I followed the growth of Google, Amazon, eBay, and the rest of the tech giants we have grown to love (or despise) today. Then in 2007, Steve Jobs introduced us to the *Star Trek* style computer in the palm of your hand: the iPhone. Finally, we were able to do prodigious things without being tethered to a desk or having to turn on a laptop. As a kid, I only dreamed of a device that would let me dictate instructions to it, schedule appointments, pay bills, search the Internet for answers, buy things, play games, store files, check the weather, watch a video, send an email, get directions, find a date, order food, send a greeting card, share photos with my friends or family, and so much more. It's actually sad to see kids growing up and taking this powerful device for granted. They just don't realize what it is they are holding in the palm of their hands.

And then to top this off, living in a *Star Wars* future, we now have virtual currency such as Bitcoin to pay for things, instead of credit cards or cash. Who would have thought that society would build a deregulated, secure, non-fee-based, non-governmental currency and put money back in the hands of the people? Many in the past came up with different predictions and a few of them are obviously correct. All of the great sci-fi novels and authors in the earlier part of the 20th century predicted many of the technologies that we have today. It's about time we give credit where it is due. It was writers like H.G. Wells, Jules Verne, Isaac Asimov, Arthur C. Clarke, Douglas Adams, Robert Heinlein, and so many other amazing authors who I grew up with and still admire immensely for paving the way for our imaginations to run wild. These writers spoke of the technologies we have today, and I believe that it was in part because of their doing that we have these gadgets today.

The burning question now is: Where are we headed? Is the singularity truly upon us? Are we going to be living in a world where we live twice the lifespan that we are living now because of organic/computerized organs when they fail on us? With the advent of 3-D printers and prices dropping, who knows, maybe soon we can print a new liver, or a new heart when we need one. Look at the American pioneering futurist Ray Kurzweil, who has all but cured his type-1 diabetes by implementing a calculated diet, as well as using nutritional supplements. Mr. Kurzweil believes the singularity is coming soon, along with the promise of nanobots fixing our broken bodies. Alan Turing, who was one of the pioneers of artificial intelligence, spoke about computers becoming self-aware and difficult to distinguish from humans. Remember Watson from *Jeopardy?* He was hard to beat, and he was just a computer. Now the government and corporations are using Watson for other important functions. It's only a matter of time, and no, I'm not talking about Skynet.

Just take a moment to think about all the software, gadgetry, and where things seem to be headed in this technological world. I wouldn't be surprised if one day soon we could plug in to a machine, with a computer chip embedded in our brains, and be transported to another part of the world, or even the galaxy, with the push of a button into another body that is cloned using our DNA, but is also computerized. With new shows popping up like *Almost Human,* it proves that people believe that is the way of the future: humans working side-by-side with androids, just like Isaac Asimov's *I, Robot*. I for one embrace this future; I welcome it with open arms. I believe that humans have unlimited potential to do things that are only limited by their imagination. By using science and technology together, there's nothing we can't accomplish. I hope to look back 100 years from now to read this article again, with artificial organs in my body helping me stay young and sane. The best part is the human race will be able to continue making the world a better place with science and technology as the singularity comes. Who knows, we may all be living on a different planet altogether in 2054. Only time will tell.



Closing the Schism Between Hackers and the Law

by the Piano Guy

This is an article in response to the one written by Scott Arciszewski (30:4), where he suggests that the only thing good hackers can do is go dark in order to help the world without getting hurt for doing so. He denigrates the concept of being a White Hat, comparing us to condoms (either useful or disposable). What he fails to recognize is that he didn't function as a White Hat, and he was screwed badly as a result.

Let me elaborate here. There were no winners in his story, or the ones like it. And, Scott received a severe punishment that was not warranted. Had he been rewarded rather than punished for what he tried to do, I would have personally felt that all was right in the world. However, there were other ways for him to do what he wanted to do and, had he done them, he would have endured no punishment and gotten his noble goal achieved. Had he not gotten his noble goal achieved, at least he wouldn't have amplified the problem he found.

While this article does not constitute legal advice, I would love to have some of our lawyers chime in on my opinion to see if it holds legal water.

If I found an InfraGard website with a vulnerability, I would consider writing a letter that went as follows:

To Whom It May Concern:

While doing research for a project on Internet vulnerabilities, I have accidentally stumbled across a vulnerability on your website. I have not disclosed this vulnerability to anyone, nor have I exploited it. I have no interest or desire to exploit this vulnerability, or reveal it to anyone that would have bad intent. However, I do realize that by disclosing it to a responsible party, the vulnerability can be mitigated or eliminated, which would be a benefit to you and your organization.

I am not seeking compensation for doing so. I am simply seeking to do the right thing and be helpful as a good Samaritan. Please advise me as to whom I should contact within your organization as a responsible party. To that person or to those people I will provide the information required so they may appraise my finding.

If you are not interested in pursuing a remedy for any vulnerability I may have located, please let me know within 30 days so I may know that I should not pursue any further actions on your behalf. Thank you for your attention.

Scott could have sent a letter like this to the Tampa InfraGard chapter and, if no response was received after two weeks, could have sent this letter directly to the local FBI field office in reference to the InfraGard site.

