Volume Thirty-One, Number Four
Winter 2014-2015, $6.95 US, $7.50 CAN

2600

The Hacker Quarterly

4 4>
0 74470 83158 7

Classy Payphone Booths

Austria. Seen on Danube Island in Vienna, this classic booth is as sturdy as you could hope for but rarely used, judging from the spider webs found inside. (But the phone works!)

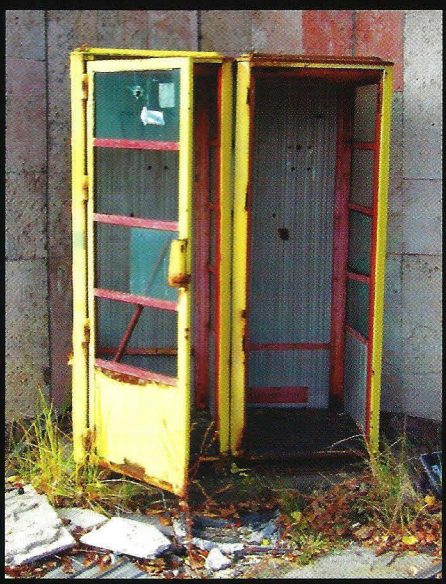
Photo by Richard Hanisch

Greece. While showing obvious signs of wear, this booth seems to be in it for the long haul. Found in Corfu near the old town square. The phone itself was in pretty good shape.

Photo by Brother Franklin

Peru. There's something really classy about this fixture bolted into the stone on what looks like a really old street in Cusco. Not much of a booth, but the protection is implied.

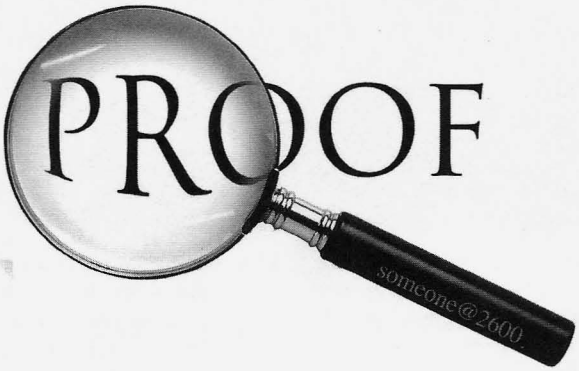
Photo by Mark

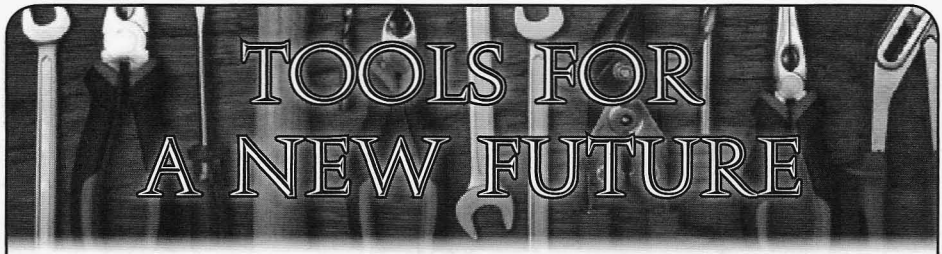


Ukraine. A quaint scene from Pripyat, where you'll soon discover it's rather difficult to find a phone or even a person due to the aftereffects of Chernobyl. The city was only 16 years old when it was abandoned.

Photo by Ashes

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 (Do not send us links as photos must be previously unpublished.)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





To say we live in interesting times would be a vast understatement. To try and keep up with the technological advancements that are made year after year is a job in itself. But to also try and keep up with the multitude of developments involving hackers, freedom of speech, spying, leaking, hacktivism, legislation, legal battles... it all can get lost in the sheer amount of content we're being exposed to. So while the times are indeed interesting, they are also overwhelming, and the frustration caused by too much data can pull us into the very same inertia we would be experiencing if there was absolutely nothing of interest going on.

Fortunately, there are options and ways that we can use all of this to our advantage. In order to do that, we have to remember a few things. First, we can't possibly take it all on or understand every conceivable nuance. For instance, you may choose to focus on the net neutrality issue and not devote as much time to the topic of NSA spying. Second, it's important for us to work together as much as possible so that we can benefit from the subject matter that others focus upon as well as flesh out those findings we're developing ourselves. Writing or speaking from one's own perspective is essential, but there is also strength in numbers. In groups, there are varieties of opinions and even disagreements, which, contrary to the belief of many, only serve to strengthen and help define the basic premise of the cause we are united on. Finally, as easy and accessible as technology has made things, actual skill remains an achievement that can't be bought or even given away. We have more of an opportunity to develop these skills, but that step cannot be skipped. Understand this and you have a much better chance of standing out against all of the noise.

Let's take a quick look at some of what has come out of this already.

Social media has been known to drag people down into pits of trivia and irrelevance, wasting vast amounts of valuable time. Worse, it can serve as a tool that can be used against us, insofar as the loss of privacy when too much of our personal information is exposed and the loss of basic social skills when we devote an inordinate amount of time and attention to what's on our phones and tablets at the expense of what's right in front of us.

But social media can also be an invaluable resource if we *choose* to use it in that way. This is a tool that can only hurt us if we let it and which can help us greatly if we recognize the potential of effective and relevant mass communication. One way or another, the power is in our hands.

By learning how to effectively use this tool to quickly reach a great number of people, we have the kind of power that would have been unimaginable only a decade ago. Of course, this is far from a revelation - we've seen social media used successfully in everything from the Arab Spring to all kinds of lobbying efforts. But all too often, the connections we make are short-lived and disappear after whatever crisis that united us is resolved. This is all very useful to those in charge who don't want the basic structure of society to change and who live in fear of people realizing the power that they could have with this technology.

Think of the mindless appeal of something like television, the true opiate of the masses. We are deluged with banality because it's safe and it quells dangerous thoughts of change. We remain firmly mired in our place where we pose no threat. But think about what such a tool *could* be if it got people to think and to see results. This is precisely why governments in every country keep tight control over such outlets. They have tremendous potential power and most people don't even realize it. Of course, that power can also be used in a negative way as well, just as tightly controlled social media could be very dangerous to individuals.

It's all about who's in control and what they do with that control while they have it. In the case of social media, tech-savvy people like hackers are clearly running the show for now, but that could easily change if we stop paying attention. Despite the negative attributes, the positive potential is simply too great to dismiss this unprecedented means of communication.

We've all seen what has happened in general with technology in recent years and decades. Faster, smaller, and cheaper. The access we have now is beyond anything we could have ever dreamed about not too long ago. But what do we do with all of the speed and storage and capability that surrounds us? Do we just do our jobs more efficiently, pile on even more work, and stay inside the box that's defined for us? Or do we dream?

As an example, let's look at how the dramatic changes in technology have affected just one part of our culture: visual storytelling.

The hacker world is filled with stories. It always has been. But we've traditionally had to wait for someone with the experience, skills, and access to the necessary tools to tell these stories for us - and to hope they didn't screw it up too badly since they were invariably outsiders. We could fill these pages with lists of all of the times this didn't go well.

What we are seeing today is a veritable explosion of documentaries from within the community. In 2014 alone, we saw theatrical releases of a revealing documentary on hacktivism (*The Hacker Wars*), the compelling story of the late Aaron Swartz (*The Internet's Own Boy*), and a firsthand and highly relevant account of the Edward Snowden tale (*Citizenfour*). These are just three of the more prominent films that came out in a single year; there are more from within and outside the States. We anticipate an even greater increase in the months and years ahead.

For a tiny fraction of what it used to cost (without even taking inflation into account), it's now possible to get video technology that looks and sounds as good or better than what only major production houses could afford in the recent past. It would have been phenomenally more difficult to produce such high quality works a few years ago, utterly impossible before then. The faster, smaller, and cheaper world has opened some incredibly important doors.

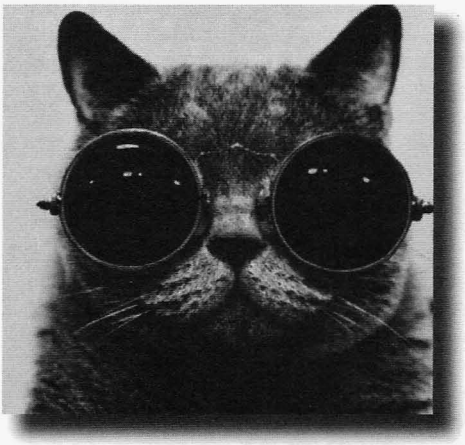
A few decades ago, hackers learned how computers worked by breaking into ones that didn't belong to them via dialups and packet switched networks. There was no other way, as the access simply didn't exist. Today, access to computers is no longer the issue it once was and the landscape has changed completely as a result. And there are no landscapes that can't be as dramatically altered due to these advancements. The plethora of new documentaries is but one example of this. Publishing, photography, music, art of all sorts all can benefit and become far more accessible. But, as with social media, this is only significant if we choose to use it to its full potential.

We know what the YouTube environment has done to the world of video. It seems as if anyone believes they can now be a filmmaker. But, of course, not everyone *is* a filmmaker. Just as not everyone on Flickr is a photographer, not everyone who has a blog is a writer, etc. The list goes on and on. The ease of access to all of these tools is huge, but the issues of skill and experience are just as relevant and vital as they've ever been. With all of the noise that's now out there, it's a daunting and frustrating task to even be heard. But at least those who have the skill and passion have a *chance* to get their perspective out there. We can think of no reason why these opportunities shouldn't be pursued whenever possible. The stories and outlooks unique to the hacking community are too priceless to be trusted to anyone who doesn't truly appreciate them. We have the means to be doing so much more as a community; we have but merely to prioritize.

We are at a pivotal point in history where we have an abundance of access to technology. Many of us are having trouble coming to terms with that. There is simply so much to do, an unlimited amount of potential, so many choices. In a way, it can be easier to be forced down a narrow path than to figure out how to traverse a huge boulevard. That is why we cannot be afraid to make mistakes and false starts as we refine our talents. The learning process has changed on virtually every level and the old rules just don't apply anymore. Rather than wait for someone to issue new rules, we need to plunge into our own era of experimentation and innovation and shape it for our own purposes of expression.

We look forward to the explosion of creativity ahead.

Password Cracking in the Modern Age



by Yuval tisf Nativ and Tom Zahov

A long time ago we understood that storing passwords leads to many issues with security. The idea behind the password or passphrase is to provide a layer of security for the user. Basically, the computer or system can work perfectly without needing a password. You can get to the login screen, see a list of available users, and just click on one of them and the machine will load the settings required for the specific user.

The issue is that sometimes, part of those settings are a bit more sensitive to the user. Or maybe you, as an admin, want to know which user is which and not have them logging on as another user. We can say today that most systems are interested in the segregation between users - sometimes due to sensitive content, sometime due to different privileges and features on the system and sometime it's just to load the content for that user. For example, you can probably post your SoundCloud credentials online. Most SoundCloud users are not content creators, but rather consumers and your playlist is most likely available to the public and you don't care about it. The only reason you had those credentials in the first place was to get your playlists when you load the application.

Password Protection on Different Systems

As always in the real world, the solution is not a single solution for everyone and everything. Take, for example, two systems which are completely different by nature. The first will be your home desktop/laptop (we'll call it your PC) and a shopping site like eBay. In your home PC, you will store a few user credentials, most likely no more than ten users. The protection you expect your system to provide is to make it difficult on a user to perform actions or access data from another account. eBay, however, is different by nature. Let's first make something clear: eBay is not a shopping site. eBay is a security company. eBay is a system whose sole purpose is to allow sellers and customers to exchange goods with security - commercial security and information security.

On eBay, your needs concerning passwords are completely different than what you would expect on your home system. You expect the system to use your credentials to identify you, keep others out of your account, and never to disclose your password. They seem like the same thing at first, but your home laptop is something which offers services only to you and maybe a few other members of your family. eBay, however, is offering services to millions of users.

In the Beginning

Let's take your home computer as an example to start understanding issues and how we commonly practice password storing today. Let's imagine you are the administrator on your own network at work. You have John, who you have just appointed as the new helpdesk manager. John is a great guy and, in order to help him do his job, you give him administrative access to your main domain controller. Remember, John needs those privileges not because he's a great guy, but because his job will require having significant changes to your network as part of his daily routine. If John has such a high access, what keeps John from

reading the file containing all of the users' passwords and logging in as one of them? One of the main problems is that in almost every system you want a principal called non-repudiation. Non-repudiation is a state where if you, the administrator, can see an action in the log of the system made by User A, User A cannot deny having taken that action.

One of the technologies used to solve this problem is hashing. A hash is a mathematical function which takes a random length of bits and maps them out into a constant length of bits. To better understand this, let's quickly go over the XOR function and a bit of your high school math classes. The XOR function is a logical operand which takes two bits and outputs the difference. For example: 1 and 0 going into XOR will give 1 since there is a difference. 0 and 0 going into XOR will output 0 since there is no difference. The important thing to notice about XOR is that if you have two parts of the equation, you are able to easily map the missing part. If, however, you only have the output, it is mathematically impossible to know the inputs. If I say that the output of XOR is 0, the inputs could have been 0 and 0 or 1 and 1 and you have no way of knowing which, unless you have more information (statistical sample or other types of data).

Now your high school math classes will be handy since they will help you theoretically grasp the way hash functions work and therefore understand the features later on. Remember that test you had and there was this question where you got that weird outcome of "-3.452x" and you knew it was wrong but you had no idea why? Later on, when the teacher returned your exam, you noticed that you flipped a "-" or just mixed up in copying a number and instead of 2 you wrote 7? That's another feature of hash functions. They work in a mode we call block ciphers. When you give the hash function an input to compute, it has a routine it has to follow, but this routine is not one. It's comprised of blocks where the output from the previous block is then fed into the next block as input. This will cause any minute change to the input to "drag" the "error" (more correctly - change) all across the computation progress and provide a significantly changed output.

So these are the features of hash functions we spoke of up until now:

- They take *any* size of input and output a known (constant) size output.
- Each change to the original input will result in a significant change to the output.
- They are one way functions. You can easily compute a nonce to the hash sum of it, but it is infeasible to compute a nonce given the sum.

How Does This Work Then?!

Well, fine you should ask. When you first enter your password for your user account, the operating system takes your password and hashes it. Depending on your OS, it can be with LM, NTLMv1, NTLMv2, MD5, or other types. After the password is hashed, the sum of it (e.g. the output of the hash function) is then stored into a file. Next time you want to login, the machine gets your password, but it does not know the previous password (it knows the sum). The machine uses your input as the nonce for the same hash function and then checks if the sum is identical to the hash stored in the file.

This allows the machine to store the passwords in a file on disk and, if an attacker gets a hold of these sums, the attacker cannot use them to know the original password for those users. There are a few cryptographic attacks which can allow an attacker to leverage those sums and be able to then login to that system. The first is if a weak hashing algorithm was used and is susceptible to collision attacks. A collision attack is when given a sum of a hashing algorithm, you can compute a nonce that will result in the same sum. Let's go over this again: we said that a hashing algorithm will compute a fixed-length sum for any given input. That was not accurate. Each hashing algorithm hashes its own nonce size limitations. Let's take MD5 for example. MD5 will give us a 128 bit sum every time, typically represented as a sequence of 32 hexadecimal digits. Now the input is practically limited to the amount of computer memory you have while mathematically being infinite; therefore we have infinite set of inputs which will result in the same output. There are two questions left: a) how common are these collisions? b) is there a way to compute them or is there just random guessing?

For this example, we'll use the work of Peter Selinger of the Department of Mathematics and Statistics from Dalhousie University. We'll add a story behind the data:

John has a remote connection to his security camera at home. The security camera stores the password as an MD5 hash. John is using a secure connection so that a man in the middle will not be able to understand the data. John

chose an extremely long password:

```
d131dd02c5e6eec4693d9a0698aff95
➥c2fcab58712467eab4004583eb8fb7
➥f8955ad340609f4b30283e4888325
➥71415a085125e8f7cdc99fd91dbdf2
➥80373c5bd8823e3156348f5bae6da
➥cd436c919c6dd53e2b487da03fd
➥02396306d248cda0e99f33420f5
➥77ee8ce54b67080a80d1ec69821bcb
➥6a8839396f9652b6ff72a70
```

Darth is a hacker who was able to clone the hard drive of the camera while visiting John. Now Darth tries to read the image of the drive and finds that the password is hashed. Darth finds the following hash:

```
79054025255fb1a26e4bc422aef54eb4
```

Now Darth wants to find the password. He knows that John used a very long password and now turns to a collision attack. During this, Darth find this value:

```
d131dd02c5e6eec4693d9a0698aff95
➥c2fcab50712467eab4004583eb8fb
➥7f8955ad340609f4b30283e4888
➥325f1415a085125e8f7cdc99fd91db
➥d7280373c5bd8823e3156348f5bae6
➥dacd436c919c6dd53e23487da03fd0
➥2396306d248cda0e99f33420f577e
➥e8ce54b67080280d1ec69821bcb6a8
➥839396f965ab6ff72a70
```

which is different than the original but has the same sum under MD5. Darth can now login to John's camera, since the camera does not know the original password, but only the MD5 sum of the password and in this case:

```
MD5(john's_password)
➥  == MD5(darth_collision)
```

Practices

Hashes today are used in many places in many forms; they are used in local machines to store passwords, they are used in websites to protect sensitive information in case an attacker can ex-filtrate the data from the database, they are used in verification of certificates and in file integrity checks. Now let's look at a more practical view of hash cracking.

There are several attitudes towards cracking hashes:

Open source cracking
Mathematical attacks
Brute forcing

We won't go over each of them in great detail. The first is quite simple: many sites today offer the service of cracking hashes (we won't go into how they work) and you can just Google a sum. For example; you can Google this hash and see what the plain text of it is yourself:

```
e10adc3949ba59abbe56e057f20f883e
```

Mathematical attacks depend on the hashing cipher used and, in any case, they are usually not valid when talking about modern ciphers. Sure, MD5 has a known collision generation algorithm (referred to above), but they will not lead us to a plain text from the hash and there are no known attacks for SHA256 or SHA512 for now, so we'll just skip them.

Brute Forcing

Assuming the hashing algorithm is a strong hashing algorithm, we cannot reverse it nor can we find a collision easily. We would prefer getting the plain text anyway. Our way of doing that would be by taking plain text values, computing the hash sum for them, and then comparing it with the original sum. It might sound like hunting with a club, but only because it is. There are ways to make this search smarter and smarter since computing hash sums consumes a lot of resources from most processors.

A word list is just an ASCII file containing words that we think might be used as the password. Sometimes we can even "improve" the file by pre-computing the sum and saving it right next to the word so we can just search the file for a given hash. This file will be called a rainbow table. They are very big files and searching through them is not easy, but most of the time it's easier than computing the hash all over again and it's more cost-effective when testing several hashes and not just one.

This might not sound like a big improvement, but imagine you just hacked a database and stole 20,000 credentials which are MD5 hashed. Most of the time, you are not interested in just one password but rather as many as possible. Instead of trying to crack each and every one of the hashes in this list, you can use the list of 10,000 most used passwords to try and crack them. A lot of them will probably fit and, again, you are rarely interested in recovering all of the hashes. You can get the top 10,000 most commonly used passwords and even the statistics.

On Kali, type these commands:

```
wget -O crypted-storage.lst
➥ http://pastebin.com/download.
➥php?i=YULUgrnd
wget -O 10k.zip http://xato.net
➥/files/10k%20most%20common.zip
unzip 10k.zip
```

Now we'll use John the Ripper to crack those hashes:

```
john --wordlist="10k most common
➥.txt" crypted-storage.lst
```

You might say, "What are the probabilities that so many people will have the same password if it's not on the top 10k list?" Well, this attack is based on the birthday problem in probability theory. This theory tests the chances for a set of randomly chosen people of a pair of them having the same birthday. Unlike common belief, the probability that two people out of a set of 23 having their birthday on the same day is close to 50 percent. With a birthday attack, a hacker randomly generates output of a given cryptographic function until two inputs map to the same password.

HashCat

Those of you who are familiar with this topic are probably a bit mad right now since I have titled this section after the name of a tool for cracking hashes. I would like to say that by my standard, HashCat is not just a tool but it is *the* tool for hash cracking. The main reason this tool is unique for me is the way this tool is configured and works for GPUs (yes, there are other tools working with GPUs and I'm going to talk about HashCat only).

I would like to refer back to an algorithm called LM. LM was an algorithm used to store passwords on the older versions of Microsoft's Windows. In the newer products by Microsoft, we generally do not see LM used anymore. The reason is because this algorithm was fine at the time that it was designed, but these days with our i5 and i7 processors, this algorithm is prone to attack and a 64 bit output is suddenly a very small range and we can easily find values.