Please note what this letter does and, more importantly, what it does not do. It makes clear that no harm, blackmail, or extortion is intended. It makes clear that the sole intent is to help close the vulnerability in a responsible manner. It only asks for contact information, and states that nothing will be done until that contact information is returned. Also note that when I say send a letter, I do *not* mean send an email. I mean send a letter. It doesn't have to be registered or certified, but keeping a copy of all correspondence would be a good thing to do, and you would be better to do that on paper than as a recording.

One of four things can be expected from sending this kind of letter. The best hope is that they will call or write and say "yes, thank you for letting us know we have a problem. Give Mr. John Smith a phone call at 321-555-1234 to discuss this matter further." I wouldn't call except to say that you'd like the address to send the information to, and then submit it by postal mail again. Send the information on the vulnerability. By constraining your substantive conversation to written correspondence, you can't be accused of saying anything you didn't say. Get your correspondence in writing, and consider that to be your engagement letter.

Another response you may get is going to be akin to "go away kid, you bother us." At that point, do so with a clear conscience. Don't do more.

The third thing that may happen is that you will get no response at all from all the proper channels. At that point, having made a proper effort, you too might think this was horrible, but you would have your hands tied unless you can get someone in power to respond. That would depend on how many letters you would want to write.

While I think it is highly unlikely that you will get the kind of response where people are threatening you with legal action, you have only written correspondence that says you've done nothing wrong, intend on doing nothing wrong, and are simply asking for a proper way to respond to this find. In Scott's article, he refers to this being the equivalent of knocking on the door, having it swing open, leaving after looking around inside, and then getting in trouble for breaking and entering. What I am suggesting is that what Scott should have done once he had the door swing open is to not go inside, but instead report it to the police.

If you were going to a friend's house and you found the place open and unsecured, looking abandoned, would you go on your merry way or would you call the police to at least keep an eye on the place until the owner could be found? Maybe it is because of where I grew up, but I'd call the police. I sure as heck wouldn't yell out in the streets "hey everybody, look here, an open house." When Scott blew the whistle on Twitter and through other public media, that is exactly what he did, which is what put the site in more danger. To me, that turned Scott from a White Hat to a Gray Hat. If you think I believe he got what he deserved, please reread my second paragraph.

The Hippocratic oath states "first do no harm." If Scott and the other bright folks like him who also have good moral intent state "I found something - someone come please talk to me so I can show you where to go fix it," no one can state that a law has been broken. If the vulnerability is revealed publicly before giving the proper authorities a chance to fix it (no matter how stupid or slow they are about it), then harm is done by revealing that information, and the White Hat nature of the intent can then be called into question.

Here's one final example to drive the point home, and to reference the point of not helping commercial enterprises. The nature of my music business (I don't just do IT security) doesn't require me to have a website, let alone use online transactions for what I do. I music is for sale on iTunes, and I let them carry the load regarding security. But, let's fictionalize here and say that I had my own website "www.ThePianoGuyIsSellingHisMusicOnline.com" with its own shopping cart, user database, and such. Because I'm totally clueless (remember, this is a fictional story), I insist on people creating an account with me before I sell them my music, and I collect Personally Identifiable Information (birth dates, SSN, what have you). And, because this is totally fictional, there are people out there who are stupid enough to provide me with that information because my music is that good (okay, the story isn't 100 percent fictional). Scott comes onto my website, finds a problem with how my shopping cart is set up, and alerts me to that. He doesn't tell anyone else, doesn't tell me to pay him in order to have him reveal the problem, and in no way jeopardizes my business or my clients. He is trying to help me. I might not be happy to hear that I have a problem, but as long as he hasn't put me in jeopardy himself, I'm not going to be inclined to attack him. However, if he tells everyone else first, my perspective is that he didn't try hard enough to let me know that there was a problem, or that his intent was to hurt me, and I'll come down on him like a ton of bricks. If I don't respond to him, he has the option to tell people to not do business on my website, or at least to not provide unneeded PII on any web site. I'd be really peeved with him, but I'd have nothing that was prosecutable. Scott is entitled to free speech and his opinion. He could also tell people that my music was bad, but then he would be wrong.

To sum up, first get the contact information of the proper point of contact. Do not move forward with any revelation of a vulnerability to anyone prior to doing so. The harm done by it being there is already done. Once you finally have the proper point of contact and they say they want your information, then reveal the information in writing. They may hire you for other gigs, ask you to do a pen test, give you a reference letter you can use while seeking other clients, or they may do nothing. But, they are highly unlikely to try to prosecute you if they are so stupidly inclined, and highly unsuccessful if they are that stupid.

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

by Andy Kaiser

Chapter 0xA

The spider slashed at my face with at least half of its legs. All were tipped with gleaming black talons. I backpedaled and lifted both arms in a defensive block.

My last conversation was yet another warning from someone else who'd seen the Naked Princess file. It had not only freaked out Lynx, a young, impressionable college kid, but Minotaur, an old-school, seen-it-all hacker.

Whatever the Naked Princess was, I had to see this picture.

The spider skittered forward, and stabbed at my guts. At least one strike got through. I hit the macro for a medboost.

Unfortunately, my conversation with Minotaur had created more questions. Sure, I had a better understanding of what was in the Dante Collection, but getting more answers required talking with more of the winners of the AnonIT competition, including the missing P@nic.

What had happened to her? Was it a self-imposed disappearance, or had someone else made the decision for her? P@nic's wanna-be-boyfriend Oober had specifically requested no police. After his casual mention of P@nic's country-level botnet access, I wasn't eager to get any authorities involved. Even acting as the Information Technology Private Investigator my business cards said I was, something told me the NSA wouldn't see my side. So, my path was clear: Finding a missing girl hacker for a love-struck boy hacker took priority over reporting a world-spanning crime.

A plasma gun fired from behind me, and vomited hot death over the low-level spider. It sizzled, fried, and died. I turned around and saw the person I'd come to meet.

"You ready?" Oober said over the public channel, his voice crackling in my headphones.

"Born that way."

I wanted to talk to Oober - likely the last person I knew who'd seen P@nic. When I'd asked for the meeting, he'd agreed, but insisted on someplace safe. Secured. Private. So I went back to my office and hauled out my dusty VR headset, and went online to Oober's recommended meetup: The "Transhuman" MMORPG.

We were gaming with a group of specialized monster-hunters, prepping for a raid on a demon nest. Our raid leader was busy trying to coordinate the actions of dozens of other gamers around the world, and was paying zero attention to us individually.

Our cover established, Oober and I worked our way to a safe spot and camped while the raid leader barked out plans. We completely ignored the leader, and switched to a private channel to talk.

"Anything new?" Oober said. He'd positioned his headset mic too close to his mouth. His breathing was repeated, static bursts that kept rhythm for our conversation.

I'd originally met this kid in real life - as a young, disheveled, skinny loner. In this game, he'd designed himself the opposite.

In the dimness of our raiding party's location, Oober's avatar practically glowed. He was a tall, lean, wide-shouldered fighter, covered in armor. Metallic implants bristled from his arms and legs, many moving independently from the rest of him. A contraption of servos and electronics was in constant motion around his head, obscuring his face while at the same time angling to display a mechanical fang-baring glare.

Having just spun up my own avatar in the last few minutes, I had no idea what I looked like. I was pretty sure I'd picked a human. There was a fifty percent chance I was male.

"I've learned a few things," I said to him.

"About P@nic?" His avatar's appearance didn't match the voice I heard. Audio-compressed IP packets couldn't hide his worry.

"Yeah. I spoke with Minotar, one of the AnonIt contest winners. He spoke to her for quite a while. I've got some chat logs to go through."

"So? And? Where is she?"

"I don't know."

I'm not even sure she's still alive.

"You don't know." His breathing hissed louder over the audio channel.

"I know a lot of other things. Just not that one. Yet."

He thought for a moment, then spoke.

"She wasn't like anyone else."

His voice was quiet, almost as if he were talking to himself, just a small voice speaking personal thoughts over a secured channel inside the buzzing chaos of a MMORPG raiding party. You couldn't get much more private than that.

"I mean, yeah, she has the whole hacker thing, the botnet control, but it's more than that. When she transferred to our school, she was the only one I'd met besides me who was outside of pop-culture crap. Clothes, TV, the school cliques, none of that superficial stuff was important. She was a higher-level operator, you know? You get me?"

"Sure."

"At first, I thought it was because she was from overseas. Like it was a cultural thing, being an Aussie, or something. But it wasn't that, because she has a way of looking at -"

"Hold up. She's Australian?"

"An Aussie, yeah. She's pretty Americanized, but you can still hear it. I dig the accent."

My brain performed a sudden bit shift, and multiple clues thunked into place.

Oober's avatar flew up and away as I yanked off my VR headset. I was back in my office. I blinked quickly and shook my head, acclimating back to the real world as quickly as possible. As I did so, I pulled out my cellphone and flicked to my notes on the case.

I scanned the list of AnonIT competition winners:

*p@nic, patient zero, agent_from_harm, dragon_bawls, minotaur *and* chixor zed*

I knew about the missing P@nic. She was the reason I was working this case for Oober to begin with. I'd talked with Minotaur already, too. There were the others, and...

Chixor is slang for a female nerd.

Zed is the pronunciation of the letter "Z" for any country outside of the USA.

I slammed the VR set back on my head and Oober's avatar dropped back into my vision. I adjusted my mic and spoke fast.

"Listen," I said. "The list you gave me is a list of names, confirmed AnonIT winners. P@nic is on that list. And if she's an Aussie hacker, could it be possible that she's *also* Chixor Zed?"

Oober's stunned silence allowed me to get out my next thought.

"If Chixor Zed and P@nic are the same person, that means she's won the AnonIT competition *twice*. Why? Why would anyone want to win it again, and have to maintain two alts? That doubles the danger and the risk of exposure."

Still no response.

"This can't be about bragging rights," I said. "There has to be something more she needed, even after the first win. Maybe she had to win it twice because she'd missed getting something the first time. Or... or *maybe she wanted to put something back."*

I was so proud to have made my little breakthrough, it took me a few seconds to realize that since I'd returned to the game, I hadn't heard Oober breathing.

"Oober?"

I pinged his Avatar.

Silence oozed over the private audio channel, covered by a thick layer of Nothing Else.