The biggest limitation we have on hash cracking is our processors. Storing and sorting through large rainbow tables is possible, but requires very large disks and very fast and large memory, so we mostly compute the hashes on the fly. Though our i7s are strong, they are still not fast enough to allow us feasible cracking of strong passwords on MD5 or SHA256. Today, when we're talking about hash cracking, most of us are talking about hash cracking using graphical processing units rather than central processing units. There are many differences between the two to make a GPU more suitable for hash cracking, but the main reason is the amount of cores. Let's take the brand new Intel i7 fourth generation 4550U processor and the AMD Radeon HD 7950 GPU. The i7 has two cores with four threads at a speed of 3.00 GHz. The Radeon 7950 has an engine clock of 875 MHz but 1792 stream processors!

GPUs are particularly good for hash cracking since they are really good in parallelism, especially if you are referring to identical operations, which is what hashing is. Remember that block feature we talked about in the beginning? Here you see it coming to life.

A Comparison Between GPU and CPU

Let's take a simple graphics card. For this example, again, we'll use the AMD Radeon 7950. There are a total of 1792 stream processors on the 7950. Without optimizing the computation to the GPU architecture, you can still get a reasonable 160 x 10^6 SHA1 computations per second on this GPU. Now let's compare this to a CPU:

We'll assume the new Intel i7 fourth generation is here to make things easier. So when referring to the technical spreadsheet, we notice the two cores and four threads. To simplify things, we'll take it as a real eight core processor. A single SHA1 computation will consume about 500 clock cycles. If we are to create an optimized hashing function to use the 128 bit registers to try and require less and less computation, we might reach even a point where we can use 300 clock cycles to compute a single SHA1. Assuming we can run in parallel (this is not such a reasonable assumption since there is a limited number of registers we can use and we assume no other application will require any CPU time), we can get to eight computations with each using 300 clock cycles, which will leave us with 2,400 clock cycles resulting in 2,450 SHA1 hashes per second.

Using HashCat for Your Hash Cracking

Let's start with downloading and compiling HashCat. Yes, there is a version on Kali, but HashCat is frequently updated and improved and you want the newest version of it.

```
# AMD Cards:
wget http://hashcat.net/files/ocl
➥Hashcat-1.21.7z
# NVidia Cards:
wget http://hashcat.net/files/
➥cudaHashcat-1.21.7z
7z e *Hashcat-1.21.7z
cd *Hashcat-1.21
```

And now you're ready to start cracking hashes. Try, for example, the following hashes:

```
5dd48674f791a9c589c4b63ac249dc4b
1781858ef825ac2074b3544453ffb49a
043763020c15dd4f34987016b6178195
3e2346e38a27ac33cca4d906880b7f80
dc77614b7737874aa1bdd2a384dc7a34
78342384e152971055d3987ad7aa64db
69f56f8117ae196ca69eead336535257
c01aec2cc879706d0a11a29ab8833657
d22a8263372bd6c79d6e2f93f0069605
5c171ed62a2a631c6162fa51a19cd41f
```

Use HashCat's default dictionaries.

Static Salting

Another solution we have created to handle these hashes is called salting. In the process, a system concatenates the original value before passing it to the hash function. For this example, if we have a database of hashed credentials with MD5, we can find many rainbow tables and easily compute many of the passwords relatively easily. A system can protect the users further on by salting the values of the passwords. In this example, John entered the password "123456" which will be found easily by any rainbow table. Our system will concatenate each password with the following format:

```
MD5( '123' && user.password &&
➥ 'abc4rfdgf4')
```

This will result in each password being harder to crack. The attacker needs to get a hold of the salting format before cracking the passwords and, even then, any existing rainbow tables will probably not fit the salting format and an attacker will have to calculate the hash sums again.

Dynamic Salting

Dynamic salting is the more recent evolution. While computing power improved, we started seeing programs like Combina (`https://github.com/ytisf/combina-0.4.2`), which are very efficient and allow users to easily create rainbow tables whenever the need to arises. The next evolution in the field is dynamic salting, which means that each value is salted with its own unique string. When you salt each value with its own data, it means that a computed hash by the attacker cannot be used twice since the salting data for the others have changed and he needs to compute his wordlist for each and every value. This is powerful, especially if you keep the salting information separate from where the passwords are stored, meaning that an attacker will have to gain access to both of the sections prior to being able to attack them.

Summary

Remember that the world changes. Hash functions decay over time, not because they were designed wrong, but rather because the world changes and people have more computing power at home, plus new devices are invented for the sole purpose of cracking hashes (e.g. Bitcoin and Butterfly Labs).

What Do Ordinary People Think a Hacker Is?

by Kim Crawley

Once a few years ago, I purchased an issue of *2600* at my local Chapters bookstore. Later that day, I was in a car with my friend and his boss, both of whom work in the financial services industry. Neither my friend nor his boss had much knowledge of computing culture.

"I really like this new issue of *2600* I just bought," I said. My friend's boss was curious.

"Let me see that," she said. I handed it to

her, because she was in another passenger seat. (Never hand someone a magazine while they're driving, kids!)

"The Hacker Quarterly?" she exclaimed. "How is it legal for a bookstore to sell something like this?"

"This magazine has lots of great articles about interesting things that can be done with technology. What's so illegal about that?" I replied.

I'm an information security researcher. That's what *CIO Magazine* says I am, so I've decided to accept that. Most of my work involves writing thoroughly researched articles about IT security. The rest of my work involves writing and editing study material for the InfoSec Institute's CISSP and CEH (Certified Ethical Hacker) training programs.

Thousands of people in IT security read my work. But I'm also read by people in other areas of IT, and I assume the odd layperson stumbles upon my work as well.

One of my favorite books of all time is Steven Levy's *Hackers*. Steve Wozniak, Richard Stallman, Richard Greenblatt, Marvin Minsky, Linus Torvalds, Lee Felsenstein, and Bjarne Stroustrup are some of my heroes. I wish I could have been at MIT during the PDP era, or even a member of the Homebrew Computer Club. But as a Canadian born in 1984, I missed that opportunity.

Ask an ordinary person what a hacker is, and they'll either think of that Angelina Jolie movie, Lisbeth Salander from Stieg Larsson's novels, or some sociopath who penetrates a big corporation's computer network with the purpose of wreaking havoc. Anonymous and other hackivists have been in the news in the past several years, as well. So you and I know the words "whitehat" and "blackhat," but Joe Blow thinks all hackers are blackhats.

Heck, it gets worse than that. I've found people in other areas of IT with the same misconception. Even the IT security articles that other people write that I edit use the word "hacker" interchangably with "cracker" or "blackhat."

The International Council of E-Commerce Consultants (EC-Council for short) administrates the CEH certification. On their website, the phrase "Hackers are here. Where are you?' can be prominently seen. The CEH covers the basic knowledge that's needed to be a penetration tester. They emphasize the phrase "ethical hacker," because in their language, the word "hacker" alone means someone an IT department needs to watch out for. I write study material for people who write the exam! I've got to cover what's on it. I do what I can.

My late father was a popular novelist. He raised me to have immense appreciation for the power of words.

Think of how the media, marketers, politicians, and cult leaders manipulate the power of language for their own ends. George Orwell inspired the term "doublespeak." We see his fiction replicated in reality. "Used cars" become "pre-owned vehicles." The "Department of Homeland Security" makes Americans less secure in their "homeland." "Dolls" can't be sold to little boys, but "action figures" can be. "This isn't a comic book, it's a graphic novel!" Here in Canada, Prime Minister Stephen Harper's "Fair Elections Act" makes elections unfair. Once a month, I need to use "feminine hygiene products," but I'd rather call them "menstral blood pluggers," dammit!

I'm an avid gamer, so don't even get me started on "Digital Rights Management."

In the CISSP and CEH study material I write, and in my magazine articles, I insist on calling a hacker with malicious intent an attacker, or a cracker, or a blackhat.

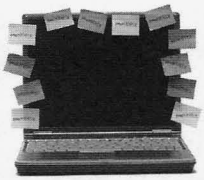
I'm doing everything I can to maintain and promote Steven Levy's use of the word "hacker."

If I can influence more people in IT and tech journalism, I can make life easier for those of us who like to mod video games, or tinker with open source scripting, or who do cool stuff with Raspberry Pi and Arduino boards.

I strongly believe that if we continue to let "non-hackers" think all hacking is blackhat, then the Silicon Valley billionaires win. They benefit immensely from the work hackers have done in the 1950s, 60s, 70s, and 80s. Now they get to reap their profits from overworked and underpaid computer programmers. With that money, they get to kill hacker innovation by spending big bucks on patent trolling. It makes my blood boil.

I'm pretty much exactly as old as *2600 Magazine*. I was born just a few months before Mark Zuckerberg. There's hope for the future. As I said, I do what I can.

Security Behavior



by Donald Blake

Everyone hates computer passwords. I can hardly remember last night, let alone a stupid x length password. Depending on how paranoid and delusional the organization is, a password can be very long and require some really crazy requirements. If I remember correctly, when I was in the Navy I had a password that was 16 characters long and required a minimum number of upper case letters, lower case letters, numbers, and special characters. I believe I used some sort of vulgar language relating to how much I hated the system for making me have to create such a long password and I wrote it down in Notepad.

At work I have access to five different systems, each requiring a password. Some of them require two step security to get access to the system. If I was paid a dollar for every time I had to enter my user name and password, I'd be able to retire! Using passwords to secure a computer network is actually silly. It's basically like having a club and all you need to access this club is the password to it. Computer networks are expensive to build and maintain and, more importantly, the information that they contain can be critical to the organization. If the network is ever compromised or abused, then the organization's world could change drastically or come to an end. With all the grief that passwords cause users, and knowing that an intruder can be really intelligent and have access to a lot of resources, no system can be 100 percent safe. There need to be better way to secure a computer network other than by using a password as the main line of defense.

Let's theorize. How do you have a computer system without using passwords and only a user name? Is it possible? Assuming we aren't corruptible and we could sit right next to that user and watch everything the user did, then yes, we could tell if the user is using the system as intended. Let's try and replicate the ability to sit right next to the user.

We need a system that can watch users in real time. This way we can watch what they are doing and if they do try to stray, then we can stop them.

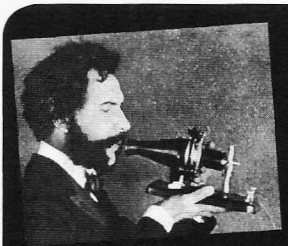
We need to know our user intimately and watch their behavior. Users don't normally access every piece of information on a computer network. They just use the network for their specific purpose. We need to keep track of the user's history and constantly compare it to what they are currently doing. We also need to keep track of their habits, such as how fast they enter commands into the system. This way, we can detect any changes in their behavior and, for an intruder to be able to use the user's account, they would have to match that behavior.

No user is an island, and the more things we can compare the user to the better. Let's organize users into groups and watch the groups' behavior. Each user in a particular group will have a similar behavior as all of the other users in the group. The users access the same files, do the same type of things, and do them in a similar way. We'll keep track of the group's history so we can make sure the users within the group are always doing the same or similar things, too. A user's behavior will match their group behavior and an intruder will now have to match the users' and the group's behavior.

No system is completely secure. Compromising computer networks is big business these days. Organizations depend on their networks to keep them and their users alive. It's far too risky, silly, and archaic to use passwords as the main line of defense for a computer network. A better solution is to use the user's behavior. If the users are monitored in real time, tracked in the right way, and grouped together effectively, then an intruder would have to know the user and the group the user belongs to just as intimately as the network does to gain access. Using user behavior will also stop a user from accessing things they aren't suppose to! Companies use human behavior to sell people stuff all the time. Let's be smart and use human behavior to protect us!

Thanks for reading.

Shout out to Violet, Norah, Kayla.



TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! Since I wrote last, I have been around the world clockwise once again. It was good to catch up with friends and fellow hackers in Europe and China, and to visit the amazing technology markets in Beijing. Technology changes very rapidly in China and despite being only six months from my previous visit, I was really surprised to see how much has changed.

One of the most exciting recent developments in telecommunications is the astonishing price drop in mobile phone chipsets, particularly for basic GSM technology. This is combined with massive improvements in both battery technology (which has gotten much greater), charging technology (which can reliably operate off of inexpensive solar cells), and power consumption (which has dropped). In Beijing, you can now buy a brand new, quad band, unlocked GSM world phone for less than eight dollars. These phones can remain powered on, able to make and receive calls, with a standby time of up to two weeks in between charges. Talk time is also truly astonishing. I remember when I barely got an hour of talk time on my enormous Motorola brick analog cellular phone, but basic GSM phones now boast talk time of up to eight hours of continuous usage - if your voice can hold up for that long!

Just stop for a minute and think about that. For under $15, you can buy a phone that works anywhere in the world for voice, text, and data, and a solar charger to go with it, and even if you don't charge the phone for two weeks, it'll still be able to make and receive text messages and can even log onto the Internet. It's completely mind-blowing when you think about it. I think the only reason that most people in Western countries haven't noticed is because handsets like these aren't widely available in wealthier places. When your mobile phone carrier's lineup is populated with the latest smartphones, it's hard to notice the availability of no-name Chinese brands at astonishingly low prices.

Now, let me be clear: these inexpensive phones aren't smart phones, and they don't support even 3G, let alone 4G technologies. However, they do work just fine for voice, low-speed GPRS data, and SMS messaging. And this is the *retail price*, and even includes value added tax! The wholesale price is about half of this, and it's for a fully assembled phone. So, you can infer that the component parts are even less expensive than this. Want to support the latest networks and fastest data speeds? The price is about five times as much, but we're still talking about $30 for the components. Making things even more interesting, you don't necessarily need all of the component parts involved in building a phone when you consider GSM scenarios that aren't phone calls.

"Wait a minute," you may ask. "GSM scenarios that use mobile phone components but don't involve making phone calls, you say? What might those be?" Well, actually, that's where things have gotten really interesting. Given the confluence of low cost, low power requirements, and creative charging solutions, some new and really exciting scenarios have been unlocked. Sensors are quietly but steadily being deployed to help automate everything from water and electric meter reading to weather monitoring.

Sure, sensors have existed in various forms and in various places for many years, and there have even been previous efforts at "smart meters." However, there have been a number of key issues. First of all, most sensors had very limited computing power because the availability of low-cost microcontrollers with low power consumption was limited. So, the technology was there to *gather* data, but *interpreting* it had to be done in a centralized location somewhere; you couldn't fit enough computing power on a sensor to do much meaningful interpretation. Today, with the availability of Arduino and similar microcontrollers, it's possible to build sensors with substantial onboard computing resources, without needing a whole lot of energy to do it. This means that sensors don't necessarily have to upload as much data to centralized locations for real-time

processing anymore because software can be more capable of making real-time decisions. Even if you didn't need to continuously gather data or centralize processing, the capability didn't exist to process data over a wireless WAN at high speed. Nowadays, GSM coverage is available almost everywhere, and 4G allows data transfer at speeds similar to Wi-Fi. This, combined with the plummeting cost of sensor technology, has unlocked some really incredible new scenarios. Some of the most interesting innovations are in utilities and - oddly enough - agriculture.

Many utilities around the country are starting to deploy smart meters, to which the tinfoil hat crowd has responded with predictable fury (they're mainly concerned about RF emissions). The Salt River Project in Phoenix has already deployed them in most areas, and the Los Angeles Department of Water and Power is beginning to deploy these as well. While the key reason (and most important application) for implementing the technology is eliminating the need for meter readers, smart meter technology also allows more data to be collected about energy usage and more creative billing to take place. You might recall that long distance charges used to vary by time of day and day of week. Calls were billed based on a day rate (the highest price), evening rate (around 20 percent less), and nights or weekends (around 50 percent less). This was done to provide an incentive to shift usage to off-peak times, so the phone company didn't have to build a lot of peak capacity that was otherwise underutilized. Your electric utility could offer similar incentives to use power during off-peak times. For example, Sunday evening is the period of lowest power usage in most cities. So, you might choose to do your laundry on Sunday evening if the rate were half as much as doing it on Monday morning.

Agriculture is also seeing a lot of really interesting new scenarios in wireless sensors, which are helping to reduce waste and improve efficiency. For example, farmers waste hundreds of millions of dollars a year replacing spoiled livestock feed. Farmers buy feed and put it in storage. The feed gets wet for one reason or another, and then it spoils. Typically, farmers will find out that this happened when they go to use the feed and find that it has spoiled. So, a company called Kongskilde has developed several types of moisture, temperature, and humidity sensors that can be stored with the feed. So, if a leak in the roof develops, the sensors will detect this and notify the farmer before his feed becomes spoiled.

Both of the above smart devices rely on a local mesh network, typically Wi-Fi, which then uplinks data to a centralized location via mobile Internet. However, there has been a lot of recent research (with some development) on sensors that communicate directly via mobile Internet. Given the water crisis in California, one of the most interesting pieces of research I have seen involves irrigation systems that are sensor-controlled. Most irrigation systems today operate on timers, and the amount of water used isn't an exact match for what is actually needed. So, most farmers overwater or under-water their crops (typically the former), which isn't good for either the crops or the water supply. However, given the vast distances, mesh networks don't make a lot of sense. These devices, along with other smart devices such as pH monitoring, can literally be "planted" along with crops. The power source? Often solar. In the case of irrigation, the amount of water sprayed can be precisely correct for the exact soil moisture level, leading to both higher crop yields and lower water usage. How can we continue to feed a rapidly expanding human population? Technologies like these will go a long way toward doing so, and they're all enabled by telecommunications.

And with that, it's time for me to finish eating this turkey sandwich. Hope you had a happy Thanksgiving, and best wishes for the new year! The world only gets more exciting every day.

References

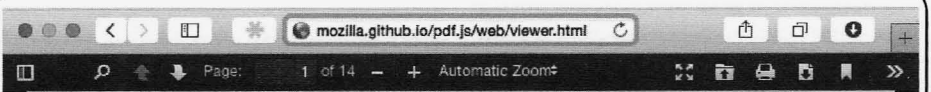
`http://goo.gl/XDxGXD` - a Smart Meter video from BC Hydro, which provides a good overview of the features and services brought by smart meters.

`http://goo.gl/AXGfsq` - Excellent FAQ and information from BC Hydro which in particular describes the science of smart meters. Designed for the tinfoil hat crowd.

`http://www.cityofgreensburg➥.com/MiNet.pdf` - Excellent technical whitepaper on Mueller Systems smart meters.

`http://goo.gl/9D4mCm` - Many technical whitepapers, along with sales brochures, for the Kongskilde agricultural sensor system.

`http://ijarcsms.com/docs➥/paper/volume2/issue1/V2I1-➥0007.pdf` - Detailed academic paper describing a prototype GPRS-based sensor network for irrigation.



Format De-Shifting

by Peter C. Gravelle
peter.c.gravelle+2600@gmail.com

Have you ever clicked on a link expecting a PDF, even seeing ".pdf" in the location bar, but instead of your friendly PDF viewer, you see a vaguely familiar interface, but with the "Print" and "Download" buttons removed? Then it's likely that PDF.js[1] is involved. But worry not, we can get you that file anyway.

Background

My wife is an apprentice plumber and, as an apprentice, has to take courses to learn her trade. This particular course was on the New York City Construction Code Plumbing Code[2]. Construction codes are made available by local jurisdictions for many reasons, including inspections, educating tradespeople, and a general commitment to transparency in government. Previous versions of the code were available in the PDF format. However, for the 2014 edition, the New York City Department of Buildings decided to use a new piece of HTML5 tech: PDF.js.

PDF.js is a PDF viewer written in HTML5 by the Mozilla Foundation. This means that any device that supports modern web standards and runs JavaScript can view PDF files. This is a big boon for a lot of reasons. The biggest one is mobile browsers with limited plugin support can view PDF files without mangling their formatting much. Another benefit comes to desktop browsers: many PDF viewing plugins are very slow to load and are very resource intensive (Adobe Acrobat, for one). Finally, PDF.js allows the content provider to (ineffectually, it turns out) block saving and printing the PDF in question.

Construction folks, as a class, are fairly technologically conservative, and do not appreciate change. In this particular case, my wife's instructor wanted to turn to sections of the code in class, but could not, as they didn't have an offline copy. Network access can be iffy on construction sites, so it's good to be able to keep a local copy in that case as well. The instructor issued a challenge to anyone in the class who could get PDF copies for him. My wife took up the challenge, but did not want to simply "print to PDF," as this would kill the anchor links. She reached out to me, and we began our investigation.

What Tipped Me Off

A few clues made it seem like this was possible. The first thing was the URL itself, which included a reference to a filename ending in PDF[3] as well as several references to "pdf_viewer/." Second, when I inspected the HTML code itself, I found each paragraph in DIV tags with very precise "data-canvas-width" attributes - out to over ten decimal places. No human would ever write that! So I took a look at the various <script> inclusions and eventually found a reference to PDF.js and the Mozilla Foundation. A little quality time with a search engine and the framework's documentation, and I stumbled my way into three possible methods of downloading the original PDF file.

Method 1: Ask Where It Got the File

My first method was the most direct. The documentation for PDF.js made it clear that most of the magic that happened took place in the "PDFView" object. So I opened up the JavaScript console in Chrome (or Firefox's Web Console) and looked at the various children of the "PDFView" object. A quick glance gave me "PDFView.url." Copy that URL out and put it into a new tab, and down comes the file!