I looked at Oober's avatar, with his collection of embedded biomechanical weapons and face-obscuring electronics. The constant motion seemed wrong, because the rest of the character stood frozen, rooted in place. There's nothing more creepy than an avatar waiting mindlessly for its player.

Hopefully he'd just bailed when I'd dropped away to check my cellphone. Or there'd been an emergency, something he couldn't get away from. Maybe something he *had* to get away from.

If that was the case, then when I'd spilled my new realizations about P@nic, had I still been talking to Oober? Had he left by then? If he was gone, then had I been talking to myself? Or had someone else been inside Oober's avatar, listening?

I dropped offline.

If I was lucky, Oober would contact me soon and explain his disappearance, hopefully something as simple as a bio break. But I'd worked in IT long enough to know: Hope is a terrible survival trait. My methods were data collection, comparisons of probabilities, and collections of "what if."

I'd just collected plenty of new data. The probability comparison told me something was very wrong, first with P@nic, and now with Oober.

As for "what if?" For the first time in this case, I wasn't sure I wanted to know.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally cost under $150 and are open to everyone. Higher prices may apply to the more elaborate events such as outdoor camps. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

July 9-13
ToorCamp 2014
Hobuck Beach Resort
Neah Bay, Makah Indian
Reservation, Washington
toorcamp.org

July 18-20
HOPE X
Hotel Pennsylvania
New York, New York
x.hope.net

July 26-27
Maker Faire Detroit
The Henry Ford
Dearborn, Michigan
www.makerfaire.com

August 7-10
DEF CON 22
Rio Hotel and Casino
Las Vegas, Nevada
www.defcon.org

September 20-21
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

September 24-28
DerbyCon
Hyatt Regency
Louisville, Kentucky
www.derbycon.com

October 2-5
Arse Elektronika 2014
Chez Poulet, CSC and Noisebridge
San Francisco, California
www.monochrom.at/arse-elektronika/

October 3-5
Maker Faire Rome
Palazzo Congressi
Rome, Italy
www.makerfairerome.eu

October 11-12
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

October 16-17
GrrCON
DeVos Place
Grand Rapids, Michigan
www.grrcon.org

October 31 - November 2
PhreakNIC 18
Millenium Maxwell House
Nashville, Tennessee
phreaknic.info

December 27-30
Chaos Communication Congress
Congress Center Hamburg
Hamburg, Germany
www.ccc.de

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

Marketplace

Events

HOPE X. *2600* presents the tenth Hackers On Planet Earth conference at New York City's HOtel PEnnsylvania July 18-20, 2014. Visit xxx.xxxxxxxxxxxxxxxxxxxx.xxx or x.hope.net for the latest news, travel info, special hotel rates, etc. Speakers wanted: email speakers@hope.net. Volunteers wanted: email volunteers@hope.net. Vendors wanted: email vendors@hope.net. Projects wanted: email projects@hope.net. You get the idea. You can help define what HOPE X focuses on and be a real part of hacker history, right in the middle of midtown Manhattan, across the street from the busiest train station in America. You can also join our announcement mailing list from the main page of our websites. Call (212) PEnnsylvania 6-5000 for the special conference room rate.

For Sale

HACKERSTICKERS.COM sells great hacker, programmer, and security gear such as shirts, caffeinated candy, laptop stickers, and lock pick sets. Get a free sticker with purchase, just add to cart and enter "freestick" at checkout.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite, get 20% off with coupon code 2600 at http://shop.secpoint.com/2600.

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

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Now available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Bulk discounts for hacker spaces are quite significant. Write to contact@club-mate.us or order directly from store.2600.com.

ET PHONE HOME FOB: Subminiature, tiny (7/10 ounce), programmable/reprogrammable touch-tone multi-frequency (DTMF) dialer with key ring/clip which can store up to 15 touch-tone digits and, at the push of the "HOME" button (when held next to a telephone receiver), will output the preprogrammed telephone number which can be heard at the same time from the unit's internal speaker. Ideal for E.T.'s, children, Alzheimer victims, significant others, hackers, and computer wizards. It can be given to that guy or gal you might meet at a party, supermarket, or social gathering when you want him/her to be able to call your "unlisted" local or long distance telephone number, but want to keep the actual telephone number confidential and undisclosed. Only you have the special programming tool to change the stored number. Limited quantity available. Money order only: $28.95. Order two or more, then only $24.95 each. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. This is a valuable tool for anyone developing Bluetooth software, security auditors looking for potentially vulnerable devices, or anyone who's just curious about the Bluetooth devices in their midst. Exports device data to a CSV file for use in other programs, databases, etc. If you've used tools like btscanner, SpoofTooph, Harald Scan, or Bluelog on other platforms, you need Bluetooth Search on your Android device. More info and download @ |http://tinyurl.com/btscan.

A TOOL TO TALK TO CHIPS. It's the middle of the night. You compile and program test code for what must be the 1000th time. Digging through the datasheets again, you wonder if the problem is in your code, a broken microcontroller... who knows? There are a million possibilities, and you've already tried everything twice. Imagine if you could take the frustration out of learning about a new chip. Type a few intuitive commands into the Bus Pirate's simple console interface. The Bus Pirate translates the commands into the correct signals, sends them to the chip, and the reply appears on the screen. No more worry about incorrect code and peripheral configuration, just pure development fun for only $30 including world wide shipping. Check out this open source project and more at DangerousPrototypes.com

Announcements

WHISTLEBLOWER EDWARD SNOWDEN is currently in Russia where he has been granted temporary asylum. The United States government is exerting substantial pressure on Russia and other countries in an attempt to force Mr. Snowden to the United States where he will face decades in prison or worse. Mr. Snowden's legal defense and its associated public campaign will be a long and expensive journey which will only be overcome with your financial help. Support the right to know. Support Edward Snowden. https://wikileaks.org/freesnowden Donation methods include online credit card or PayPal. Checks can be mailed to Derek Rothera & Company, Chartered Accountants, Units 15 & 16, 7 Wenlock Road, London N1 7SL, United Kingdom. Bitcoins can be sent to 1snowqQP5VmZgU47i5AWwz9fsgHQg94Fa.

Help Wanted

BE A TACTICAL TELEPHONE INSTALLER. Successful telephone service provider Shadytel is seeking applicants for the position of tactical lineman at ToorCamp 2014. Approximately four positions are available. Applicants must be able to attend Toorcamp, scheduled for 09 through 14 July 2014, at Neah Bay, Washington, USA. We will provide landline service to people in tents. You'll be responsible for helping to make that happen: taking orders, laying and terminating cable, configuring switchgear, tearing down the network afterwards, et cetera. On-site training will be provided. Qualified applicants will display a hobbyist interest in cable management, record keeping, and (optionally) customer service. Strong applicants will be able to recite the Shadytel Core Values and demonstrate familiarity with telephone industry regulations. No monetary compensation is offered. You will receive some of our schwag, possibly to include: Shadytel polo shirt, Shadytel hardhat, Shadytel branded hand tools, other Shadytel branded items. Send email to careers@shady.tel to apply. Include relevant information. Also include a phone number and preferred times to talk (Seattle time or UTC).

Wanted

WE ARE AN UNDERGROUND EXPERIMENTAL DUBSTEP RAP BAND along the lines of the Beastie Boys and Mindless Self Indulgence, creating music outside the system exclusively for the Internet. We are in need of an awesome web designer to redesign our outdated wordpress website: www.tvmessiah.com. Check out our latest tracks on youtube (http://www.youtube.com/user/tvmessiah/videos) and, if you dig us and believe we are worthy, please reach out to us: number7@tvmessiah.com.

Services

DIGITAL FORENSICS FOR THE DEFENSE! Sensei Enterprises believes in the Constitutional right to a zealous defense, and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We recover data from many sources, including computers, external media, and smartphones. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. Sensei's digital forensic examiners all hold prestigious forensic certifications. Our principals are co-authors of *The Electronic Evidence Handbook* (American Bar Association 2006) and of hundreds of articles on digital forensics and electronic evidence. They lecture throughout North America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703-359-0700 or email us at sensei@senseient.com.

WANT SOMEONE'S FBI FILE? Check out GetGrandpasFBIfile.com, a site that shows you how to get the FBI files for any dead person. Or use GetMyFBIfile.com, the site that shows you how to get your own FBI file.

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

GET YOUR HAM RADIO LICENSE! KB6NU's "No-Nonsense" Study Guides make it easy to get your Technician Class or General Class amateur radio license. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. And the best part is that they are free from www.kb6nu.com/tech-manual. E-mail cwgeek@kb6nu.com for more information.

THOUSANDS OF GOVERNMENT DOCUMENTS are published at GovernmentAttic.org. New material available each week. Click on the Documents homepage link to start.

NOPAYCLASSIFIEDS.COM - Free advertising - 50 countries! Free business directory, classified ads (6 free photos) with link to your website to help you expand your business and improve search engine placement. Search over 35 million classified ads (mostly USA) to help you find what you want. Thank you for being part of our online audience!

SECURE UNIX SHELLS & HOSTING SINCE 1999. JEAH.NET is one of the oldest and most trusted for fast, stable shell accounts. We provide hundreds of vhost domains for IRC and email, the latest popular *nix programs, access to classic shell programs and compilers. JEAH.NET proudly hosts eggdrop, BNC, IRCD, and web sites w/SQL. *2600* readers' setup fees are always waived. BTW: FYNE.COM (our sister co.) offers free DNS hosting and WHOIS privacy for $3.50 with all domains registered or transferred in!

BASEMENT TECHIE* AND *THE DYSTONAUT: Two great tastes that taste great together! Better than a kick in the ass with a steel toe boot! DIY - Dystopias - Poor Hackers playing with Electronics and RF - Living Outside The System - by Ticom - http://www.oberonsrest.net/

Personal

USED PROGRAMMING BOOKS WANTED! I'm stuck in federal prison and I'd like to learn some new stuff, especially programming languages. I was always able to take existing code and extensively modify it (trial and error) to do what I wanted, but I'm tired of doing that. I've got all of this time to try to wrap my head around different languages, so that's my goal. I'm decent with PHP and Perl, but I'd really like to strengthen those as well as learn some new ones. I can receive paperbacks as well as magazines from any source, as long as they're not in a bubble envelope and are marked "Authorized by BOP Policy" on the box/envelope they come in. Media mail or flat rate envelopes are two good options. I can receive up to 5 books in each envelope/box. Please send to Rob Santon 32574-160, FCI Elkton, PO Box 10, Lisbon, OH 44432. Thank you!