Method 2: Watch It Get the File

Since the PDF viewer runs in JavaScript on your browser, the PDF is being sent directly to

you. Wouldn't it be handy if you could catch it in flight? Well, these browser consoles also have a lovely tab called "Network." Select this tab and run the Network tool, and you can watch the files in flight. In the case of Chrome, you need to reload the page. In Firefox, you click the button to start the process. In Chrome, the PDF is immediately visible and you can click it to download it. With Firefox, I had to click on the "xhr" tab to grab the PDF link.

Method 3: Just Ask It for the File Directly

This third method is an excellent demonstration of the value of looking at all options first. Another child of "PDFView" is the function "download()." Guess what happens when you run "PDFView.download()" in your browser console? Yep, the PDF file is immediately added to your download manager and into your downloads folder.

Conclusion

PDF.js is an excellent tool for a lot of things, including making PDFs more palatable on mobile devices. But sometimes you want the original format. And things like the construction code of your city is yours by right to read in whatever format you want. If you put all the smarts in the browser, then the browser has ultimate control!

Acknowledgements

In all things, I'm grateful to my wife, who puts up with my dicking around with tech until far too late at night. Thanks to the Mozilla Foundation for making PDF.js, a great tool with excellent documentation and a lovely backdoor of sorts. Best to faboo, TecknicalTom, and the Neg9 crew, and all those around the world yearning to be free.

Links

1. PDF.js: `https://github.com/mozilla/pdf.js`
2. New York City 2014 Construction Code - Plumbing Code: `http://www.nyc.gov/html/dob/html/codes_and_reference_materials/2014_cons_codes_table_of_contents.shtml#plumb`
3. NYC CC PC Chapter 1: Administration: `http://www.nyc.gov/html/dob/apps/pdf_viewer/viewer.html?file=2014CC_PC_Chapter1_Administration.pdf&section=conscode_2014`

by lg0p89

Just like sharks smelling blood in the water, the fraudsters will always be around when there is money to be had. This will continue to be a problem as long as consumers are click happy and don't *stop-think-connect* (does that look familiar?). People click, either at home - or much worse at work - on a link they think is legitimate. Suddenly, and too late, they realize this was a fraudulent site. As a result of their misfeasance, the person is told to pay a certain amount. They can only hope they are given the correct key to unencrypt their drive(s) and are once again able to access their information.

As we get more accustomed to one form of this, it always seems to generate slight variations to be released into the native environment. More ransomware has been in the news lately as this has occurred yet again.

The esteemed researchers at ESET have found the newest variation of ransomware that is beginning to run rampant. It was coded for the Android OS and has been titled Simplocker.

Business Model

Too often, we limit our thoughts of ransomware and other assorted malware as simply a few knuckleheads trying to get a few dollars and move along. This may occur in a limited portion of the instances. However, there has been a change in thought and operations. To have a clearer view of the motivation, one needs to remove the thought of the criminal aspect and look instead at the business aspect. To the fraudsters, this is not right or wrong, moral versus immoral. This is a business with a mission statement that boils down to their goal of bringing in more revenue.

Originally this started as Russian malware. The "uh-oh" message was in Russian and the ransom had to be paid in Russian rubles or Ukrainian hryvnias. The deviants, as the good business people they are, did not want to limit their target market. This, after all, would be a poor business decision. Think of it as if you were a retailer, for example. Would you limit your business model to only Arkansas, or would you expand to other states and countries? The natural and clear rationale was to expand. As long as there is a market for the product (although this is unlawful) and the delivery channel is present, this is a natural progression. The management of these people followed this same model and expanded their market. It has moved to English speaking countries. The notification has been changed to English and the ransom is now in U.S. dollars.

How it Works (To Your Detriment)

Once this precious piece of malware is loaded, it gains admin privileges. It then shows the infamous ransom message on the screen. This states, among other things, that your device is locked due to your illegal activities with the phone. To unlock your precious device, you have to pay a certain amount, which so far has been up to $300. It may even attach a photo of the user to the message, as taken by the phone's camera, ala RAT (remote administration tool). Once the user sees the picture of themselves holding the phone, they usually feel their stomach fall nine inches.

Another feature differentiating this malware and making it more fun to work with is that it encrypts compressed files on the SD card. It also uses AES for the encryption. It is notable in that the attack itself is complex, yet the encryption is not. It would appear prudent to have a more robust encryption, however this is adequate. It was also coded to gather information on the device itself, including but not limited to the model, operating system, and manufacturer. This information is returned to the C&C server. The curiosity with this is that malware of this type generally does not do this. The coders are generally more concerned with the money or ransom and how to get that into their account.

Resolving the Issue

The quick and relatively painless resolution to this stressful situation would be for the user to quickly uninstall the malware. The issue here is that the malware loads too quickly to do this.

The user can simply pay them and hope they are given the correct key to de-encrypt. If not, they are out of luck and $300. As a rule of thumb, it is strongly advised not to do this. This may be the quickest method, in theory, to regain access to your data. However, quick is not always good. If the user ends up paying, they will be on the list for others to try to infect, as they will know the user has a disposition to pay to make the problem go away. They may also not send you the correct key "by mistake" and demand another payment or two in order to send the "correct" info to decrypt.

ESET has a tool available to decrypt that would be helpful. Also, the user could use the last backup and recreate the files worked on in the interim.

Ongoing Issue

With this malware, there is easy money involved. All they have to do is send out their hundreds of thousands of automated emails to get someone to click. People do click on these. Although this number is not significant, it is money they don't have to do anything to earn. The users and business devices will continue to be targeted. The process will change ever so slightly as one attack is recognized and its definition placed in the anti-virus dictionary. It may be modified enough so it is not recognized as malware for the latest version. To decrease the user's headache and pressure in the chest after they see the ransomware message, the user needs to review what they want to click prior to doing it. If not, there will be yet more pain coming down the pipeline.

HOME DEPOT HACKS

by DKN

Yesterday, Apple announced its Apple Pay platform. I turned to my friend, a head cashier at Home Depot, to ask about their credit card breach and support for NFC (Near Field Communication). I'll call this person Shanayna.

Regarding the payment card breach, for "lots of weeks" before its discovery, Shanayna described to me how she would need to close a register for several days because a payment card reader failed to work. As soon as Home Depot got a card reader to work again, another card reader would fail. The failures, to her recollection, happened in incremental succession down the register line. Reader failures would start at Returns, then proceed through the second Returns device, then customer service, then Register 1, and so on. Since the failures and their fixes were spread over several days, nobody in the store noticed any patterns or correlations.

Regarding NFC, Shanayna described how, for a short time, her store had payment card readers that supported NFC. While the cashiers knew about the device support, it never worked. "It was never hooked up," she said. Some months after the NFC payment card readers were installed, Home Depot came back to replace them again with NFC-free readers. The NFC-free card readers are supposedly the ones her store had during the window of the payment card breach.

When she went to work today, "tons" of people came into the store to ask if they would be able to pay with their new iPhone. Home Depot had not prepared for this event, so in addition to having no NFC readers in the store, many of the cashiers didn't even know what Apple Pay, NFC, or tap-to-pay were. Remember, I'm asking this of a head cashier with several years' experience at the same location - a person you might expect to know if their registers support NFC payment or not.

Her story didn't stop there, though. She also described how the anti-theft devices can be hacked for petty theft.

Home Depot has been expanding its use of self-checkout. When there's a shortage of cashiers, the preference is to open self-checkout with four registers instead of a single, traditional register. Stores that still have traditional registers are then completely unattended by a cashier, though Home Depot has a compensating control: cameras. Cameras are only reviewed as part of specific suspicious events, however.

Higher-value items in the store have an RFID chip that should be deactivated during checkout. A zone on the counter of each traditional register is designated for RFID deactivation - and the deactivation zone works even when the register is unattended. Moreover, the deactivation field is not unidirectional. Thieves who pocket high-value, RFID-tagged items can apparently bump into the side of the register counter to deactivate a pocketed item, then continue to walk out the door without even slowing down.

Shanayna described a store near hers which went completely self-checkout, disposing of traditional cashier stations altogether. As part of the experiment, they saddled a single person to monitor eight or more self-checkout stations at once in addition to watching people exit the store.

The self-checkout solution compensates for flaws in the RFID field for traditional registers because the RFID deactivation field only activates when an item is passed over the barcode scanner. In the case of the overwhelmed self-checkout monitor, thieves can scan a $2 screwdriver at the same time they pass an expensive drill over the scanner without being noticed. They let the scanner read the screwdriver UPC, but cover the UPC for the drill. While the $2 screwdriver is logged for payment, the register activates the RFID field and the drill's RFID is deactivated.

For either the traditional register or self-checkout, the thieves walk out the door, then right back in to Returns and claim they lost their receipt. Home Depot gives store credit for the pocketed item and drill. You can guess what happens next, but if you get caught, they'll absolutely have the whole thing on camera. It seems Home Depot is betting that the losses from stolen items won't cost as much as the employees' wages that could have prevented the theft in the first place.

Leeching Music From YouTube For Fun, Learning, and Profit

by Synystr

Disclaimer: Downloading copyrighted music is illegal, blah, blah, blah. You guys already know this. Let's begin, shall we?

YouTube has become one of the biggest resources to find music on the Internet these days. Which is odd, since it started as a video-sharing community. This becomes more apparent as time goes on in this age of social media, as people continue to post music videos they like on Facebook and other communities to share with friends and family. Recording artists and labels have even begun to do this themselves in the form of lyric videos and preview clips, harnessing the power of sharing through the Internet to get their product out there and noticed.

I listen to a lot of chiptunes and ambient music, two less-than-mainstream genres of music. You could argue that they are getting more popular due to the advent of social media and sharing, but for a while, it was hard to find anything of the sort. YouTube has made that easier. Whether it is live performances, one- or two-hour mixes, remixes, covers, etc., you can find pretty much anything now, and YouTube is a great starting point in looking for it.

It didn't take long for people to figure out how to strip the music from these videos and save them as mp3 files so they could burn them to CD and listen to them any time they wanted to. Various websites have popped up that allow you to simply copy and paste a URL to a YouTube video, click a button, and download it as an mp3, allowing for an easy method in gaining new music.

I used these sites for a while, but I soon found myself tiring of the various pop-up ads, flashing "CLICK HERE!" buttons, bandwidth limitations, etc. Some of them didn't even work properly. Most sites I found were just trying to make a quick buck off of everyday computer users who just wanted their music. Thankfully, I found a solution in youtube-dl, a public-domain application in which you could download music from YouTube, SoundCloud, and other sites, using the same method of URL-pasting, only without all of the annoying ads.

Youtube-dl was a life-saver for me, and when I found out about the batch-download option, it was even better. However, I still had the task of encoding the files to mp3 manually, as youtube-dl just downloads the file as its native mp4 format. Enter ffmpeg - an open-source program that can convert video files from one format to another, including mp3 audio. With this, I could download the videos with youtube-dl, then encode them with ffmpeg. It was a pretty nice setup.

Still, I soon found that it was not enough. While this method was a lot more efficient than dealing with the crap-infested websites I previously had to endure, it seemed like it was less efficient than it could be. Doing one thing in one program, then doing a second thing in another, all to achieve one result - it seemed like the process could be simplified somehow.

During all of this, I was teaching myself Python 2.7 as a hobby. I hadn't coded in forever, and I felt like Python was the best way to whet my appetite and ease my way back into programming. At some point, it clicked - who's to say that I can't write a Python script that glues these two programs together cleanly and produce the same result with minimal effort? I would have coded my own standalone app in C or another language - that would have been the cooler, more respectful option - but I wasn't (and still am not) that experienced yet, so what's the next best thing? Take various already-existing resources and glue them together to make them work the way you want! Hackers do this all the time, so I figured it was the natural solution to my conundrum.

Thus, I began writing a script to download mp3 from YouTube. Eventually, I had a full-fledged script that, when executed, simply asked me to enter URL after URL of YouTube videos until I pressed ENTER, and then the script did all the work for me. I eventually even added in the option to burn the downloaded compilation directly to CD-R, which is really cool when I need a mix-CD for long trips in the car.

I will now walk you through how to achieve this yourself.

Note: This script utilizes system calls to the bash shell on a Linux machine, which is what I was mainly using when I wrote this script. As such, this exact script will only work on Linux. However, it is simple enough where you can easily modify it to any other OS you are using, Windows included.

Here is the first block of code. This is not required (other than the import statement, which definitely *is* required), but it makes maintaining the file structure and youtube-dl/ffmpeg binaries a little easier.

```
#********** LIBRARY
IMPORTS **********
#os for system
```

```
calls, time for delays so user can read output

import os, time

#********** INSTALLATION AND UPDATES **********
#This script utilizes ffmpeg, youtube-dl and cdrdao

print("Checking for youtube-dl and FFMpeg...")
time.sleep(3)

os.system("cd /usr/local/bin")
if not os.path.exists('/usr/local/bin/youtube-dl'):
       print("youtube-dl is not installed. Installing now.")
       time.sleep(3)
       os.system("sudo wget https://yt-dl.org/downloads/2014.05.12/
➥youtube-dl -O /usr/local/bin/youtube-dl")
       os.system("sudo chmod a+x /usr/local/bin/youtube-dl")
       os.system("sudo chmod rwx /usr/local/bin/youtube-dl")
       print("youtube-dl has been installed.")
       print("Now updating youtube-dl...")
       os.system("sudo /usr/local/bin/youtube-dl -U")
else:
       print("Checking for update to youtube-dl...")
       os.system("sudo /usr/local/bin/youtube-dl -U")

if not os.path.exists('/usr/local/bin/ffmpeg'):
       print("FFMpeg is not installed. Installing now.")
       time.sleep(3)
       os.system("sudo wget http://ffmpeg.gusari.org/static/32bit/
➥ffmpeg.static.32bit.latest.tar.gz -O /usr/local/bin/ffmpeg.tar.gz")
       os.system("sudo tar -zxvf /usr/local/bin/*.tar.gz -C /usr/
➥local/bin")
       os.system("sudo chmod a+x /usr/local/bin/ffmpeg")
       os.system("sudo chmod a+x /usr/local/bin/ffprobe")
       os.system("sudo rm ffmpeg.tar.gz")
       print("FFMpeg has been installed.")
else:
       print("FFMpeg is already installed.")

print("Installing/Updating cdrdao through apt-get. This is for burn
➥ing to CD-R. Install manually if you do not use apt-get and wish
➥ to burn CDs with this program instead of an external one.")
time.sleep(5)
os.system("sudo apt-get install cdrdao")
os.system("clear")
```

- First, we import the OS and time libraries, OS for system calls and time to insert a delay between operations. It makes the output easier to read.
- Next, we check to see if the youtube-dl binary exists in the /usr/local/bin directory. If it does, the program moves on. If not, it downloads a fresh copy of the binary to this location. In both cases, youtube-dl is also updated to the latest version using the built-in -U option, as sometimes YouTube can change their encryption algorithms and render youtube-dl largely useless until it is updated. We then do the same thing with the ffmpeg binary, to the same location.
- cdrdao is then downloaded and installed using apt-get. I put a warning in to compile from source if the user is using a non-Debian distro and wants to have CD-burning work.

```
#********** DOWNLOADING VIDEOS/CONVERTING TO MP3 **********

urls = []
currenturl = "1"
while currenturl != "":
   currenturl = raw_input('Enter URL (just hit ENTER to stop and
```

```
➥ begin downloading): ')
   if currenturl == "":
       break
   urls.append(currenturl)

print ("done with queue entry. Downloading videos from YouTube:")
time.sleep(3)

count = 1
for i in urls:
   if count <= 9:
       os.system("/usr/local/bin/youtube-dl " + i + " -o 'Track_0"
➥ + str(count) + "-_%(title)s.%(ext)s' --restrict-filenames")
   else:
       os.system("/usr/local/bin/youtube-dl " + i + " -o 'Track_"
➥ + str(count) + "-_%(title)s.%(ext)s' --restrict-filenames")
   count = count + 1

print ("Finished downloading queue. Finding downloaded videos: ")

downloaded = []
for file in os.listdir('.'):
   if file.endswith(".mp4"):
       print file
       downloaded.append(file)
       print ("Here are the found files: ")
print '[%s]' % ', '.join(map(str, downloaded))

print ("Now converting videos: ")
time.sleep(3)
downloaded.sort()
for x in downloaded:
   os.system('/usr/local/bin/ffmpeg -i ' + x + " " + x + '.mp3')

print ("Finished converting. Cleaning up: ")
time.sleep(3)

for file in os.listdir('.'):
   if file.endswith(".mp4"):
       print ("Deleting file " + file + "...")
       os.system("rm " + file)
```

- The first part of this section is an infinite loop which asks us for a YouTube URL with each iteration, which we then paste in. The URL is then appended to a Python list and kept track of. If no input is entered and we simply press ENTER when it asks for a URL, the loop breaks, and we move on.
- After the loop breaks (ENTER being pressed with no input), another loop begins, with one iteration per URL we entered. Each iteration calls youtube-dl, stored in /usr/local/bin where we downloaded it earlier, along with a custom formatting option (this can be changed however you see fit - consult youtube-dl's documentation for more options) and also the option --restrict-filenames. This option is required, as problems can arise with formatting due to YouTube files containing spaces and Linux/bash truncating the filenames because of this. As you can see, an IF/ELSE statement is coded in, appending a 0 before the track number if the variable "count" is less than or equal to 9, and taking the 0 away if not. This is to conform to a naming convention that will allow burning to CD without messing up the order of the tracks.
- The program then lists all of the files it downloaded, complete with extensions. This part is not required to get functionality out of the program, but I added it in while debugging the script so I could tell if it was working correctly, and I liked it so I kept it in. Feel free to remove it if you feel otherwise.
- After this, a third loop is executed, one iteration per mp4 file downloaded. This time, it calls ffmpeg, also in /usr/local/bin where we downloaded it earlier. The call to ffmpeg takes the mp4

files that youtube-dl downloaded and converts them into an mp3 with the same name. (The .mp4 is still retained in the final filename, but I was too lazy to code around that.)
Finally, the script deletes all mp4 files, as we no longer need them.

Shortly after this article was accepted, I used my script to get some more music, and ran into some issues with the name formatting I explained above (adding in track names and such). After some research, I found that my script updated to a new version of the youtube-dl program that it utilizes, as it is intended to do, but the new version, for some reason, switches the order of the -o option and the URL to download. I was able to remedy this by modifying the applicable section of code above to:

```
count = 1
for i in urls:
    if count <= 9:
        os.system("/usr/local/bin/youtube-dl -o 'Track_0" +
➥ str(count) + "_-_%(title)s.%(ext)s' --restrict-filenames " + i)
    else:
        os.system("/usr/local/bin/youtube-dl -o 'Track_" +
➥ str(count) + "_-_%(title)s.%(ext)s' --restrict-filenames " + i)
    count = count + 1
```

This basically is just switching the order of the -o option and the URL to download. I am not sure why this change occurred; I was unable to find a changelog for the program. I am unsure if this is a bug in the youtube-dl program, or an intended feature/syntactical change.

```
#********** BURNING TO CD-R **********

switch = raw_input("Would you like to burn the downloaded MP3 to
➥ CD-R? 'y' for yes or anything else for no:")

if switch == "y":

   for file in os.listdir('.'):
       if file.endswith(".mp3"):
           os.system("/usr/local/bin/ffmpeg -i " + file + " " + file
➥ + ".wav")

   wave = []

   for file in os.listdir('.'):
       if file.endswith(".wav"):
           wave.append(file)
   wave.sort()

   os.system("touch cd.toc")
   os.system("sudo chmod 777 cd.toc")

   f = open('cd.toc','w')
   f.write('CD_DA\n\n')

   for z in wave:
       f.write('\n\nTRACK AUDIO\n')
       f.write('AUDIOFILE "' + z + '" 0')
   f.close()
   raw_input ("Please place a blank CD-R into your CD drive, then
➥ hit ENTER:")
   print ("Now burning CD...")

   os.system("cdrdao write cd.toc")

   for y in wave:
       print ("Deleting file " + y + "...")
```

```
        os.system("rm " + y)
    os.system("rm cd.toc")

else:
    print ("Skipping CD burning.")
```

- The burning part of the script begins by asking if they want to burn a CD or not. If so, a loop begins encoding all downloaded mp3 files back into WAV format, as this format is required for cdrdao. If they don't want to burn, this entire block is skipped.
- A new Python list is created and filled with all of the new WAV files that were just encoded, and then we use the sort() method to sort them by track name for burning.
- After sorting, we create a new file called cd.toc, which is the table of contents file for cdrdao, used to tell the program what to burn and in what order. This has to be formatted a certain way, so we first add the CD_DA part at the top of the file, then two line breaks, and then we use a for loop to write the data required for each track.
- After the cd.toc file is created, the program asks the user to put in a blank CD-R and press ENTER. When this is done, cdrdao is finally called, inputting the cd.toc file we generated earlier as an argument. The CD burns.
- After the CD is burned, we remove all the WAVs, as they are no longer needed, as well as the cd.toc file. We then move on.

```
#********** POST-OPERATION ORGANIZATION **********

name = raw_input("Give a name to the compilation you've made:")
name = name.replace(" ", "_")
os.system("mkdir " + name)
os.system("mv *.mp3 " + name)
print("Moved MP3 into a folder called " + name + ".")
print ("All finished. Enjoy! Hit Enter to terminate program.")
raw_input("")
```

- This final part is optional but recommended. Since the script runs and writes to the current working directory, I made this block of code for organization purposes. First, it asks for a "compilation name," which the user can name any way they want. I like to name them after genre type.
- This name is then converted to a format where underscores replace blank spaces, and then a new folder is created with the name the user types, and all mp3 files are moved into this new folder.
- At this point, just hit ENTER to end the program!