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 subs@2600.com.

Deadline for Autumn issue: 8/21/14.

"If you don't want to be replaced by a computer, don't act like one."
- Physicist Arno Penzias, 1978

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Bob Hardy

Layout and Design
Skram

Cover
Dabu Ch'wald

Office Manager
Tampruf

Infrastructure
flyko

Network Operations
phiber

Broadcast Coordinator
Juintz

IRC Admins
beave, koz, r0d3nt

Inspirational Music: Braindrops, Lion Rock, Finn and the Rustkickers, Mykal Rose, Beardyman, Skinny Puppy, Madame Chaos, A$AP

Shout Outs: Yes Lab, MARCH, Big Head, Gilfoyle, Dinesh, joelfreak, Dr. Rip, Pearson Ropebeltz, NYCCampDrupal

Welcome: Lily Morticia

RIP: Robert Knight, Howard Smith

***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);
Summer 2014, Volume 31 Issue 2, 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 - $27 individual,
$50 corporate (U.S. Funds)
Overseas - $38 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2013 are $27 per year or $6.95 each.
Shipping added to overseas orders.

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

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

MEETINGS

ARGENTINA

Buenos Aires: Bar El Sitio, Av de Mayo 1354.

AUSTRALIA

Melbourne: Southgate Shopping Complex, outside food courts.

Sydney: The Crystal Palace Hotel, 789 George St. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

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

BRAZIL

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

CANADA

Alberta

Calgary: Food court of Eau Claire Market. 6 pm

Edmonton: Elephant & Castle Pub, 10314 Whyte Ave, near big red telephone box. 6 pm

British Columbia

Kamloops: Student St in Old Main in front of Tim Horton's, TRU campus.

Vancouver (Surrey): Central City Shopping Centre food court by Orange Julius.

Manitoba

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

New Brunswick

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

Newfoundland

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

Ontario

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: Free Times Cafe, College and Spadina.

Windsor: Sandy's, 7120 Wyandotte St E. 6 pm

CHINA

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

COSTA RICA

Heredia: Food court, Paseo de las Flores Mall.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Leeds: The Brewery Tap Leeds. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Entrance to Chapelfield Mall, under the big screen TV. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Cannes: Palais des Festivals & des Congres la Croisette on the left side.

Grenoble: EVE performance hall on the campus of Saint Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 7:30 pm

Paris: Quick Restaurant, Place de la Republique. 6 pm

Rennes: Bar le Golden Gate, Rue St Georges a Rennes. 8 pm

Rouen: Place de la Cathedrale, benches to the right. 8 pm

Toulouse: Place du Capitole by the benches near the fast food and the Capitole wall. 7:30 pm

GREECE

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

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court.

***Safed:** Courtyard of Ashkenazi Ari.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Kagoshima: Amu Plaza next to the central railway station in the basement food court (Food Cube) near Doutor Coffee.

Tokyo: Mixing Bar near Shinjuku Station, 2 blocks east of east exit. 6:30 pm

MEXICO

Chetumal: Food court at La Plaza de Americas, right front near Italian food.

Mexico City: "Zocalo" Subway Station (Line 2 of the "METRO" subway, the blue one). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

NETHERLANDS

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

NORWAY

Oslo: Sentral Train Station at the "meeting point" area in the main hall. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

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

SWEDEN

Stockholm: Starbucks at Stockholm Central Station.

SWITZERLAND

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

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

Huntsville: Newk's, 4925 University Dr. 6 pm

Arizona

Phoenix: Cartel Coffee Lab. 6 pm

Prescott: Method Coffee, 3180 Willow Creek Rd. 6 pm

Arkansas

Ft. Smith: River City Deli at 7320 Rogers Ave. 6 pm

California

Los Angeles: Union Station, inside main entrance (Alameda St side) between Union Bagel and the Traxx Bar.

Monterey: East Village Coffee Lounge. 5:30 pm

Sacramento: Hacker Lab, 1715 I St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Center near street level fountains. 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Tustin: Panera Bread, inside The District shopping center (corner of Jamboree and Barranca). 7 pm

Colorado

Loveland: Starbucks at Centerra (next to Bonefish Grill). 7 pm

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

Arlington: Champps Pentagon, 1201 S Joyce St (in Pentagon Row on the courtyard). 7 pm

Florida

Fort Lauderdale: Undergrounds Coffeehaus, 3020 N Federal Hwy. 7 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Jacksonville: O'Brothers Irish Pub, 1521 Margaret St. 6:30 pm

Melbourne: Sun Shoppe Cafe, 540 E New Haven Ave. 5:30 pm

Sebring: Lakeshore Mall food court, next to payphones. 6 pm

Titusville: Krystal Hamburgers, 2914 S Washington Ave (US-1).

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700.

Pocatello: Flipside Lounge, 117 S Main St. 6 pm

Illinois

Chicago: Golden Apple, 2971 N. Lincoln Ave. 6 pm

Peoria: Starbucks, 1200 West Main St.

Indiana

Evansville: Barnes & Noble cafe at 624 S Green River Rd.

Indianapolis: Tomlinson Tap Room in City Market, 222 E Market St. 6 pm

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Davenport: Co-Lab, 1033 E 53rd St.

Kansas

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

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Stratton Student Center (Building W20) at MIT in the 2nd floor lounge area. 7 pm

Worcester: TESLA space - 97D Webster St.

Michigan

Ann Arbor: Starbucks in The Galleria on S University. 7 pm

Minnesota

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

Missouri

St. Louis: Arch Reactor Hacker Space, 2400 S Jefferson Ave.

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

Elko: Uber Games and Technology, 1071 Idaho St. 6 pm

Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Somerville: Dragonfly Cafe, 14 E Main St.

New Mexico

Albuquerque: Quelab Hacker/ MakerSpace, 1112 2nd St NW. 6 pm

New York

Albany: SUNY Albany Transfer & Commuter Lounge, first floor, Campus Center. 6 pm

New York: Citigroup Center, in the lobby, 153 E 53rd St, between Lexington & 3rd.

Rochester: Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Charlotte: Panera Bread, 9321 JW Clay Blvd (near UNC Charlotte). 6:30 pm

Greensboro: Caribou Coffee, 3109 Northline Ave (Friendly Center).

Raleigh: Royal Bean Coffee Shop, 3801 Hillsborough St (next to the Playmakers Sports Bar and across from Meredith College). 7 pm

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

Cleveland (Warrensville Heights): Panera Bread, 4103 Richmond Rd. 7 pm

Columbus: Easton Town Center at the food court across from the indoor fountain. 7 pm

Dayton: Marions Piazza ver. 2.0, 8991 Kingsridge Dr., behind the Dayton Mall off SR-741.

Youngstown (Niles): Panara Bread, 5675 Youngstown Warren Rd.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Oregon

Portland: Theo's, 121 NW 5th Ave. 7 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, food court outside Taco Bell.

Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window.

State College: in the HUB above the Sushi place on the Penn State campus.

Puerto Rico

San Juan: Plaza Las Americas on first floor.

Trujillo Alto: The Office Irish Pub. 7:30 pm

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: West Town Mall food court. 6 pm

Memphis: Republic Coffee, 2924 Walnut Grove Rd. 6 pm

Nashville: J&J's Market & Cafe, 1912 Broadway. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Dallas: Wild Turkey, 2470 Walnut Hill Ln. 7 pm

Houston: Ninfa's Express seating area, Galleria IV. 6 pm

Plano: Fourteen Eighteen Coffeehouse, 1418 Ave K. 6 pm

Vermont

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

Virginia

Arlington: (see District of Columbia)

Blacksburg: Squires Student Center at Virginia Tech, 118 N. Main St. 7 pm

Charlottesville: Panera Bread at the Barracks Road Shopping Center. 6:30 pm

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

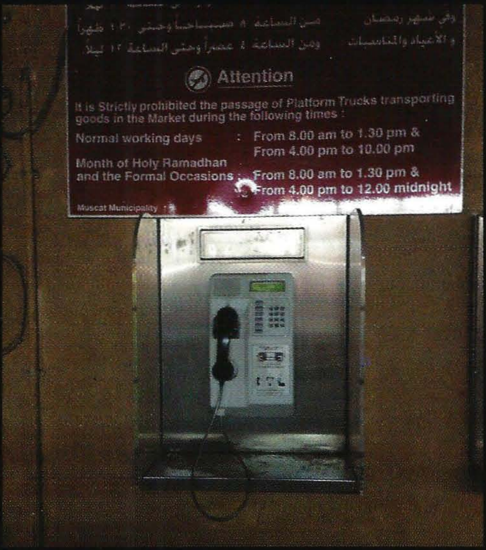
Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

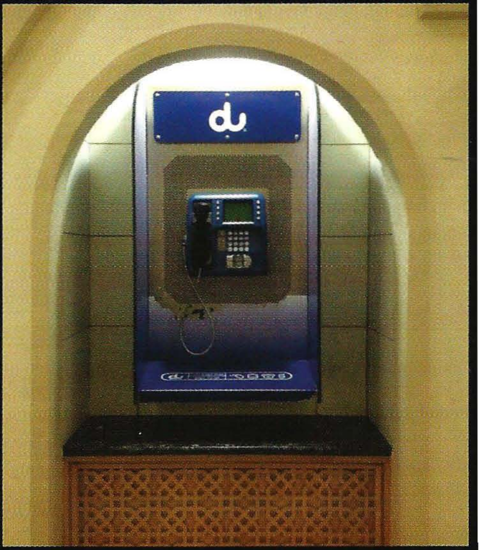
All meetings take place on the first Friday of the month (a * indicates a meeting that's held on the first Thursday of the month). Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Middle Eastern Payphones


Attention
It is Strictly prohibited the passage of Platform Trucks transporting goods in the Market during the following times :
Normal working days : From 8.00 am to 1.30 pm &
From 4.00 pm to 10.00 pm
Month of Holy Ramadhan and the Formal Occasions : From 8.00 am to 1.30 pm &
From 4.00 pm to 12.00 midnight
Muscat Municipality

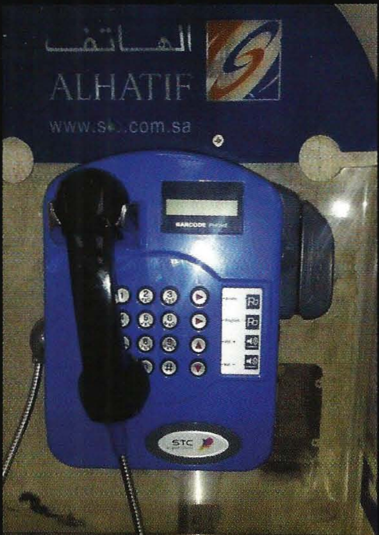
Oman. Seen in Muscat along with a thorough list of times where your phone conversation won't be disturbed by the sound of platform trucks.