Sure, it was a quick, dirty, and noobish Python script, but it works just fine. I was able to figure out how to automate two programs into completing one task with some Python grease. And because of this, I am now even more eager to learn as much as I can about programming, and I encourage anyone who is reading this, no matter what skill level you are at, to take a look at it yourself if this article piqued your interest. Even if you don't know how to code, try learning it. Pick a language (I'd recommend Python, it's doing wonders for me), use Google, and teach yourself. You'd be surprised at what you can accomplish.

That's the cool thing about this. Sometimes, you get an idea, and even if you can't create something entirely from scratch, if you have the resources, or at least the knowledge to find said resources, you can still make something that works the way that you want it to.

Feel free to use, modify, and distribute this script in any way you see fit. I already am doing so myself. I plan on adding in GUI and porting it to Windows.

Rock on, everyone!

Sources

youtube-dl: `http://rg3.github.io/youtube-dl/`
ffmpeg: `https://www.ffmpeg.org/`
cdrdao: `http://cdrdao.sourceforge.net/`

Recon on Disney's Magic Band

by EndlessFapping

The people at Disney have invested a billion dollars in developing a waterproof high tech wristband that's meant to be an all inclusive pass to everything Disney. The wristbands are in use at the resorts, parks, and cruise ship. The bands can be used for a multitude of things like resort room access, purchasing products, ride fast passes, individualized ride experiences, and even location tracking. Purchases are made by establishing a PIN, in conjunction with the wristband. This creates a two-factor authentication mechanism when visiting concessions or buying products.

The wristbands are a marketing data gold mine. Disney will be able to track which rides get used as well as family spending habits and perhaps even track foot traffic through their parks. It also makes spending money easier for their guests - think people at the pool.

Intrigued, I wanted to learn more about these new high tech toys of Disney's, so naturally after looking online I was able to locate the FCC ID (Q3E-MB-R1G1) of the wristband and search the FCC website for information on the band itself. Unfortunately, I'm not an RF guru, but I figured doing some recon would be fun and I could let others use the information.

Digging through the FCC site, I was able to find out the wristbands themselves are powered by a non-replaceable coin battery and contain UHF and HF RFID tags. The antenna is embedded into the PCB, which itself is overmolded in plastic to prevent access to the internals without creating permanent damage to the parts. The antenna type is an inverted F with a maximum gain of 0 dBi with no RF connector between the radio and itself. The wristband operates completely in the 2.4Ghz band. NFC and RFID appear to be enabled on the device.

I wanted more info on the infrastructure the wristband communicates with, so I started snooping and found a LinkedIn profile of a Disney employee that has all of the FCC IDs of the proprietary infrastructure devices listed proudly as devices he helped develop. Those FCC IDs may have been a bit more difficult to find were it not for the that profile. Thanks, Disney Manager guy!

The following descriptions were pulled from the LinkedIn profile and will probably be useful:

- "Experience Touch Point" - FCC ID: Q3E-XTP-R1G1 and FCC ID: Q3E-XTP-RA-R1G1 - An HF RFID reader used at Disney park entry locations, FastPass+ Attractions, and the Test Track attraction at Epcot. Combines advanced light and sound to deliver a unique touch interaction with the MagicBand.
- "Long Range Reader" - FCC ID: Q3E-XBR-R1G1, FCC ID: Q3E-XBR-S-R1G1, and FCC ID: Q3E-XBR-R1G2 - A 2.4GHz RF transceiver that communicates with the MagicBand and provides Magical experiences for Disney Guests and key operational metrics. There are three models in use today to support various use cases.
- "Experience Payment Device" - FCC ID: Q3E-XPD-R1G1 - Provides a unique payment experience for Disney Guests supporting "Touch to Pay" with the MagicBand and other payment methods. Highly themed to fit the MagicBand ecosystem. Can be seen today at all Disney Resort front desks and Point of Sale locations.

Magic Band FCC ID: Q3E-MB-R1G1

Experience Touch Point: FCC ID: Q3E-XTP-R1G1 and FCC ID: Q3E-XTP-RA-R1G1

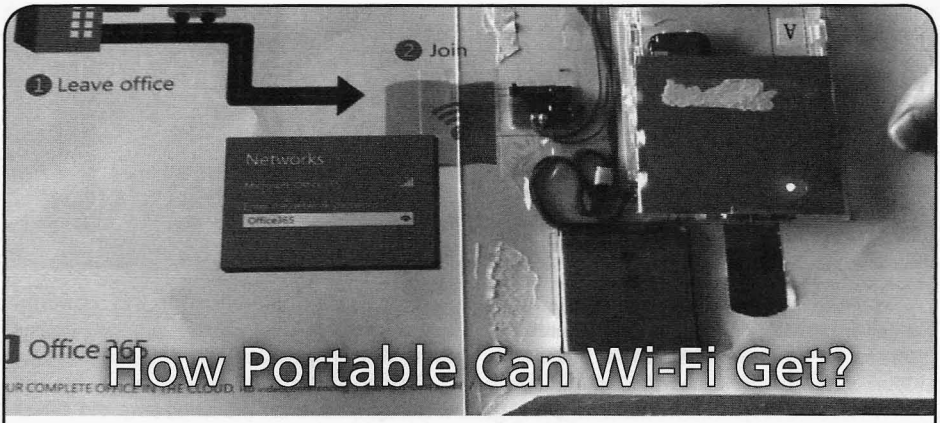
Long Range Reader: FCC ID: Q3E-XBR-R1G1, FCC ID: Q3E-XBR-S-R1G1, and FCC ID: Q3E-XBR-R1G2

Experience Payment Device: FCC ID: Q3E-XPD-R1G1

Interestingly, I tried sharing the guy's LinkedIn profile with a friend of mine and my friend was unable to view the profile because he was too far removed from the guy in question. Ironically, I was able to see the guy's profile almost entirely because I was not logged in as a LinkedIn user. Go figure that rationale.

Browsing through the FCC documentation, I could see requests to keep some of the information confidential. Unfortunately, it looks like that was accomplished on some of the material. I figured more information would likely eventually be pulled off the public facing FCC site, so I copied all of the information I could find, including snippets from the LinkedIn profile. I've zipped all of that information up and made it exclusively available for *2600* readers here: `http://www.filedropper.com/magicbandsystem-2014-05-29`

Enjoy!



How Portable Can Wi-Fi Get?

by the Piano Guy

If you subscribe to *Fortune Magazine* in the United States, and if you're on a select list of high-roller technologists, you may have gotten some hardware included with a recent issue. Microsoft decided to promote Office 365 by putting a T-Mobile Wi-Fi router in the magazine. Thin enough that it could go into a magazine, the router is set up to provide 15 days of service for up to five devices at once, and is supposed to work three hours on a charge (it is rechargeable).

In some ways, doing this was kind of a waste. They only sent it out to select technology professionals (alas, I was not among the lucky anointed), and it is very likely that these people already carry Wi-Fi access around with them on their cell phones. While it certainly gets the attention of the movers and shakers in the industry, Office 365 should have already been on their radar.

Making a router small enough to go into a magazine, irrespective of the reason or the client, carries other ramifications. The router was manufactured by a company named Americhip. I expect that Americhip is going to be the recipient of many social engineering attempts to get samples of the router, and that people will be dumpster diving outside of tech companies for their routers out of used *Fortune* magazines. I've already sent in my request for one to do research on it.

More importantly, as the Canadian government noted, these magazines were carried by tech managers into government secure facilities. I have to think that this also happened in the United States, though we will never know for sure if it did. Government secure facilities aside, most major corporations with research and development facilities have a "no transmitter" policy in their research and development areas. I have personally worked in areas in corporate America where before a person can go into certain areas of headquarters, all transmitting devices and photo-capable devices must be relinquished and are locked up in RF-shielded lockers. They won't be thinking to look for magazines unless alerted.

Unless we can get our hands on a unit, we will not know if the SIM card is removable. My thought is that this has to be a design feature, since Americhip may want to use a different carrier for a different advertiser. If the SIM card is removable, so is the 15 day limit on the service, as well as the restriction on using T-Mobile. If we get our hands on a unit, then there is the possibility of hiding a Wi-Fi hotspot in very inconspicuous places. It would be illegal to set up the Wi-Fi hotspot at a Starbucks and tempt people to connect to it for use with Wireshark, but I expect that it will be done. The equipment that is currently sold that works in such a small form factor is quite expensive. Being able to get this hardware this small at a price that it can be repurposed to function this way and is small enough to put into a magazine will increase the vulnerabilities that are out in the wild.

The takeaway from all of this is that technology, as it gets smaller and less expensive, will increase the vulnerabilities that black hat hackers can perpetrate, and increase job security for the white hat hackers that will help protect average people. Keep everyone safe out there.

The Hacker Perspective

by Shadow E. Figure

The stage is set as follows: my entire hacking career has developed in prison. Bill Clinton was still the President when I arrived. Since then, Moore's Law has transmogrified technology to science fiction proportions. Think back a little bit. Google was in its infancy, Microsoft ruled the world, cellular communications few and far between, two-way paging the latest trend. This was my reality the last time I was in the free world! Most telling, the size of the entire Internet then was about equal to its output each day now.

Rather than finding myself immersed in this decade plus of advancement, I have been positioned to study it from afar. Lurking on the periphery, silently assessing the effects of this whirlwind which has ensnared the entire globe.

Considering the cosmopolitan nature of consuming technology and the strangely esoteric nature of understanding technology, hacker culture's orientation in society suddenly becomes of paramount importance.

I don't think hacking is an outgrowth of digital technologies. I believe we can trace its origins all the way to the primordial genesis of our bipedal ancestors. It is an inborn spark, an inherent element of consciousness. A meta-program or sub-routine which developed as a high-level adaptation during the burst of human evolution. The ephemeral instinct expressed as curiosity, that desire to know and interact within one's own terms; even today these traits have taken a hand in shaping the future. If you have read your McLuhan, you know that the various shapes and forms of technology are externalizations and outward projections of consciousness. Consider then, the latent power of pushing the envelope in every direction.

Seeking evidence of the hacker spirit in antiquity, we must look no further than the mythic archetype of Prometheus. Zeus, father of the Gods, has forbidden to mankind the use of fire. Covertly entering Mt. Olympus, Prometheus liberates fire from the god's abode and delivers it to man. Consequently, man nearly destroys himself with this powerful new technology and, in the process, dooms Prometheus to punishment for his actions.

Behind this myth lies the ingenuity and curiosity of humankind harnessing the forces of nature towards its collective benefit. What eventually came to be science was the continuation of these traits. Every new invention or theory has always been a revolution against orthodoxy....

These revolutions have driven civilization forward. Zeus has become Big Brother; Prometheus, Emmanuel Goldstein. We now stand at a crossroads where the virtues of ethical hacking, exploration, experimentation, and the sharing of discovery are the most potent weapons against obscurity, ignorance, and totalitarianism. Our symbiosis with advanced technologies is nearly complete. Every sphere of our activity has become increasingly dependent upon them. Who else is going to discover and elucidate what is going on? ISPs? Cellular carriers? The FCC?

To anyone with the moxie and drive to engage in "hacking," the methods and inclinations are natural, if not hard fought in the trenches of doing. So how do we gauge the importance of our work? Only by continuing to carry on can we hope to give voice to our need for freedom. I can think of nothing more important than that.

Lofty philosophical musings aside, I'm sure some have begun to wonder what types of opportunities for hackers there are in prison. Believe me when I tell you that finding out from me is perhaps much better than learning first-hand. There may even be a segment of people who are unaware that such opportunities exist at all. In my experience, the entire process is catalyzed from the endless series of what we will call "unfortunate luxuries," which seem to dominate prison life.

The first and most obvious is time. With no social responsibilities (aside from keeping a good grip on the soap), I can pursue at my

leisure massive amounts of hard data. Prison libraries tend to make this situation dynamic; strange donations and weird bequests have stocked the shelves with outdated textbooks and obscure how-to reference manuals. In a minimal amount of time, the entire history of communications technology was assimilated. But more than this, I developed a penchant for "hidden" or "secret" knowledge. This lead to a study of cryptography, which is nestled snugly right next to hacking. To pursue such studies in books leads to a tendency to transfer this knowledge into the real world. The ordinary and mundane transforms into the wondrous and magical; how does all this stuff work? Thus begins the endless quest.

The second unfortunate luxury happens to be security. Prison epitomizes the illusion of security. This is an important distinction, because security by design is only imposed through acceptance (or force). If you accept a restriction, it becomes a fact. Entire industries exist within the prison underground geared towards subverting and passing security. There are some interesting implications in this, which we will get back to.

For now, let's examine another unfortunate luxury: prison labor. If you are picturing a chain gang on the side of the road, wait a minute - this is far more dubious. Corporate America has had an epiphany which has led to a long series of contracts to employ prison labor for all sorts of interesting tasks. Think of it as outsourcing within the country.

So this is how I came to find myself seated at a Windows box for the first time. It's one thing to read endlessly about bits and bytes and code and packets of data and networks. It's quite another to get to experience it. I landed a "data entry" job, once the demand for computer-literate individuals became apparent.

Really, any robot could have done my job. And I suppose this eventually led to a little exploration. That, and the fact that curiosity seems to trump inhibition. It started innocently enough - just some poking around to discover what was on the server and what I had permissions to do. Is finding one's limitations where it always begins?

Spaced over 13 drives were hundreds of gigs of disorganized and mostly obsolete data. Clicking on a hyperlink one day, I discovered that I had access to a browser, but port 80 was blocked. I went right to telnet for a net scan. Since everything else appeared to be opened, I went for FTP. I had thumbed a few copies of *2600* at this point; this is the only way I can explain the first destination that popped into my head. I quickly retrieved everything available, but to this day one file has haunted me: "This is an unrecognized IP address." With the sheer volume of data on the server, I figured it would be safe to access some harmless information. No one ever forbade me from doing so.

I didn't even look at what was obtained. Instead, I just printed it all out and took it back to my cell for processing. It is not every day that you behold the Holy Grail; this is what the HackFAQ was to me at that time. Reading all the box plans was an irrevocable step in my life down the road to hackerdom. As I sat reading, a terror began to dawn on me however; the possibility of a bread and water diet, left to rot in the hole. Action was swift; armed with a new set of resources, I hoped back on FTP and retrieved a packet sniffer. With no ability to install programs, I had to camouflage the executable as a customer file and coerce my boss into the task of unwitting hacker.

When I accessed the data dump in Notepad, I immediately thanked my luck; no encryption. Obtaining new credentials became a trivial task. From a workstation, I was able to log on as "sysadmin" and cover whatever tracks I could think of. I never did anything diabolical, but here I was: a Class A felon with unrestricted network access to a vast corporate playground. Account data, credit card information, unlimited Internet access. Not to mention all the havoc that could be wreaked from the ability to spoof emails and impersonate various executives.

My task accomplished, I moved on to other, more constructive projects. Buckminster Fuller noted that you cannot expect to change a system by criticizing it; you do so by making it obsolete. Being able to view the overall architecture of their data flow, I was able to spot a few bottlenecks. I proposed a common sense solution and they actually provided me with some development tools. I went from being a data monkey to being tasked with creating a new database. I quickly understood the common disdain for script kiddies. How can you develop a proper respect for data security until you write those first few lines of code? The bug bit me; the desire to program only seems to grow over time.

Unfortunately, I lost the job due to some non-work-related shenanigans before I was able to complete the project. My departure was in haste. With no one to maintain the data dump, I often wonder how large the file got before they

detected the network breach?

I lamented that this was the end of my digital life. It turned out to be the beginning. Do all hackers at some point develop a sixth sense? An automatic gravitation towards mischief?

What caught my eye about the new law library computers were the giant steel plates bolted on the front of the slave towers. Really? USB rootkits and live CDs are pretty few and far between here. This is such a great metaphor for D.O.C. security. I sat down to investigate. The available d-base seemed straightforward enough (two words, both rhyme). Many links were disabled, shortcut keys were off, and text fields couldn't read JavaScript. I surfed around a little and found myself on the parent company website. I typed a search string into the search portal and stared at Google for about a minute trying to compute the use of this giant steel plate.

The only question that remained for me was how to force a reboot. I puzzled over this long enough to notice the wall outlet. The boot sequence showed a Linux platform, but I ended up with a strange prompt I hadn't seen before. It notified me I had 20 seconds to authenticate, but if I entered any credentials, even bogus ones, the count would renew. Worse, there appeared to be no intrusion countermeasures whatsoever. To solve this problem, I had to revert back to old but useful methods; I shoulder surfed some valid credentials. I now had access to the Department of Corrections LAN. The account I compromised was pretty boring. But in the process of trying to get a better one to peek around with, I realized something. Every username was the officer name. Every password was their badge number. It couldn't be any easier.

There are many more adventures and exploits, but you get the picture. A new dimension has recently arisen; corporations have delved into every area of our lives. You can purchase an inordinate amount of stuff suddenly. I have an MP3 player which can send and receive emails and pictures (only to pre-approved addresses and the data is uploaded via Fireware to a kiosk on the yard, then to a central server for forwarding). There are kiosks for video-calling and flat screens which double as monitors. The latest rumor says secure cell phones are next. In an institution of over 3,000 inmates, at least one unauthorized cell phone was confiscated in the last year for every ten inmates. It's pretty obvious why they would consider doing so. They can't seem to get control any other way, even if cellular jamming seems trivial. Perhaps the intel is too good?

I may not have any high tech anecdotes of de-obfuscating code or other Herculean tasks, but these experiences should at least illustrate that no matter where hackers are, there is something worth exploring. Hopefully, there is some inspiration also; the level of access to all of you on the outside is miraculous, an endless plethora of gadgets and information. I, on the other hand, live in a world where an oppressive agency suppresses my rights any chance they get. Their hand touches everything with control, and nearly everything is outlawed. Thought crime is a reality. You may say that people in prison deserve this, but you would miss the point that this type of control is not only coveted by nearly all authorities, it is a possible future for everyone. This is our gauge of importance for what hackers do; it is our job to prevent this future.

I leave you with one final thought. It has occurred to me that the propensity to designate hackers as criminals stems from a similarity in operating procedures between the two. In either case, the world view tends towards dissecting the systems encountered. Once the exploits, vulnerabilities, and weaknesses have been exposed, the distinction occurs. A criminal will use the information for some type of personal gain and attempt to horde it. More often than not, this activity is in service to some other felonious pursuit, rather than learning. Hackers, however, experiment with the structure of the system, doing all sorts of things that were never intended, all the while uncovering many new discoveries in the process. They then share their experience with the community, pushing the collective a little further along.

This free and open exchange of information undermines the illusion of security which the creators (read: "profiteers") of such systems hope to propagate. An unwillingness to address the issues, which are exposed, makes the hacker paradoxically more dangerous to those interests, and creates a motive to vilify the observant voice. Criminals exploit ignorance; hackers expose it. Thus, all the confusion.

Well, I'm off to buy some more low compression MP3s for $1.80 a song, and to do some more exploring. If parole comes through, perhaps I'll see you at a *2600* meeting. Until then, Happy Hacking!

Shout out to the warden, Left to Rott, and the Secret Society!

The Surveillance Kings: Who's Really Behind Who's Watching Us

by DocSlow

Several years ago, I had been working on an article involving corporate computer security and how malware was changing the way companies approached security. I had conducted over 100 interviews with various computer security analysts from small companies to very large corporations. Most of these analysts simply related to me that they were too busy fighting on the malware front - both night and day, and had little time or no authority to actually analyze what was going on. Then I met Brad (not his real name - he was afraid to speak publicly). Brad told me he had information that went far beyond the current story I was writing, and that if we could meet, he would show me all the evidence he had collected.

Brad said that the story was not so much about malware, but rather about a developing surveillance project he uncovered, and the fact that it could be used like current malware to spy on anyone at any time. This story unfolded around 2005 and is only now relevant in light of all the recent whistle-blowing concerning the surveillance of everyone on the planet by certain governmental three-letter orgs. Brad had some 4000 pages of accumulated documentation, all collected and stored on CD-ROMs. Now, it has been almost ten years since this article was started, and recent events warrant that the story be told.