Photo by secuid0



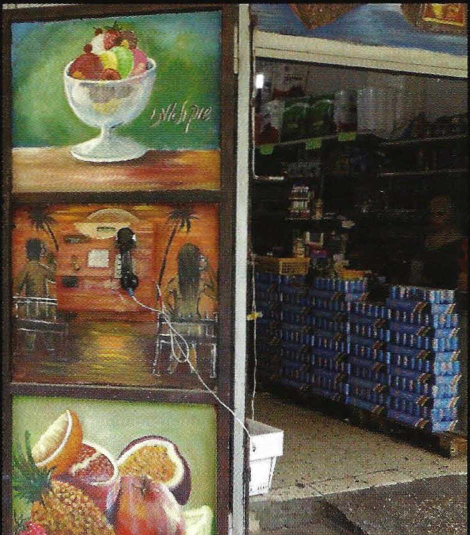
United Arab Emirates. This model was seen in Dubai and is operated by Emirates Integrated Telecommunications Company, commonly known as "du."

Photo by secuid0



Saudia Arabia. This was spotted at the airport in Jeddah. Despite its pristine condition, no sequence of button presses or twiddling on/off-hook yielded a display or dial tone.

Photo by Estragon

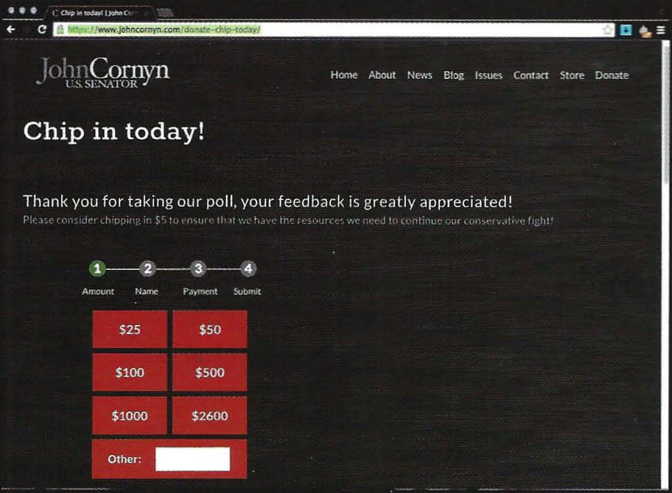


Israel. We've never seen such a well camouflaged phone. There may not be much practical purpose in hiding a payphone, but it sure does look nice. Found in Jaffa.

Photo by David Mizrahi

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

The Back Cover Photos



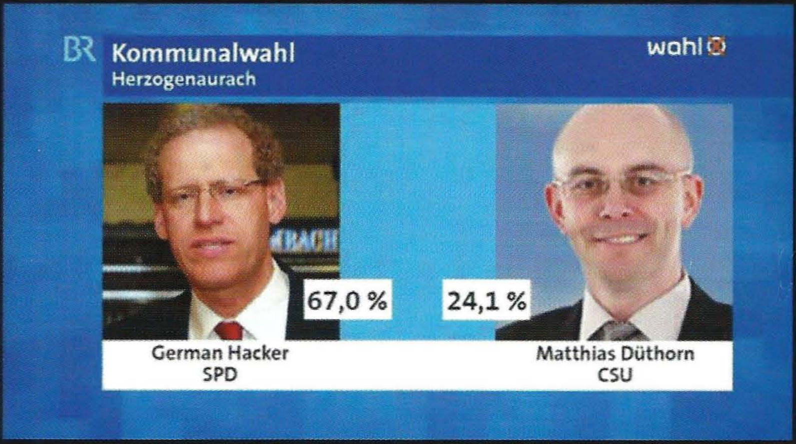
https://www.johncornyn.com/donate-chip-today/

Chip in today!

Thank you for taking our poll, your feedback is greatly appreciated!

Please consider chipping in $5 to ensure that we have the resources we need to continue our conservative fight!

Well, isn't this a surprise! Here's an image from the donation section of Senator John Cornyn's website, as found by **RykVR**. In addition to proudly proclaiming himself the second most conservative senator in the country, he apparently has fond eyes for hackers. Why else would he use that number instead of something more standard, like $2500?



Continuing with our political theme, did you know that there's a politician in Germany with the actual name of German Hacker? Turns out he's the mayor of Herzogenaurach (and popular, too)! We know many German hackers, but this is a first. Thanks to **Casandro** for this one.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

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) or a *2600* t-shirt of your choice.