Computer security was Brad's main avocation for nearly 30 years, with malware forensics as his specialty. He was hired by a very large company to deal with a growing malware problem in the fall of 2005, and he was excited to do his job. He told me he had succumbed to the indoctrination offered him by the company (called "orientation") and fully accepted their brand so as to be a part of what he assumed would be an elite group within the organization. The company was IBM.

Initially, Brad said that he and the new recruits that were hired with him were given tip-top laptop computers, installation CDs labeled "IBM Transitioner" with Microsoft XP at its core, and a stipend to set up their home offices. Brad jumped into the fray with both boots, eager to get started thwarting those whose intentions were to cause havoc within the company. Brad and the new recent hires went about setting up their machines to do the tasks they were assigned, and Brad noted that there were some curiosities with those laptops that immediately started to arise. There were two coworkers who were initially hired with Brad, and Brad said they were mostly unobservant of the anomalies that accompanied the new machines - they just assumed "the things were slow." The first thing Brad noticed after he installed the "IBM Transitioner" OS CDs was that the CPU usage at idle was around 60 percent. The others mentioned that they did notice it, but declined to investigate as to why this was happening. Brad told me his first simple exploration into the anomaly was to observe what was happening to the XP OS with Sysinternal's "Process Explorer." It showed that an application on the hard drive entitled "PC" was responsible for the excessive activity.

Brad then stated that he began to look in "Program Files" for the application, and it existed, but the activity of the CPU as presented in Process Explorer was curiously absent. He was sure the rest of this application should exist somewhere on the hard drive. It didn't. Brad related that his first assigned task with the company was to research the possibility of a viable BIOS malware application, and so he thought maybe that's where it was residing - in the BIOS. But further investigation revealed it was simply installed on a hidden partition on the hard drive. The structure of the app was such that many calls were derived from the application's base install, and then redirected to the hidden partition. WTF was going on here?

Brad was able to access the apps being called on the hidden partition and found audio recording apps, video capture apps, screen capture apps, and keyloggers. Brad thought, "Great... what have I gotten myself into here?" He wondered what the purpose of these apps was, and why they were being run without any interaction from the user?

Brad then employed another Sysinternals app, and it would appear to reveal what was actually going on. Brad had installed and run "TCPView" on his assigned laptop and found that, periodically, packets of the collected data were being sent to an IP address in Boulder, Colorado - a mainframe station for IBM. As he tracked the data transfer, it became apparent that the transfers were happening every five

minutes. Apparently, IBM was spying on its employees.

Tasked with protecting the company's some 300,000 employee computers from malware attacks, Brad brought his discovery to the attention of his new "superiors." He assumed they would understand that this activity was a compromise to the real security of their systems. He was wrong. Brad was told they would get back to him shortly. Two days later, they convened a meeting with Brad and told him not to speak of what he discovered, and that he would probably be terminated should he do so. Brad had already alerted a few coworkers that they should slap black electrical tape over the video cam, and insert a dummy phono plug in the external mic jack. They did so, and were soon approached by corporate goons to remove them - or else. Soon thereafter, Brad was removed from the Malware Forensics program, and was relegated to a simple sysadmin position.

IBM has a long and sordid history of nefarious data collecting practices in its background. Edwin Black, author of *IBM and the Holocaust* (*http://www.ibmandtheholocaust.com*) chronicled that the sale and implementation of the IBM Hollerith machines significantly advanced Nazi efforts to exterminate Jews, and IBM has never once officially commented on the allegations prodigiously referenced in Black's *New York Times* bestseller.

His book details the story of IBM's strategic alliance with Nazi Germany. It is a chilling investigation into corporate complicity, and the atrocities witnessed raise startling questions that throw IBM's wartime ethics into serious doubt. IBM and its subsidiaries helped create enabling technologies for the Nazis, step-by-step, from identification and cataloguing programs of the 1930s to the selection processes of the 1940s. And guess what? Brad was aware of this and told me that he contacted Edwin Black. Black warned him to be careful if he ever related any of his experiences with the company. Shortly after Brad's encounter with his corporate controllers, he told me he quit IBM.

"One of the guys I worked closely with on the 'team' was fired within days of my resignation," Brad said.

"I called him and we chatted about all of this. Initially, he was quite keen on exposing the old guard. A few days later, when I spoke to him on the phone, he stated he wanted no more to do with me... and hung up on me. I never spoke to him again."

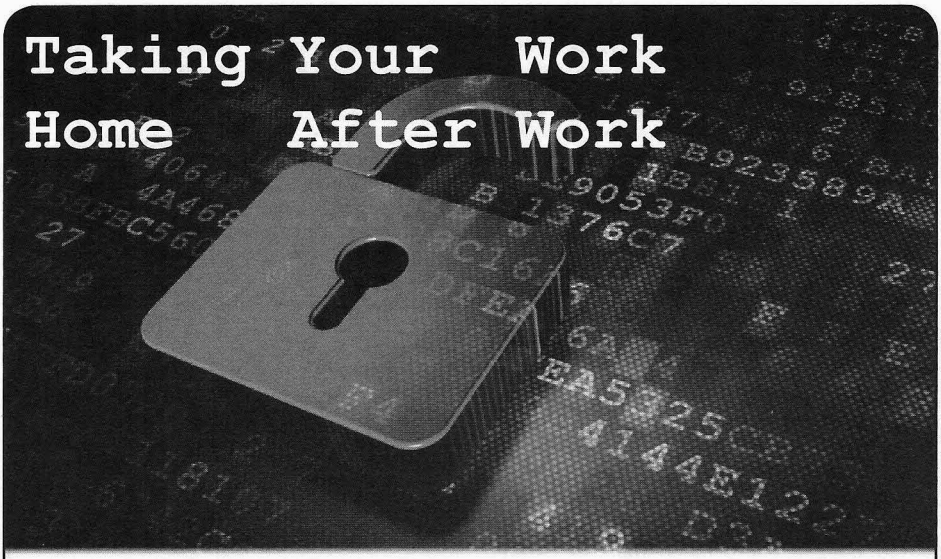
What had become clear to Brad soon after having left the company, and after analyzing all of the data he had collected, was that IBM was developing and perfecting a surveillance program - not simply for spying on employees - but for spying on U.S. citizens as a whole. IBM's inter-connectivity with DARPA and hints at the company's capabilities with respect to their surveillance abilities were, curiously, mostly public. It can be easily looked up on their website. Their perfection of early data mining practices had evolved over several decades into applications that could watch over all activities of the general public. Already, private commercial applications were being offered for sale to companies to spy on their employees, and human resources divisions across most corporate entities embraced them wholeheartedly. Brad said he has been asked at many of the companies he has worked at to spy on employees and covertly record their computer doings on a very regular basis.

One of the spookiest things Brad told me at the time was that he had uncovered a completely proprietary operating system developed by IBM that almost perfectly mimicked the Microsoft OS on its surface, but that it secretly contained all the surveillance applications noted above - and it was being tested on employees and civilians alike. I asked him how he thought it could be unsuspectingly delivered to the public. Brad said he had evidence that it was actually delivered in real OS security updates, and it could entirely replace the real OS!

I recently contacted Brad (he's doing well with his own company now) and asked him after all these years what his thoughts were concerning his experiences.

"With recent allegations that the U.S. government has implemented programs to spy on its citizens without any accountability, this information finally has some credibility." Brad then stated, "This technology was being developed long ago, and has now been perfected by all of the giant tech corporations most of us think of as friends of new technology." I asked Brad if he had kept up on the technology and if he had seen any new developments within it. He said, "Yes, it's far better than it used to be. Back in 2005, it was being tested only - now it has been widely implemented, and has been ported to many other operating systems. No one is safe from it. The kings of surveillance are all around us, and there's no going back."

Taking Your Work Home After Work



by GerbilByte

So there I was. I was drafted in to work for a small company (who shall remain nameless, but for this article we will call the company Bumble Bee Internet Security Services) for several months. At the end, in addition to receiving a juicy paycheck, I realized that I had written a load of little scripts that I wanted to keep.

I zipped up my folder of goodies to email to myself and encrypted it for obvious reasons, then attached it to an internal email to send it.

DENIED!

Bumble Bee Internet Security Services (BBISS from now on) was a company whose email systems were in "lock-down" and they had mega security implemented all over the place. You couldn't even send an email with a swear word without a "digital complaint!" (##...
➥email not sent as it contained
➥ the word 'BUM'...!##)

Instead, I tried to open my Yahoo Mail email account to add it as an attachment, as I knew Yahoo Mail wouldn't complain.

DENIED!

I changed the file extension and tried again.

DENIED!

Yahoo Mail didn't complain, but the bloody monitoring system of BBISS bloody well did!!! How frustrating!!! (##...You are not
➥ authorised to send outgoing
➥ files of that type...!##)

With a bit of a social engineering chat with the systems admin, I realized that the monitoring systems blocked *all* encrypted content as it couldn't be scanned, and all .zip, .gz, .exe, .sh, .pl etc. files are also blocked due to.... obvious reasons!

"Hmmmm!" I thought, as I often do in these circumstances. "How do I get around this?"

I went back to my internal email account, as I knew my email's signature included the BBISS logo which was a .jpg.

"Aha!" I thought. For obvious reasons. But due to lock-down, I didn't want to use the email systems due to "tracing" and prevention of any future employment with BBISS. "Are the same monitoring systems used for outbound files?" I wondered.

Going back to my Yahoo Mail account, I attached a .jpg to an email and it got uploaded.

BINGO!!!!!

"So what did you do next Gerb?" I hear you ask.

Part One. Saving The Data

Well, what I did was a very simple task and very easy to do. Let me talk you though it in steps, boys and girls, as it will make more sense that way. By the way, despite being an Internet security company, BBISS used Windows. For *un*obvious reasons.

- Grab a normal .jgp file from somewhere. I used the .jpg from the internal email signature. Place this in a folder to keep things easy and separate. We will call this file piccy.jpg.

- To the same folder, copy the encrypted .zip file. We will call this file scripts.zip.
- Open up a cmd (or command, depending on Windows flavor) prompt and cd to the required folder. Then run the following command:

```
copy piccy.jpg /b + scripts.zip
➥ /b combined.jpg
```

What have I done here? Well, Microsoft have been really nice and allowed the stringing together of files into a single file using the copy command. I have used this to create a single file that consists of a .jpg file and an encrypted .zip file.

Back to Yahoo Mail.

My next step was to try and attach this file to an empty email.

```
##File uploading.....Complete!##
```

Excellent!!!

The file was now in my draft email and saved. Logging out of Yahoo Mail then back in allowed me to confirm that my "loaded" .jpg file was there in my drafts email. Excellent news! I didn't even get a single electronic complaint!

So what was my next step?

Part 2. Recovering The Data

When I got home, I opened my Yahoo Mail account, opened the draft email, and saved the combined.jpg to a folder on my Ubuntu machine. Back to using *real* computing power!

My task now was to split the file into two: piccy.jpg and scripts.zip. I wasn't actually interested in extracting the .jpg file, so I needed a way of extracting the info.zip file, which was the second part of the file. Which makes it harder as I didn't know where the start of the second file began!

So how did I go about this? Well....

Perl is a fantastic scripting language that allows you to do *anything*. If you don't know Perl, learn it. Seriously, learn it. Your life will be much enhanced once you've learnt it! Trust me on this.

Using Perl, I quickly wrote the following script:

```
#!/usr/bin/perl
use strict;

my $bytesToIgnore = $ARGV[0];
my $bytesRead = 0;
my $fileName = $ARGV[1];
my $fileOut = $ARGV[2];
if ($#ARGV != 2){
 print "\nUsage:\n   extract.pl
➥ <bytes to ignore> <source>
➥ <dest>\n\n";
}
print "Extracting $fileOut\nIgnor
➥ing $bytesToIgnore bytes from
➥  $fileName...\n";

open FILE, "<:raw", $fileName or
➥ die "Couldn't open $fileName!";
open FILE2, ">:raw", $fileOut or
➥ die "Couldn't open $fileOut!";
binmode FILE;
binmode FILE2;

my ($buf, $data, $n);
while (($n = read FILE, $data,
➥  1) != 0) {
 $bytesRead++;
 if($bytesRead > $bytesToIgnore){
   print FILE2 $data or die
➥   "Error writing $fileOut!";
 }
}

close FILE;
close FILE2;
print "$fileOut has been created.
➥\n\n  *** 2014 GerbilByte ***
➥\n\n";
```

To run the script, you have to run it as follows with the following parameters:

```
perlscript.pl <image_size_in_
➥bytes> <source_file.jpg>
➥  <destination_file.zip>
```

What the script does is run down the source file and ignore the first x amount of bytes (x being the file size parameter, the size of the "real" .jpg image). Once it has skipped these bytes, the rest of the file is then read and copied to the destination file (destfile.zip). This is the one we want! And it works!

If the example command above was to run, then you would end up with a file called destfile.zip. Have a look at it. Open it. Read one of the files in there. Unzip it. Do whatever you want with it! Whatever you do, you will be asked for your password to unencrypt your file! That means one thing: you've successfully extracted your encrypted .zip file! Well done, you. Give yourself a round of applause.

And there you have it. How to take your work home after work. Obviously, don't try this with sensitive data or anything that - depending on your employer's rules and work ethics - you would still be liable for and face disciplinary action or even prosecution. So be wise.

Now go celebrate by having a beer. Unless you are a kid, in which case have a glass of milk!

Enjoy yourself and be safe.

The Perils of Lackadaisical Updates

by lg0p89

Organizations differ in size. There are the massive multi-national corporations (MNC) and the small- and medium-businesses (SMB). The MNCs could be the familiar General Motors or Royal Bank of Scotland. The SMB may be the mom-and-pop business or the community banks. There is a wide variety to choose from for these.

There is a natural economy of scale with activities. There is a cost with any activity, such as pushing updates or implementing a new system. These costs may be comprised of not only the direct costs (e.g. if you have to purchase the software), but also the indirect costs (e.g. the labor of installation and the overhead attached to the people doing the work). If there are very few users to push an update to, the cost per user is higher. For instance, if the cost to push a patch is $200, and there are three users, the cost per user would be higher than if there were to be eight users. Thus the more users, to a point, the cheaper the cost will be per user. I note the "to a point" due to certain instances where the number of users require more personnel to do the work. So the line showing the cost per user would be straight to a point and then slightly change when more people would be needed. Think of it like walking up a mountain. You are walking straight up the mountainside until you reach a plateau, when you have to adjust and continue up the mountain.

This equation, while simple, may not quite work as well for the MNC due to the number of IT workers involved across regions of the U.S. and countries across the planet. There may not be the scalability with this that would be hoped for. It's moderately clear that there is an economy of scale with pushing patches at once. This is basically simple algebra.

Twist

This is not referring to Chubby Checker (from the way back machine). If the admin does one push for the patches, it seems as though it would in theory be less costly than doing the same push multiple times. The cost, in terms of time and money, would naturally increase if you had to check every machine to see what version of the application was being run.

Reality

Recently, I was sitting at work trying to find something to do. You know the drill. You are in between projects and you don't want to open a case to get started on just yet. I had heard of an issue for a few months where an application was working as it should and for another user it was not. Seemingly, there was an issue here. For all the users, the application should work the same. If this is not the case, then there probably should be a red flag and an opportunity for a project. For my disclaimer, no I am not the admin.

We received an email early in the afternoon re: the forms library. This is where we stored the documents that are used frequently by the business. One of these forms was a PDF where the users would type in a customer concern and forward it to the department that it affected. As they typed in the issue, it was maintained in the form. As it was sent, so was the information that was typed into the form. So this was an interactive PDF.

It turns out there are numerous versions of Adobe floating through the business being used by all the happy users. No one knew or still knows all the different versions that are being used. The issue was that the older version did not support the function of sending the completed PDF form.

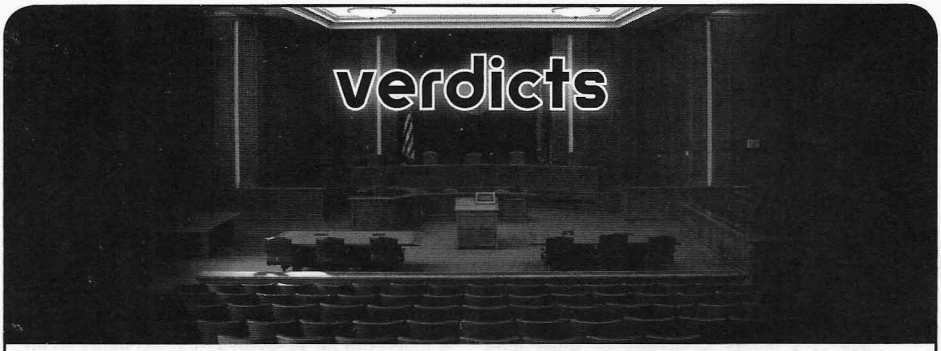
Solution

One would think, as there is an issue, it should be addressed in some format. The scope would be to check all of the boxes (this is a small business, so it could be done within four days), verify which version was in use, and update if needed. The second goal would be to see what happened so this would not occur again. Seemingly....

Well, the plan is to do nothing. All the while, with the sound of crickets in the background, the problem is not being addressed. To fix this in the future would erode any economies of scale and the cost would increase exponentially. To not fix this does appear to be the route taken.

Conclusion

When you have a project or updates to push, as we all do, it makes more sense to do these as needed across the board. To ignore them appears to be foolish and only adds to the eventual cost and complexity to eventually fix this. Then, of course, I would not have much to write about or you to read.



Curiosity

Dear *2600:*

My wife and I are very interested in educating ourselves with all your knowledge. How do we become members? Is there a process? If so, please do tell us what that is, so we can get it started! Thank you!

David and Sarah

Your enthusiasm is very inspirational. And maybe just a little scary. The best way for you to learn is to read and experiment. There's no membership or formal process. Anyone telling you there are courses you can take to learn hacking is basically trying to sell you something and it's something that doesn't work. You can certainly gain knowledge with the more information and interactions you expose yourself to. But to become a hacker requires you to think like a hacker - ask questions, push the boundaries, think differently, and don't be surprised when you meet resistance in all sorts of places. That spirit can be nurtured and inspired, but it ultimately comes from within. Good luck.

Dear *2600:*

May I please have a public key from you so I can encrypt an article submission? Thank you.

Undecodable Name

While we still believe this process is entirely too kludgy and poorly designed for most people to make use of efficiently, we will make one and only one key available on our website. Invariably, people will use an invalid key from decades ago that can't be canceled or will encrypt to their own key instead of ours or perhaps use an incompatible version or application, all of which will ensure that we can't read the encrypted message. Until such time as encryption is the norm and it's implemented sensibly and transparently, please only use our key if it's really necessary, as we've found that problems arise more times than they don't. We simply don't have the time to try and debug whatever issues arise each time and we certainly don't have the time to engage in lengthy correspondences to try and troubleshoot the problems.

Dear *2600:*

What is your Phoenix address?

Renee

What a strange question. We don't have one. Why on earth would we? Perhaps you mean the address of our monthly meeting that takes place there. Rather than take up valuable space reprinting the same information, we instead direct you to the meetings section which appears in this publication, as well as on our website.

Dear *2600:*

When is the cutoff date for submitting a meeting for the summer issue? And what kind of info would you need from me to put this in motion?

Mel

Well, here's a little tip, considering that this is now the winter issue. Waiting for us to send you a personal reply is going to result in frustration and a lot of time going by. Unlike other magazines, we don't have a huge staff of people dedicated to all kinds of tasks. Rather, we focus primarily on publishing and pretty much leave it to our readers to shape things to their liking and keep us apprised. So our autoresponse would have told you what is expected for a new meeting and, if you send us updates, your meeting will become official. Simple. Many people, however, expect us to contact them directly to discuss this, which is simply not going to happen unless, perhaps, you're planning one on Mars (and have the means to get there).

Dear *2600:*

Good morning. I want to know if this message has anything to do with you or members of your site: HACKED BY DEBIAN EVILZ MAYHEM AX1S NICK1 - TUTTI I DIRITTI FREGATI!!!!!!!

If so, I ask that you please un-hack my site.

Dan

Well, that does certainly sound like us. But to unhack a site, you need the services of an un-hacker. Regrettably, we don't have those certifications. Next?

Dear *2600:*

I locked my iPhone 5. Can u guys unlock?

Willie

We publish a magazine, sell hacker soda, and occasionally put on a kick-ass conference. We don't unlock phones for the public, but will happily print any info that could help people achieve such goals.

Nothing personal, but this, incidentally, is indicative of a disturbing trend among many of our recent letter submissions. They're basically the length and style of SMS messages, with lousy grammar, poor spelling, and lack of depth. We prefer real words, sentences, and paragraphs. Plz!

Dear *2600:*

Someone helpfully suggested I submit this blog post as a *2600* article. It's currently licensed under Creative Commons, but I wouldn't mind licensing it under something else if it helps.

Liraz

A blog post is already public, so that alone disqualifies it as an article. You're free to make an article you write public after it's published, but we don't print material that's been previously published, whether online or on paper.

Dear *2600:*

i was wondering if i could speak to you about a security problem i was having?

Blake

Another one of those Tweet-like messages that we hate. We're not security consultants, but we've been known to pontificate on security issues when they're presented to us in more than 140 characters. Please don't expect a personal reply or give us specific info that would violate anyone's privacy, as we intend to address such problems right here in the open.

Dear *2600:*

Who was the manufacturer of custom padlocks at the HOPE with the Big Brother banners?

Thom

And it's the 140-character messages that somehow expect us to do the most work. So we have to figure out which of our conferences had Big Brother banners (wasn't too hard - The Fifth HOPE from 2004). Now we have to go through our records and figure out who was involved in custom padlocks. We spent about an hour trying to track this down before realizing what a waste of time this is. You've likely gotten distracted and stopped reading before the second sentence, if you even remembered to pick up this issue at all. For anyone else interested, perhaps watching the lockpicking talk from that conference (Channel2600 on YouTube) might reveal a clue. We'll happily share any info discovered on this mystery.

Dear *2600:*

Do you have any resources for cyber-security? Thanks.

Antony

Yes, we're good, thanks. (Perhaps we should make a rule that answers to vague SMS-like questions cannot be longer than the questions themselves.)

Dear *2600:*

Why does *The Hacker Digest* have volumes 1-4 and 25-30? Where are volumes 5-24? I'm new to *2600*, and I'm trying to find the answer. Were they ever created, or are they just not archived? This is a great periodical, and I'm going to support it!

Alexander

We started releasing The Hacker Digest each year after we started digitally publishing. We then got to work on the earlier editions and that's pretty much what we're in the middle of now (Volume 5 will have come out since you wrote this). We've managed to speed up the process quite a bit (thanks to a suggestion from a reader right here in the letters section) so that five digests now come out each year. We suggest our lifetime digest subscription for those who want to get everything we've ever printed and will ever print in digital form.

Dear *2600:*

Regarding *The Hacker Digest* in PDF at the *2600* store, I assume that's the same as the quarterly edition of the magazine. Is the PDF searchable or was it just scanned so it's an image?

Chris

The Digest has the same content as the previous year's issues. Some of them are rearranged so they flow better as a single publication. The more recent editions are searchable while the really early ones are scanned as images.

Dear *2600:*

Is there a rough estimate on when submissions for presentations and panels can be submitted for the next HOPE?

Steve E.

Now this is what we like to see: eagerness for the next event almost as soon as the previous one ends. We should know more once the main coordinators start checking out of their respective asylums in the spring.

Dear *2600:*

With all the news on the "new" chip card credit cards, could someone reading this please write an article on how they work, maybe a dump of the chip, and how one would attempt to crack it? Also would be interested in the target chip cards as I've played with them and the reader a little bit. Also, *USA Today* claims you can't make a counterfeit chip card. I find that hard to believe and I'm sure you should be able to get a "blank" one that can be read and written to. Any thoughts?

Bryan

If anyone would know, it would be some of our readers in Europe, where those cards have been in existence for years. We would love to see a thorough article on this technology and any weaknesses it might have.

Deals

Dear *2600:*

If memory serves, I have had eight published articles with this one in your magazine. As I understand it, ten can be used for a lifetime subscription.

I will write them anyway, but I'd like to know if I may send $52.00 in lieu of getting two more articles published before achieving the lifetime subscription?

Article Writer

We don't recall any such deal, but then, we've had a lot of them over the years. If you can find evidence of our ever having offered that, please let us know. As far as we're aware, ten articles will get you ten years (subscription, not prison - hopefully).

Dear *2600:*

Greetings from a longtime follower. www.2600.com/magazine/domains.html describes the arrangement by which one who registers and maintains a "2600" top level domain receives a subscription while the domain remains registered. I think I first became aware of this offer in the 1990s, saw an opportunity yesterday in Slovenia's .SI, and grabbed it.

2600.SI shall be NXDOMAIN no longer!

The wording isn't precise in terms of the desired technical arrangements, but I'd like to set this up and take you up on the offer. Quickly spot-checking 2600 -dot- a dozen or so ccTLDs, I see participation in this program is not universal across the namespace. I have not found a working example of what I think this should look like which I can emulate.

If I were to simply CNAME www.2600.si to www.2600.com, would that do the trick and qualify me for a subscription? What would be optimal? I guess the web server has a static enough address (been in the same /24 for around 13 years per Netcraft) that an A record would work? I don't have any dedicated infrastructure built behind this, but can do whatever can be done with somewhat extraordinary DNS.

I found some samples of this - 2600.SK and 2600.CZ - which seem to have A records, not just CNAMEs. (WWW.2600.CZ is CNAME'd to 2600.CZ which is an A record.) Shall I arrange 2600.SI like either of these?

The phrasing "have a machine of some sort in another country, [...] free lifetime subscription for as long as you keep the machine up" doesn't precisely describe what I have here, but I get the feeling the requirements aren't terribly rigid. I registered a Slovenian domain, the authoritative name servers for that zone (at least some of which are in Slovenia, but are not mine in any sense) know and tell others about the domain's delegation (SOA) to some other name servers (not in Slovenia and also not mine). I expect most of these "other people's boxes" should remain up and reachable for the near future, so resolution can happen. To me, this seems to capture the essence of the objective. I think the intent is to claim the name and not necessarily to have some dedicated physical presence in each currently recognized political section of Earth, and we can accomplish that for certain.

I've delegated the domain to afraid.org and made it semi-available for others' use of *.2600.si subdomains, potentially utilizing afraid.org's snazzy and open dynamic DNS service.

If I were to plant another such flag in another section of the EU or elsewhere on the globe (where I find NXDOMAIN and presumably could register another 2600.*), maybe you'd throw in a shirt, back issues, or other swag?

Many thanks.

Sangamon

You did indeed manage (somehow) to find our old outdated page that made this offer many years ago, so we will extend it to you. (We have since deleted the page.) This was once a neat way to spread news of 2600 to other domains back when there weren't so many of them. It would be a bit much for us to take an interest in every possible top level domain now, although there are probably a few (like .mil and .gov) that could spark some interest. Please just forward your domain to the existing www.2600.com page and we'll keep the issues coming.

Fun with Meetings

Dear *2600:*

First off, *love* the magazine! I just recently got into it a month ago and I love the articles! I even love the telephone booth pictures in them - sad to see most of them get all rugged. Fanboying aside, I would like to start a meeting in my local area. I would like to start just one until I am sure it will be successful. I would like the meeting to be called "Coffee and Code." We won't be primarily discussing programming, but really anything in our alike minds that we would like to talk about. I'll report back on how well the first meeting goes.

Please respond soon.

Stephen

A couple of things. As we try to make clear, the only response you'll get from us (other than these replies to letters) is the auto-response if you email meetings@2600.com. That answers nearly every possible question someone could have when organizing a new meeting. Second, our meetings don't have names. They're just 2600 meetings. And these aren't meetings with agendas and a board of directors. They're the equivalent of a cocktail party without the cocktails where you mill around and talk to different people without any age or background restrictions. It's always been about more than just programming. This is also where we open the doors to the rest of the world, which is why we should always welcome outsiders when they wander in. Good luck.

Dear *2600:*

Unfortunately, the meeting cannot be held on Friday due to high customer traffic near the end of the week. However, they say Monday through Wednesday is perfect for it, especially for the default hours. Is it possible to make an exception for this? Please respond as soon as possible.

Stephen

OK, a couple more things. All meetings take place on the first Friday of the month, with the only exception being places where this conflicts with religious observances, in which case the meetings are on the first Thursday. Next, it is not necessary to ask permission to gather in a public space. (This is one of the reasons why we don't recommend anything that isn't completely public.) Places like malls may technically be private property, but they are in essence public gathering areas, particularly food courts. If most of the people in the group are customers of something in the area and there aren't any disruptions or illegal activity going on, you generally won't run into any problems. If you do, we need to know about it.

Dear *2600:*

I finally found the wherewithal and attempted to attend the last *2600* meeting in Leeds, U.K. Sadly, the bar staff told me that they had been asked about it by a few people, but they knew nothing of it. I fear this gathering may be defunct or, worse, full of drunken wedding guests (in the room the meeting usually takes place in).

On another topic (another letter?), I was not aware of any financial difficulties *2600* may have (I ought to pay more attention?), but would, say, a two

year subscription to your physical magazine help?

Null

Concerning the meeting, if a few people are asking about it, that means there is at least still an interest in the meetings taking place. Somebody may have dropped the ball on being consistent and communicating with people. It's not hard to salvage it. Either continue to show up and wait for other people and/or get the word out locally that the meetings are still happening. You can also come up with a better location and start fresh. This is why it's good to have an updated website for your meeting, so people know it's still current and so that people can write in if there's a problem.

As for helping us out, subscriptions of any sort are always the best way to do that. We appreciate it.

Dear *2600:*

"2600 Reader Meeting" is listed as a music group on SongKick.Com. This allows anyone registered on the site to list a "concert" by this hot "phreak rock" group at their local meeting venue. Why bother? Because when you use your Foursquare app while at a meeting, you not only get to "check in" to the location, but you can check off that you're here for "2600 Reader Meeting" as well. Cool, eh?

Richard Cheshire, Phreak & Hacker

As long as people aren't expecting a concert, sure, why not?

Some Facts

Dear *2600:*

I just downloaded the HOPE talks and can't stop listening to them. After hearing all the BS from corporate media for years, it's so great to hear the truth from the people who really know what's going on. Thank you for putting on the conference and providing this content online. I just wish more people knew about the important work you guys are doing. Over the past 20 years, I've told a lot of friends about *Off The Hook* and the HOPE conferences, mostly electronic and software engineers and they all love your show. No one else is putting out this kind of content.

I've heard about the illegal eavesdropping for years, but having Snowden and so many other experts talk about this in one conference really hit home. This is such an important message that I'm sending out a link for HOPE X to everyone I know.

It was great to hear Daniel Ellsberg encouraging anyone who can make a difference to become a whistleblower. I hope it leads to something. After hearing him say this, I started to think about how I might be able to help the cause. I don't have anything earth shattering, but I am very knowledgeable in the details of the main digital switch used in this country for voice calls, the 5ESS system. And there is a detail about the design of the system that can be used for surveillance that very few people are aware of.

I started in Ma Bell in the late 70s, just as the 5ESS was being designed, and worked with the equipment for many years. I got to work with the very first microprocessors produced by Bell Labs in 1982. By the late 80s, AT&T was producing one billion dollars of 5ESS equipment per year as the whole country was being converted to a digital telephone system. Watching the digital revolution happen beneath one 33-acre roof was a remarkable sight. Many of my friends tell me I should write a book about it. Maybe I will someday.

For many years, I had the electronic schematics for the entire 5ESS system and studied them extensively. Part of my job was to analyze the designs and help the techs troubleshoot the bad circuit boards.

When your voice signal comes into the central office, it goes through protection circuits (in case of lightning) to an 8:1 concentrator and then is converted to a digital signal in the TN335C circuit pack. And this is my main point: after it is converted to a digital signal, it splits into *two* paths! One is the primary channel and the other is a back-up channel in case the primary one failed, so you wouldn't get a dropped call. We were told repeatedly that this was done for reliability. There was a joke going around that if the system didn't need the back-up channel, the signal would just go into the "bit bucket." But now I'm starting to wonder about this. Ma Bell and our government have been in bed together for the last 100 years. Dropped calls mostly happen when going at least ten miles, so for this to make sense, the back-up channel of your voice must leave the local central office and travel some distance. Think about it - every single phone call in this country for the past 30 years has had a real-time duplicate channel of voices running through the phone system!

I'm sure this is how the FBI does a wiretap; it's very easy to send a software command to reroute the back-up channel of your voice. Maybe the phone companies have found a way to make money by re-routing every back-up channel of everyone's calls to the NSA. Send it all to the Utah center in real-time, use voice recognition software, and you've got Big Brother! Maybe this has been secretly ordered by the President because of the emergency powers they grant themselves every six months since 9/11 like Tom Drake has been referring to.

Looking back, it seems obvious now the 5ESS was designed from the very start in the 70s to provide this total 100 percent eavesdropping capability. An example of how close Ma Bell and the government are occurred in the 80s just as the digital revolution started. I'm not sure how well known this is, but the 3B central controller for routing phone calls for the 5ESS was purchased by the NSA for years! Not an entire phone system, just the 3B controlling unit. It's hard to say how many, but it could easily be over a hundred. The rumor in the factory at the time was that the NSA was using them for code breaking. At the time, the 3B controller had hundreds of the fastest processors in the world and it kind of makes sense. On the other hand, I now wonder if the NSA modified the 3B controllers to be implanted into strategic locations wherever the 5ESS was installed, especially in foreign countries. I'm starting to realize a lot of what we were told was probably disinformation to keep anyone from knowing what was, and is, really going on.

The rumors from the truck drivers who delivered them to the NSA were kind of strange. They were told to go to a certain intersection at 3 am, get out of their truck, don't look back, and get into a waiting car. They would be driven back to work and the empty truck would show up at the factory docks a few weeks later.

Just thought you might be interested in this.

Keep up the good fight and thanks again for all your hard work.

Anonymous

Had we printed these suspicions a number of years ago, we believe they would have been widely dismissed, even amongst our own community. Today is a very different story. We encourage anyone with firsthand knowledge to write in with their theories and facts.

Dear *2600:*

Here's how to use a U.S. bank mobile address to get around the U.S. bank's website's refusal to support Linux. (It accepts only Windows and Mac OS!)

Obtain a U.S. bank mobile logon address. (For example, https://mm.usbank.com/webkit/Username.aspx?9C83487808C1BDA9=AFA42EAA81C7E349EC75FC7B454FB5EB)

Enter your username, challenge, and password.

Easy. But *log out!*

(Keep my name out of the papers, please.... A free issue would be nice.)

A Friend of Freedom In Cottage Grove

We honestly didn't know this was a problem. We'd be curious to see if anyone is helped with this info. As for free issues, we can't afford to do that for every letter writer. For your next discovery, flesh it out into an article and you could get a subscription!

Dear *2600:*

One of my favorite tools as a sysadmin is Cain. For years, I have been using it to discover user passwords across a Microsoft domain running Exchange Server with webmail access. So here's the step by step.

Download Cain and Abel from http://www.oxid.it/.

Set up your sniffer interface.

Start the sniffer.

Go to the network tab and hit the + function to start a network scan. Once completed, click on the APR tab in the bottom.

Click in the empty top half of the screen where it says status, IP Address, etc., etc.

Again, click on the top + function.

On the left side, select the exchange server. On the right, select the gateway IP. Click OK.

Now start APR (radioactive icon).

Once you see packets flowing, go to the Passwords tab in the bottom and click on the http filter on the left.

You should now see all usernames and passwords from users using webmail or active sync to retrieve mail.

Enjoy and play it safe.

The 3rd Bit

Dear *2600:*

Comcast has a history of crippling firmware in the Comcast branded modem/router combos given out to customers. The latest one of these caused port forwarding issues and disabled bridging mode, which essentially crippled any "power user." To rectify the port forwarding issue, one has to contact Comcast to enable bridging mode so you can utilize your own router. Comcast allows you to do this in three possible ways: Calling them and being put on hold for 200 years; contacting a tech and having them do it on site; and finally, you can do it via live chat. Being the Internet savvy gentleman that I was, I decided to head over to live chat to see what I could do. Upon reaching the live support page, I was prompted to enter some basic personal information (name and address), yet no account number or "secure" personal data was required. I realized I was onto something.

After rebuffing the rep's attempts to sell me home phone service, we finally got down to discussing enabling bridging mode. After explaining why I wanted bridging mode, the friendly tech (surprising for live chat support) instructed me that I may lose my Internet connection once she enabled bridging mode. Sure enough, my network went down as the tech predicted and the router/modem proceeded to reboot. Once rebooted, I found that the wireless access point built into the router/modem was disabled, so I hooked up my replacement router to the router/modem combo and, sure enough, that worked. The significance of this exercise? Well, by knowing someone's basic personal info, you have the ability to shut off the default wireless setup, thus locking out their Internet connection until someone can get a hold of a Comcast tech, which is unlikely considering that the only method to contact a Comcast tech in a timely manner is via live chat, which can't be reached without Internet. Solution? Comcast needs to require the account number and should enable bridging mode anyway because the provided router/modem combo is beyond terrible.

DaRkReD

Offerings

Dear *2600*:

I heard your late June podcast. Bad luck! Here is some cash to help out. Cash is king.

S&T

Thanks, but we're not looking for handouts. If people send us money, we will send them something in return. If they don't include a return address, we'll track their DNA off the envelope and make sure they get something of value in exchange for their donation. We are quite relentless in this.

Dear *2600:*

Perusing your site, I saw some allusion to funds being in short supply. Follow this email back (if you receive it at all, which is doubtful). Y'all being in New York isn't particularly helpful but, perhaps, y'all got some folks in SoCal. If so, should one have the time, or inclination, to visit me at [redacted] (phone number is worthless, all eight are hacked, along with five computers... sender's name is mine), I'd bet dollars to doughnuts you could get real flush by having

a look at this computer. Add to that the other four and I'd guess y'all could have funding into the '20s. Hawaiian vacations, catered lunches notwithstanding. A government that robs Peter to pay Paul can always depend on the support of Paul.

Bruce

This is the kind of offer we really should accept every now and then, just to make life more interesting.

Dear *2600:*

Having read the Barret D. Brown saga complaining about payments and such, I want to say this on my Hacker Perspective submission I sent in recently. Honestly, as cool as being paid for a writing would be, I don't give a shit about the money. I've spent the last two months of my life not working for a business, but getting by on personal work and part time labor.

Living below my prior fiscal means has taught me many things in this short time. Number one is how valuable personal time is, and how much more productive you can be when not letting an alarm clock and schedule dictate your day. I read tons of current events in an effort to protect myself from the U.S. data regime (government) and share this data with friends and family, not yet fully keen to the truth of television's lies. Slowly, it seems more people are awakening to the lie.

Ramble coming to an end, if you decide to print my "Hacker Perspective" article, that would be reward enough. I want more people to overcome the trope of Hacker being a bad thing. Maybe more people on Earth will be motivated to do more and seek a more viable day-to-day existence, where extorting others for personal gain is absolutely at the bottom of their objective lists (as in to not exploit others at all).

Pic0o

We intend to always fulfill our promises, so if your submission to "The Hacker Perspective" is accepted, you'll get $500, like it or not. But your sentiments are exactly in the right place, as that shouldn't be the primary motivating factor, just as whatever meager rewards we can offer for regular articles shouldn't be. Suffice to say, we'll always do the best we can on that front. 2014, in particular, was a real challenge but, unlike certain corporate conglomerates who ripped us off, we feel we came through it all with integrity and without turning our problems into someone else's. And we would never have been able to do that without the support of our readers.

Dear *2600:*

I'm currently incarcerated at FCC Yazoo City Low. We have had MP3 players for just over a year. When I was out, I used to do my fair share of firmware hacking on a MobiBLU 2GB Cube and some video MP4 watches that used the Sigmatel chipset. I could change menus displayed, features, etc. with the correct "factory" firmware editor. We have Sandisk Sansa Clip + 8GB MP3 players with a custom "clear" backing and clip. They have a custom firmware for inmate use. If anyone would like to do an article on one, I'd gladly send you a working used one if you would take apart the firmware and detail how it works. The players cost us $69.20 and are sold by ATG Allied Technology Group. When sold to us, they are deactivated. We have to log into our Trulincs computer to activate it and sync it to our accounts. Once activated, they are good for 14 days until they expire. When turned on, they show the Sandisk boot up logo and then the inmate's name and register number. Then they show how many days remain. From there you can select music, radio, settings, and voice. The voice recorder is deactivated and shows the inmate name and register number as an audio file that cannot be played. Sadly, the mSDHC is disabled. From time to time, we do have access to "real" computers, although without Internet. ATG also offers a repair service where we can send them out and they come back to us as long as they are from ATG's address.

I'm pretty sure a simple firmware update on Sandisk's site would get everything back to normal, meaning I just need the update tool. I'm also curious as to how the flash is partitioned and what the root directories look like, as well as if the inmate info is in the firmware or on the root - I'm guessing both. Anyways, if anyone's interested, you'll get an MP3 player out of it, some random 128k encoded (yeah, I know) songs, and a fun little project.

Contact me if you have any questions. This is costing me out of pocket for the player and shipping, so if you could send a little my way, I have a BOP lockbox account - found online. If not, it's cool.

Solomon B. Kersey #87754-020
Federal Corrections Complex - Low
P.O. Box 5000
Yazoo City, MS 39194

Ideas

Dear *2600:*

I have a request/suggestion. It would be really nice if I could just get the quarterlies as PDF files. No messing with DRM readers. And a really nice way to distribute them would be creating an RSS feed to the PDF files, then giving each subscriber their personal RSS link that has a ?token=hash at the end, so if they stop their subscription, their token can simply be disabled.

I'd really appreciate it if you guys were able to do something like this! Thanks!

Loyal Kindle Subscriber
Blake

We are constantly working on alternative ways of publishing, but they all take time and coordination. We're currently focusing on getting all of the digests into PDF format as well as coordinating a number of other digital formats, plus dealing with all of the challenges of continuing to print on paper. We find that for every new thing we do, we get multiple suggestions on other new things. This is all good and we encourage more suggestions, and we hope people understand that we're doing our very best to make as many of them happen as possible. Five years ago, this was all a dream.

Dear *2600:*

I really want to order some back issues of *2600*, as I've recently rekindled my childhood obsession with the magazine. I was somewhat surprised to see that Bitcoin wasn't offered as a payment method. I

desperately want to order some issues from you. How can I pay using Bitcoin?

Evan

We used Bitcoin for HOPEX registration and it was quite successful. We are actively working on applying it to other items. As always, a simple idea is unnecessarily complex to implement and we're trying to get past the various barriers that make this difficult, such as inflexible interfaces that make the whole operation more clumsy than we're comfortable with. We're happy to listen to specific suggestions that don't involve our having to reconstruct our entire online store or other overly labor intensive activities. Stay tuned.

Dear *2600:*

I have seen that in the following location a buyer can get flash drives full with the conference videos: store.2600.com/hofldr.html

Since I wouldn't like to wait and I am in no need of extra flash drives, is there a chance you can upload these videos on a web repository where we could download them in (HD) mp4 format after paying?

Efthimis

It took us far longer to get you an answer than it would have taken for you to get the flash drive. Right now, this is the most efficient way for us to handle this. It took this long for technology to get to the point where we could fit an entire conference onto one or two flash drives that didn't wind up costing a fortune. And it took us quite a while to get them reencoded into this format at the request of those who no longer wanted to deal with DVDs, which also was a huge amount of work. Before we consider moving into yet another method of distributing this content, we need to finish launching this one, not only for HOPEX, but for all previous events. Plus, an extra 64 gig flash drive can be pretty handy.

Dear *2600:*

Ever thought of turning *Off The Hook* into a video podcast? I think it would be pretty dope and I know I can't be the only one. Just a thought.

A

Some things are best left to the imagination.

Dear *2600:*

I'd like to second Wolverine Bates' request for bound digests of back issues.

Tyler

Again, the more people who write in for this idea, the more attention we'll pay to it. So far, it isn't exactly a deluge of requests. But we remain open to the idea.

Rules of Publishing

Dear *2600:*

I don't know if your definition of "Payphones of the World" includes imaginary locations but, if so, here's my album of some prop phone booths the TV show *Gotham* has set up for filming on West 30th Street in Manhattan this morning. Http://imgur.com/a/hyuze One's an old Nynex!

R

Unfortunately, we can't print anything that is already online. Actually, that's not unfortunate as we don't want to ever be just a rehash of what's already out there. We're sharing the link in this case so that people can still see these unique shots. But to have future material immortalized on our pages and hence stored in the Library of Congress, various time capsules, and at least one potential private deep space mission, be sure to send it to us to publish first.

Dear *2600:*

I don't know if this is interesting for your readers. The following article says that German Telekom sells old phone booths. The article includes some nice photos of the area where they store their old phone booths.

Gunnar

While indeed interesting, this is even further from what we can print. An article from another publication clearly doesn't belong in our pages, let alone the pictures from that article. However, anyone is free to write up a piece on the subject if they believe it to be interesting enough for our readers. What makes that scenario even better is the fact that our writers can speak from a hacker perspective and thus make it all the more intriguing to our readers, a good number of whom wind up becoming future writers.

Dear *2600:*

In my travels around the world, whenever I see an interesting payphone, I snap a picture with an eye towards getting it included in *2600 Magazine*. Who should I submit these to? What is the best media? (CD ROM, DVD ROM, USB stick, Flash, etc.?) I would love to see one of my photos gracing your fine magazine.

Robert

You can submit it in any of the methods mentioned above, but email to payphones@2600.com is the most preferred, as you don't have to physically mail anything and it's also the fastest method. Just remember to attach your photos and use the highest quality settings since the standards of a printed photo are generally much higher than what gets shown on a website. Also - and this is important - please include as much information as possible about your submission, such as location, any details about phone features or functionality, or anything else that could possibly be of interest. We discard so many submissions that are just labeled "payphone" or something equally nondescript.

Article Comments

Dear *2600:*

Kudos to D.B. LeConte-Spink for the great article "Sabotage the System," which appeared in the 31:2 edition of the magazine. I wish I had written it. It put into words what I've been thinking for some time now. Attacking illegal mass surveillance from an economic perspective is simply brilliant. Drive up the cost of mass data collection and watch the system start to crumble. The best way to defend our privacy and keep Big Brother honest is to make wholesale data collection prohibitively expensive and too time consuming to be feasible. A great way to do this is to proxy our IP addresses and encrypt our data. Nothing will frustrate government snoopers like an IP

that doesn't tie back to a person and data that is fully encrypted. Imagine if even a fraction of all Internet users took these steps. The government would be collecting mountains of useless data and attempts to trace and decrypt it all would be futile. They would be forced to do the right thing and only target actual criminals and not everyone else. The hacker community should promote privacy tools at every opportunity. Tools like Tor, the Whonix Gateway/OS, VPNs, Silent Circle, Tails, and a host of others make privacy and encryption easier than ever before. I firmly believe that good encryption on a large scale can help restore the balance of power between corporations and the government on the one hand and the average citizen on the other.

Encrypt Everything!

Jim L

This is almost certainly the way to go. Among our challenges are those of us who believe they have nothing to hide and that convenience trumps privacy. It doesn't have to be a choice. If you really want to advertise your whereabouts or share minute details of your life with complete strangers, you can still do that. But by default, anything between you and the site you are communicating with would be unobtainable by others. Those companies who insist they need to share your personal info with outside entities or who demand access to unrelated content of yours in order to serve you better need to be challenged and overridden. But probably our biggest challenge is that of unity. We need for the best minds in our community to work together and support the many projects that have the same goal. There will always be disagreements on style and function, but what's truly important is that we're moving forward to a place we all want to get to. And all of this becomes little more than the toys of an elitist group if we're unable to make it understandable to the general public. Our work is indeed cut out for us.

Dear *2600:*

I was fascinated to learn, from lg0p89's spam article in 31:3 that both Europe and Asia are not, in fact, in the Northern Hemisphere! This means I've had my globe upside down all this time. (Someone better email the Google Maps folks as well.)

Brain the Fist
(sent from my Canadian igloo
near the South Pole)

Yes, clearly that word should have been "Western." We apologize for any confusion, inconvenience, or laughter this may have caused.

Dear *2600:*

2600 has been my favorite magazine (along with some comics magazines, but definitely my favorite scientific/philosophical one) for 11 plus years, since having visited 2600.com in the mid 1990s. Thanks for publishing my first article, "The Demoscene," in 31:3! I must apologize for a mistake and point out something in the editing (and, at the time of this letter, your website's code archive) that could confuse people. I had based my article on my even longer, unpublished, final academic research paper, but had shortened it when noting article sizes and, in doing so, I omitted some cited code, which caused another code section to be mis-cited.

The Pascal subroutine was not by Denthor, but HELiX, and is bump-mapping, not just texture-mapping. The two sentences starting from the one with citation 11, should have said "Jim Blinn discovered bump-mapping, which simulates bumps and pits on 3D surfaces[5, pp 27]. A display hack/intro by HELiX gives the following Pascal bump mapping code[11].", and the source is "[11] HELiX. (1997). 2d bump mapping. Available FTP: ftp.scene.org. Directory: /mirrors/hornet/code/effects/bump. File: bumpsrc.zip" Also, a comment section in HELiX's code was edited from large code text to smaller article text, but the code is really one piece, including from (originally) "{Those two lines are the heart of bumping}" and past "col:=abs(vlx-nx);." If you want the barely explained (missing) code by Denthor on texture-mapping, here it is:

```
textureX = 0;
textureY = 64;
textureEndX = 64;
textureEndY = 0;
dx := (TextureEndX-TextureX)/
(maxx-minx);
dy := (TextureEndY-TextureY)/
(maxx-minx);
for loop1 := minx to maxx do BEGIN
PutPixel (loop1, ypos, texture
[textureX, textureY], VGA);
textureX = textureX + dx;
textureY = textureY + dy;
END;
```

I plan to upload my original paper and a corrected article to my homepage (http://www.cwu.edu/~melikd, which also has more display hack code, a list by Rod of demo secret parts, links to my traditional and digital art, and demostyle electronic music, etc.) in time for 31:4., and I hope to write more articles, not on networks or their security (not my academic areas). I think there are a few other interesting things to write about.

David
darwin@sdf.org

Thanks for the correction. We've also updated our code section at www.2600.com/code.

Dear *2600:*

This is in response to "Checkmate or How I Bypassed Your Security System" by DreamsForMortar from 31:3. What you discovered is certainly a weakness in the physical barrier, but likely not in the security system itself. In fact, you would probably be better off just smashing that glass door, as it would less likely alert someone to your unauthorized entry (unless there's also a glass-break sensor in the area). Allow me to explain: those small "motion sensors" above the inside of each door, which you suggested using a warm glove on, are called "REX," short for "Request to Exit," sensors. When you approach those on your way out, they will "detect" you, click slightly, and typically release the maglock, or the electric strike, so that you can walk right out of the corresponding door. But what they also do, at the same

time, is "shunt" the door contact for that particular door. Each door normally has a small "contact" in the form of a tiny magnet in the door and a wired sensor in the frame (for wooden doors) or a built-in release sensor for maglocks. The entire purpose of this sensor is to detect whether the door is opened or closed at any given time. By forcing the push-bar with a sting, you have caused the maglock power to shut off, releasing it as per fire code, but without triggering the REX sensor and shunting the built-in door contact first. As a result, the door opened, but the contact, not being shunted by the REX, likely generated a "door forced" alarm in the access control system, which probably relayed the signal to the alarm/theft prevention module and alerted either your local security company or law enforcement organization. Now, if by the time you're reading this letter, nobody came to have a serious talk with you about what you did, there is most certainly an issue with either the way the door contacts are implemented, how the alerts are monitored, or what level of coverage the video surveillance system has around that door. But the point I wanted to make is: breaking in is easy, but doing it without tripping the alarm is a whole other story. If you found a way to do that in your scenario, I would love to read a Part Two in the next edition!

Alex W

Dear *2600*:

Re: "Sabotage the System" in 31:2, LeConte-Spink wrote some very profound things that I found to be inspiring, such as "We must sabotage the system. But how?" and "Break the efficiency of automation." To me, the two parts when put together inspire a solution. The NSA's illegitimate metadata stealing operation is efficient because of its algorithmic automation. If sabotage by frustrating its algorithmic automation can prove that systems' operational integrity is based solely on conditions of data, then that algorithm would be the NSA's Achilles heel. I'm a former network security analyst in prison for botnets. You see, if my understanding is correct, the NSA's vast amount of stolen data is passed through a filtering algorithm which sifts through the data, looking for certain key words and phrases ("trigger words"). Then, the suspicious content is tagged and flagged into another database and categorized by a designated priority list consisting of various levels of offensive criteria and then passed to a ticket system for a live analyst to approve or discard the validity of the suspicious content. For an "omniscient" surveillance machine whose only foundation is dependent on algorithms, I wonder how it would stand up against an onslaught of spam bots blasting trigger phrases into Google's search engine. The amount of false positives would be staggering. In a world where good old-fashioned police work is an "arcane inconvenience," I believe that breaking the efficiency of automation is the answer to how you can sabotage the system by exploiting its algorithm to demonstrate its vulnerability to false positives. How many people are in prison based on such a limited system? Though implementing this is obviously illegal and I don't encourage it as opposed to the legality of a warrantless spy machine which the majority rightly feels threatened by. I hardly can contest the issues of legality here, since this government appears to be a rogue personification of anarchy itself.

Ghost Exodus

More Observations

Dear *2600*:

Some time ago, I had the opportunity to speak with the folks in Verizon's Legal Compliance Center; their number is 888-483-2600.

Though you might find that amusing.

Steve

We're more amused at the name of their office. It's good to see them trying something new.

Dear *2600*:

I know about an automatic-USB app that opens up Mac's passwords.... 2600 ROCK ON.... msg me.

Jeffrey

a few seconds ago - Like

Yeah, this is the sort of thing we're talking about. We don't even know how this wound up in email format since it's the kind of thing that shows up on a website for about a second before it's completely forgotten forever. Instead of getting the coherent observations that our readers are known for, we're increasing getting every trivial thought that pops into someone's head that may or may not be even remotely relevant to what we're about. We wind up spending more time and thought going through these things than the people who sent them ever did. We're hardly the only ones affected by this trend, but it's rather dramatic when compared to what we're used to.

Dear *2600*:

My 13-year-old got us free Wi-Fi and I'm very proud. Here is how he did it. You download TMAC v.6 Technitium Mac address changer. We don't have a Mac. I have Windows 7 and my kid has Windows 8. So you make sure that you delete history and restart your browser (we have Google) as well as reset your IP. Then you just click to your neighbor's Xfinity hotspot (suckers!) and start it up. You are directed to an Xfinity sign-in page, click "sign up," then you are directed to a sign up page which has a dropdown with $2.99 selected. Click the dropdown and select $0.00, put in a bogus (five digit) zip code, a bogus email, then the button. You should have one hour free, but when that goes out, you open your TMAC v.7 and "change address." Now your Xfinity thinks you have never been there before, and you just sign up for another free hour! I tried this hack with my old Windows Vista and it didn't work for some reason. Xfinity recognizes that I've already used the free hour. This Xfinity free hour is only available until February 2015, so I thought I should get the word out. Thanks.

sueicloud

So you know, a MAC address has absolutely nothing to do with a Mac (Macintosh) device. MAC stands for Media Access Control and is supposed to be a unique identifier for network interfaces. This method seems like a bit of a hassle if you want access that lasts longer than an hour and beyond February. We can only hope and assume that free Wi-Fi will become easier to access with less hoops to jump through.

Dear *2600*:

this classic video sums up technology's relation to man circa 1991: https://www.youtube.com/watch?v=d5drsL13ai4

Dusty

Sigh. We have no idea what you were trying to tell us. Perhaps if we had responded within the few minutes that this link worked, we might have gotten something out of it. But we would have forgotten all about it by now, which you no doubt have already. We're starting to suspect that there are a number of people out there who don't even know we're a magazine, don't understand what the letters@2600.com address is actually for, and perhaps aren't aware of printed publications and how they work.

Dear *2600*:

Loving the magazine and my subscription, enjoy looking forward to reading the articles. However, a slight annoyance has arisen with the last three issues. They have all arrived with the envelopes opened. No attempt to reseal has been made. Is this something that is likely to happen to your envelopes on an international delivery (to the U.K.) or is it once again the idiots at my local mail office playing silly buggers? It wouldn't be the first time I've had to make a complaint. They seem to excel at siphoning out birthday cards and DVD shaped packages to keep for themselves. Also, I'm not missing anything as a result of this fiddling with the mail, am I?

Sorry, the paranoia is a little high today, but it is annoying since it keeps happening.

K

We'll go with the "silly buggers" theory for now. All of our envelopes are sealed when they're sent off. It should be possible to tell the difference between an envelope that was never sealed and one that was sealed and then opened. For one thing, it's unlikely you'd be able to seal it again in the latter case. Since this seems to be a recurring problem, presumably with your local post office, perhaps you should go above their heads and file a complaint. You will certainly make enemies by doing this, but then you'll have even more to write about. And as long as you send your next letter via email, we'll likely receive it. If, however, the opening is taking place higher up the chain, perhaps your local post office can actually help you figure it out.

Dear *2600*:

I love the radio show and magazine!

I clean pools for a living and am currently residing in an old farmhouse with leaky ceilings, no Internet/data coverage, and limited phone services. My companions are a few roommates, two dogs, several chickens, peacocks, and cane spiders as big as the palm of your hand. I'm about as low tech as it gets, but slowly over the years I've been collecting various bits of electrical equipment and reading publications like *2600*, *Make*, and *Robot*. I've ordered different kits from Adafruit and taught myself how to solder, code, and use various tools from videos on YouTube and around the web (I spend a lot of time in cafes).

Over the last few months, I started piecing together a new product idea using a Raspberry Pi, which (after a lot of duds) has started giving me some promising results. In a few months, I'll be making a move to Florida to attend UCF and (hopefully) earn an engineering degree. My point is anyone who has an interest in electronics, wearables, fabrication, or who just wants to understand the world around them a little more can start from anywhere, any age, any educational background. My advice? Take it from a pool guy: Grab up a few DIY magazines, pick a project that looks fun! And try it. You might just change your life.

Aloha from Maui
John

We believe you may have changed a few just with these words.

Dear *2600*:

I had stopped by at your booth/table/van at the World Maker Faire this past September with my younger brother (to pick up some back issues, subscribe, etc.). My parents, not realizing that he was with me, contacted the faire's security. I just thought that it was interesting that he was with *2600* while security was trying to find him.

By the way, I love the way that *2600* is packaged. Nice nondescript envelope. Thank you.

ibid 11962

We're good at eluding security even without realizing it.

Dear *2600*:

Please forward as appropriate - if there is a "contact us" link on your website, it escaped me.

I just glanced at my 2014 *2600* Hacker Calendar, and the November 14th entry states that on this date in 2007, the last DC grid in the U.S. was shut down in New York by Con Edison.

According to the IEEE, Pacific Gas and Electric shut down their last DC grid in San Francisco as late as late 2012.

IEEE Spectrum in general is highly recommended reading for anyone with even a passing interest in the workings of electrical and communications networks.

Vennlig hilsen,
Odd Erling N. Eriksen

There does seem to be some contention here. It doesn't help that this is referred to as a "secret grid" which makes it a bit harder to verify, but which would also explain why it wasn't known about while still in operation. We will look into this and make any needed corrections for 2016 and beyond.

Dear *2600*:

Enclosed are some ads from the May/June 2014 issue of *WoodenBoat Magazine*. Specifically, pages 113, 117, 118 from issue #238 in 2014. 113+117+118+238+2014=2600. Yeah, I know that there's nothing hacker related on page 117, but otherwise it only added up to 2483!

P.S. You guys have some really nice boats!

Swamp

We're impressed at the numerology skills at work here, even if the answer is a bit of a reach. If you include page 117, then you also have to include page

114 (the opposite side of page 113), which brings the total up to 2714, which is as meaningless to us as 2483. The ads are for Hacker-Craft (www.hacker-boat.com), which dates back to 1908 and one John L. Hacker.

Dear *2600*:

As a specialist in philosophy of computing, I have developed three statements defining the essence of computer literacy. When someone says that they do not understand computers, these three statements will clear that misunderstanding up right away.

Computer Literacy:

1. The computer was, and is not, and is about to come.

2. The computer comes in programs of assignment and programs of transfer of control.

3. The wonder of the computer is among the program of that computer.

I thought your readers might appreciate these statements, something to fall back upon when pressed for "what is computer literacy?" It can be said now.

Yes.

John

It must be effective because we can't think of a single thing to add.

Dear *2600*:

If this letter makes it to you, check the postage meter strip on the envelope. We just might be able to save people gazillions of dollars! Get Peace in Our Time! End Poverty!

In the latest round of U.S. Postal Service rate hikes, they boosted the price of the basic one ounce envelope stamp to 49 cents. This time around, though, they set up a slightly lower rate for all those postage meter imprints that businesses use, namely 48 cents. So I got to thinking (yes, I know, watch out...).

The Automated Postal Kiosks (APKs) in the USPS lobbies will let you print out "stamps" in whatever value you want. For example, I use them to make 21 cent strips for use on heavier envelopes. (That's the price for the second and third ounce. Not sure how high up the chart it goes nowadays). I also use them for media mail.

So I just printed up some 48 cent sheets, and am using one of them to send this letter to you. Let's see if it works.

D

It did indeed work, but we believe you may have unintentionally played by the rules after all. If, indeed, there is supposed to be a slightly lower price for "postage meter imprints that businesses use" and you used the equivalent of a postage meter imprint from the post office (which is a huge business), then that is precisely what the system is designed to do. The idea seems to be mostly geared towards businesses that will send many more letters now that they're paying less, but the same logic can be applied to individuals doing this en masse. We're not sure how many people will flock to these automated kiosks to save a penny, but we're pleased to help convey this message.

Dear *2600*:

In this letter, I will detail a new way of programming artificial intelligence that not only will make it possible to "teach" a computer, but to have a computer teach itself.

First, I started with the question, how do humans learn? Well, look at a baby. When a baby is born, it only knows how to do certain things. Let's call these things "base functions." These base functions are broken down into electrical signals, the human equivalent of code. We learn new things by performing a set combination, or algorithm, of these base functions. Let's call these "compound functions."

I believe, in this way, we can teach a machine. If you made every code command into a line of English, with a set and limited syntax, then they would function as the base functions, and the base ontology of the machine.

You could then use a command line interpreter to parse base functions into code. What happens when you plug a compound function into this hypothetical interpreter? It would check your command against an XML file that stored all the learned "compound functions." If it found the function, it would parse the line into base functions, and then those base functions into code. If the function is not recognized, however, then it will enter a program asking you to enter a list of functions to perform the desired task, essentially having you pseudo-program the computer, but with English. What happens if you plug in a compound function at this time? You go through the same recognition process detailed before. When you were all finished describing commands, you would enter a keyword and then you would run the new function, which would be stored in the previously mentioned XML file.

I said in the beginning that the computer could also program itself. This is the easier part, once you have the code worked out for the first bit. All you have to do is have the computer try random combinations of the functions it knows, and bam! Sooner or later, every now and again, it has a new, useful function.

I hope someone beside me pursues this project. I think it's not only educational, but fun!

joshua

Dear *2600*:

The world of today is an interesting one. In the last five to ten years, technology has thrown itself forward into a sky of ever expanding possibilities. Allowing people to take a small, but very high-powered computer in their pockets, socialization no longer requires real life contact. Instead, we now bring our attention to a web of constant social stimuli fulfilling our needs.

Yet, as I write this, I feel like there is an art that I am desperate to master, yet social convictions defy me from attempting. I'm fairly sure I do not need to name this art, so instead I shall get straight to the point. Hacking is a formidable act and, to me, an interesting subject. The idea of opening an object, bending the rules of the creator, and telling that object to defy its rules and follow your way astounds me! When I first found this magazine, I was quite honestly perplexed; never had I thought of hacking in such a way. These concepts were an opening to a curious mind.

Needless to say, to actually launch myself onto this platform is a challenge (one I have not mastered myself). In fact, to even open a CMD window on a school desktop is to immediately be categorized as a hacker. It is quite embarrassing to have an entire Year 8 class ask to be taught how to hack. My generation in particular seem to have been taught the definition of hacking from short statements sprouted from those who lament of their social networking account being "hacked" (when, in fact, their bad sense of password security led them into this hole) or hearing of the "heroic" conquests of a certain "hacktivist" (a term I despise with a passion) group fighting for the small people. When simply put, I want nothing to do with that! Yet, opinions are useless and I've heard many a time that "teenagers are terrible people!" and I agree! We are terrible people! We should be separated from this planet and kept there until we realize how stupid we are!

But alas, I'm not here to shame my generation, since we're all in this together. I suppose I should make a point now, despite that most of the readers of this magazine are thinking that I am just being lazy and blaming all of my issues on those who antagonize me. I don't disagree. I am lazy, I am paranoid, I am stupid at times, but I feel as if even though no one cares, I need to relate this tale! Hacking is not the same as you remember it. The articles I see here are for those who many years ago simply found that punching in a certain number directed you to a test line. Instead now, this curiosity is sparked by hearing of gaining access to secret documents and bank accounts. I do realize that criminals have always existed, however, I like to think that at least their curiosity started off with no wrongdoing in mind. (I may be wrong, so feel free to kill me for that.) But every time I make an attempt, I am thrown back by social constructions and daft IT departments afraid of all those who attempt to break their nicely laid systems (which really are just a bunch of VB scripts and some firewall programs).

If you ever see this on a page or screen, I hope you stuck through my ramblings and heard a semi-cohesive message. I know it is different from the usual, but I felt like my arrogant mind needed to be appeased and I felt as if I conveyed some sort of message to the people. Then again, I suspect I will grow up and realize the error of my ways. Until then, I have another hurdle to accomplish and another social boundary to crash into.

Vel Co

The important thing is that you're attempting to think all of this through and not blindly buying into anyone's philosophy or definitions. We're confident enough in our values and beliefs that we're certain anyone who approaches our world with a fair and open mind will eventually at least acknowledge the value of what we stand for even if they don't reach the same conclusions. We wish you well on your voyage.

Controversies

Dear *2600:*

I don't know if you have been following the Gamergate controversy, but there have been numerous allegations on both sides of hacking attacks, DDOSing, etc. Hackers tend to brag about these things. Have there been any rumors in the community about someone taking responsibility for the attacks on either side?

David T.

There are more rumors than we could possibly fit into this issue. But there's nothing unusual about that. Who attacked whom, what comments were made when... it's largely irrelevant to the bigger discussion. Gamergate is something we believe people should read up on, as it's quite telling of much of the issues and problems that plague the online world. The particulars here concern video game culture, which is peripherally connected to the hacker scene. We're not going to get into the specifics as we don't have much in the way of firsthand knowledge. But we don't need that to be able to see that there are serious issues in that community that need to be dealt with, regardless of the facts of this particular incident. And we do recognize a lot of the disturbing symptoms as existing in our own culture, perhaps not as bad as it once was, but still worse than it should ever have to be. We've seen numerous instances of sexism and racism in the hacker world since our very beginnings. And we've always tried our best to confront them and defeat them. Our community has grown tremendously over the years, not just in numbers but in maturity and thoughtfulness. We like to think this is the result of confrontation. Too often, unless a problem is exploding all around us, our tendency is to avoid even acknowledging it as an issue. It's the easy way out, but it's also a total cop-out. There is absolutely nothing wrong with expressing your anger and frustration at a system that is unfair to you or to anyone else because of race, religion, sex, preference, etc. It makes no difference if most people don't agree - how many times in history have "most people" been completely ignorant? As hackers, we're used to confronting obstacles and challenging the status quo. That's why it's particularly inspirational when we see progress within our community - and especially sad when we see elements moving in the wrong direction. These are problems we all have to take an ongoing interest in if they're to be conquered. In truth, we will probably never consider the battle to be completely won, but we also won't shy away from acknowledging the positive. As an example, back in 2000, H2K became the first major American hacker conference to inject activism-leaning content into its program. What we've seen since at subsequent HOPE conferences, and throughout the community in general, is more awareness, concern, and, ultimately, more power from our united interests. It was a natural progression, not forced upon anyone, and it's made a huge difference in helping to define who we are.

We're proud of the entire community for the growth we've seen. But we believe there's a lot more growing that still needs to come. To bring this back to Gamergate, there are still huge challenges ahead for so many online communities and when something like this comes up, it needs to be seen as an opportunity

to confront them head on, educate those who remain unaware, and make a better place for us all. Perhaps the offline world may even learn from this.

Dear *2600*:

My boyfriend is a lifelong fan of *2600* and *Off The Wall* and is facing a felony network hacking charge with time in prison after a mere Wi-Fi prank within a computer club.

Not mentioned in the enclosed press release is the long list of unscrupulous and illegal actions by the Department of Justice, including when the prosecutor called me personally and tried to convince me to entrap my own boyfriend by filing a false request for a protective order and then hoping that he'd violate it. That's why I'm on the warpath to save him.

Please help.

Jessica

What we've been able to read about this case seems unbelievable. The site listed in the press release you sent us (SaveaNerd.net) has been taken offline "per recommendation from counsel," which is what lawyers generally tend to do. However, there is an active petition up at change.org (search for "hacker dojo" which is the name of the organization at the heart of this whole thing). We will reserve judgment until we hear more facts from more people, but this is something that should definitely be looked into by everyone, as it's not at all the chain of events one would expect in a hackerspace environment. As for the actions of the prosecutor, if only we could say we were surprised. But one does have to wonder why there is such an interest in prosecuting someone for something so minor.

Dear *2600*:

Happened upon an article regarding Pirate Bay's founder and the "Hollywood manhunt." I'll let the staff of *2600* decide if this is of any importance to your readership. Personally, I have not accessed Pirate Bay much at all. I like its premise and its "mission." The situation regarding Pirate Bay's founders may be something to take under serious consideration. One has to wonder who manipulates the MPAA bringing about this legal action? What should the *2600* community take from this?

Love your pub.

Joethechemist

Thanks for the pointer. The story of the MPAA managing to get an Interpol arrest warrant issued for the Swedish founder of this organization is truly sobering. We would like for someone closer to this to give us some insight into what's really going on. The power of Hollywood can indeed be frightening, as we learned a while back. We could fill our pages with similar stories.

Speech

Dear *2600*:

Please send me the blacklist of Google. I need to ban it from comments on my website.

Thanks, guys.

Paschal

First off, we haven't updated any of that in years. We only put it together to show how Google chooses not to auto-complete certain words. It quickly got out of hand, but you can see how far we got at www.2600.com/googleblacklist/. Second, we're not entirely sure what your intentions are. You're going to ban the same words on your website? We don't recommend that as there are a lot of good words there. Plus, banning words simply leads to different words being used for the same thing. It doesn't really solve the problem, whatever you define that to be. If you're having trouble with the intelligence level of website comments (hardly a rarity), there's nothing wrong with moderation if a free-for-all isn't what you want.

Thanks

Dear *2600*:

Thank you for over 30 years of giving hope (in the original sense) to so many creative, yet often alienated, people! And thank you for HOPEX!

By the way, these are from Silver Lake Farm in "The Garden State." Support your local farmer!

Anonymous

This was actually a note that was left for us at HOPEX along with a beautiful plant that we regretfully didn't water and it died within a week. But it's the thought that counts.

Help Needed

Dear *2600*:

I am currently incarcerated and am looking to hire someone to set up a source code system. I am looking to be able to send mass text messages. I read your publication, but I am in no way a hacker or understand much of what I read.

Please refer me to someone who I can hire to set this up for me. Or where I can find them and what it is called.

John

We don't give referrals or act as go-betweens. As a subscriber, you're entitled to a free Marketplace ad and you can probably find someone to help you there. But, seriously, mass text messages? Nobody is ever happy to get those.

Injustices

Dear *2600*:

When is a punishment enough? After the experiences of the last three years, it's difficult to rationalize the reasons why I should continue.

I didn't complain when I was arrested for hacking a local ILEC and received my punishment. For a hacker understands the time old saying "if you can't do the time, don't do the crime." Understanding that prison isn't an environment built for this 120 pound, geeky, pasty white kid with Asperger's, I admit that I struggled to logically integrate the upcoming punishment by burying myself into research to better understand what would occur. I was incorrect.

For I've endured: inmate peers stealing everything I own twice, being beaten down and scammed for every cent in my account, learning the bloody wrath of leukemia and her effects, and my own family turning away from me all because of my hacking behaviors. Nonetheless, I still didn't complain. For

I look upon my situation and use my abilities as a hacker to adapt.

However, my skills only could take me to a point. Not just six weeks after receiving a cancer remission diagnosis, I was violently attacked and raped. Crushed pelvis, broken ribs, traumatic brain injury, and other various injuries too painful to even... left for dead, not found until three hours later. After waking up from a week-long coma, I thought that I had right on my side. I was incorrect.

It's been almost two years since the attack, and today the emotional and physical pain is ever present in all realities. I'm lost for words: it's been recently explained to me that because of statewide budget cuts, this individual who attacked and raped me, infected me with HIV, and whom I see every time I close my eyes is going to get away with no criminal charges against him. All to save the taxpayers money. He was already under a 25-to-life sentence - it's cheaper to do it administratively than through our courts.

As I consider the rationalization of my fate, whom or what should I blame? Entropy? No. Hacking? Bloody hell, no. Myself? I don't really know. The individual? Maybe. There isn't one item I can point out as the one cause of my experiences other than the law of unintended consequences. For I miss the touch of my well-worn keyboard on days like today, because the weight of my pain alone is forcing me to self-harm, like the autistic child I once was before I met hacking. Now I complain. I was incorrect.

When is a punishment enough?

Preston Vandeburgh
Larkgeco

From what you've told us, this is way more than enough. In fact, not even the most despicable criminal should endure these kinds of conditions within anything resembling a civilized society. It seems that many of us have become numb to anything that happens behind bars, justifying it by telling ourselves that those who find themselves there deserve whatever happens to them. We feel that cold attitude is where much of the blame lies for the horrible events outlined above. But in many ways, it's those people on the outside who are also victims, as they have lost something that will be next to impossible to replace.

Nonviolent offenders - if they have to be imprisoned at all - should never be placed in an environment with violent people. Period. And if something violent does happen to them, it's the state that should be held accountable, as they are the ones who set up the unfortunate events in the first place. In that respect, they have already done far worse to you than anything you ever did to them or anyone else. We know these words won't help your situation, nor are we in a position to commit to doing anything beyond getting the word out in these pages, but if there's any comfort in knowing that there are people who will read this and who will care, then maybe that's a start. If nothing else, perhaps this can be shown to people who actually believe there's no harm in sending someone away to teach them a lesson or to send a message. If that can help keep one more person from being subjected to this kind of barbaric treatment, you will have given back far more than you ever could have taken.

Dear *2600*:

I am writing in regard to a violation of my First Amendment rights. I ask for your assistance in protecting these rights. I am a federal inmate.

On July 24, 2014, a book entitled *The Basics of Hacking and Penetration Testing* was stopped from being delivered to me. Not only was the book rejected and returned, but I was also given an incident report for "Introduction of a Non-Hazardous Tool (Attempted)." The justification for rejecting the book and writing me up is that "[t]he security of the institution's computer system is at risk when inmates have access to resources like the book mentioned above."

My intentions for ordering the book are twofold: First, I plan to open a school that will cater to military veterans and ex-convicts. The school is going to have a cyber-security curriculum. In preparation of taking the school live upon my release, I wish to develop as much knowledge and curriculum in advance as possible. I selected this book precisely because it was written by a college professor, and it is currently being used to teach cyber-security students at Northwestern University. My second reason for ordering the book is that I plan on starting my own cyber-security firm. I believe the book would aid in my goal of rehabilitation in that it will equip me to work in the computer security field when I am released. In short, I need the book precisely for purposes of rehabilitation.

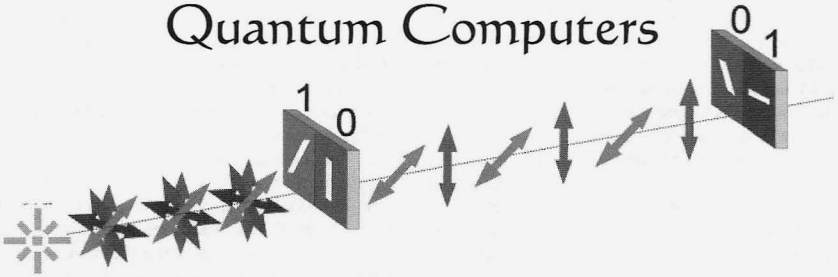
I submit that the freedom of speech that is protected by the First Amendment is not just freedom to speak, but also the freedom to read. The Courts would agree. In King v. Federal Bureau of Prisons and Charles Gilkey, 415 F.3d 634, 2005, the Court stated, "Forbid a person to read and you shut him out of the marketplace of ideas and opinions that it is the purpose of the free-speech clause to protect."

Please, help me to take the steps needed to gain the skills that will enable me to be a productive member of society and protect the rights of all inmates. Specifically, I ask that you aid in informing the community of my situation. In addition, any legal help you may offer would be greatly appreciated.

Justin L. Marino

We get so many letters like this and it's indeed distressing to see such unfair and ultimately self-defeating restrictions imposed upon people, especially those who need something new and inspirational to focus upon. We'll do what we can to help get the word out by printing such letters whenever possible. We need to again point out that this is pretty much our limitation as we are not legal experts. Over the years, we have received an immense amount of legal papers, documents, and correspondence from people in prison who think we have a lot more power and time than we do. It's unfortunate, but this is most always a wasted effort. We encourage those in the legal community and prisoner rights advocates to regularly look at our letters and Marketplace ads in order to take additional steps when possible. The goal is to stop these injustices from being the norm and, for that, we'll need significantly more people to take an interest.

Crypto Systems Which Resist Quantum Computers



by Dave D' Rave

Previously, I described how trends in quantum computer technology are likely to result in the total loss of security for mainstream crypto systems such as AES and DES. In this article, we will look at crypto methods which are resistant to known algorithms used in quantum computers.

One-Time Pad

One-time pad encryption appears to be completely secure against quantum computers. Unfortunately, this system suffers from extreme key distribution problems.

Quantum Cryptography

Quantum cryptography is a term for various technologies which use entangled photons to send information such that it detects any eavesdroppers in real time. Such systems are highly resistant to attack by quantum computers, as long as proper operating procedures are followed. Encrypted fiber optic systems which use quantum cryptography are currently being sold commercially. These are semi-practical, in that they require a dedicated fiber optic cable between the two endpoints, and in that they cannot be used for encryption of stored data. It is possible that future variants on the idea of quantum cryptography will allow information to be sent over a public network, or that a long-term stable method of storing Bell-state qubits will be developed.

The other problem with quantum crypto is, well, hackers. For details, just go onto YouTube and do a search for "Vadim Makarov" or just go here: `www.vad1.com/lab/`. As my redneck friends used to say, "If one monkey can build it, another monkey can break it."

Exploiting Weakness in the Quantum Algorithms

Many of the proposed algorithms for breaking crypto systems use either a quantum Fourier transform or some kind of amplitude amplification algorithm. The weakness in both cases is that these algorithms work a lot better if there is one and only one right answer.

Consider the case where we are using Grover's algorithm to perform a known plaintext attack on a given cryptogram. The general situation is that the system starts with a state vector in the solution space. We measure the error between the trial vector and the target vector, and produce a new state vector (named state vector 1). Then, repeat using the new state vector. Typically, each iteration produces a vector which is closer to the solution, and a relatively small number of iterations will provide the answer. (Yes, I am leaving a lot of stuff out. This is not a review article.)

Now consider a crypto system such that the cyphertext can be decoded using any of four different keys. When the quantum computer attempts to find the current error vector, it will get a superposition of four vectors. Depending on the details of how the algorithm works, this will either collapse to one of the four values, or will collapse to some weighted average value, or will produce some superposition of answers. Each iteration of the error-and-update cycle will typically move the vector in a random direction, and the algorithm will never converge to a solution.

Multiple-valid-key coding systems have a similar effect on quantum Fourier transform algorithms. When using such a system to break DES, the expected code space contains one valid decryption and (2**56 -1) invalid decryptions. These have been scrambled in digital phase space using some transform. The quantum

computer is going to perform an inverse transform on the superposition of all 2**56 possible decryptions, and then use Fourier transform methods to identify the one we want.

This method works on DES, because DES only supports one correct decryption key. If we use some alternative algorithm which allows a large number of equally valid decryption keys, then the Fourier transform will produce an output which is some kind of superposition of the valid keys' descriptions. If the number of valid keys is large enough, this output will be unintelligible.

Multiple Valid Key Code Systems

Multi-key crypto systems have the characteristic that a given cyphertext can be decoded into the correct plaintext by using any one of a number of keys. For example, we could have a system which uses 512 bit blocks of data, and a 1024-bit key, such that 2**512 of the possible keys are valid.

For a conventional computer using a brute-force attack, this would be equivalent to a key size of 512, since attempting 2**511 keys would give a 50 percent chance of guessing the plaintext. For a Quantum computer, having this many correct results in the code space would restrict the number and type of algorithms which could be used.

Multiple valid key systems can be implemented by using RSA-type algorithms such that, instead of using two large prime numbers, you would use n (where n is something like 16) large prime numbers. If the decryption problem requires that a given large number be factored, it would only require that one of the factors be known.

Another class of multiple valid key systems involves the use of error-correcting codes, such that a key which produces a decode which is close to the plaintext will work, after the error correction operation has been applied. (Note that modern block cipher systems, such as AES and DES, have excellent entropy properties. There will be no general way to find the other members of the key set, given one of the valid keys.)

Another way to produce a multiple valid key situation is to use two encoding methods in sequence, discussed below.

Multiple Use Pad Systems

The one-time pad crypto system consists of a very long key, which is used only once. The modern procedure for encryption is for the sender to exclusive-or the key with the message. To decrypt the message, the receiver will exclusive-or the key with the cyphertext.

The one-time pad is well-known as being unbreakable by any crypto system, as long as you have a reliable, secure, high-capacity key distribution system. Wikipedia has a very good article on the subject. At the same time, using a one-time pad more than once produces very, very weak crypto. This is because the exclusive-or of two plaintext messages contains a lot of redundancy which is easily exploited by cryptanalysis.

Also, multiple-time pads fall apart instantly when attacked with a known plaintext.

Oddly, using a multiple-time pad on top of a moderately strong block cipher such as DES gives a result which is stronger than the sum of the parts. This is because the usual attacks on a multiple-time pad do not work if the message was pre-encrypted using something like DES or AES, which have good entropy characteristics. The result is that 56-bit DES plus a 64-bit multiple-time pad provides better security than either method by itself. How much better? That depends.

In the case of a quantum computer, you can see that increasing the number of bits in the key will increase the cost of the decryption device, which is gratifying. More important, you will observe that, for every possible 56-bit DES key, there exists a 64-bit "one time pad" which will make the output equal the plaintext. In other words, this system has the characteristic that it supports 2**56 valid decryption keys, each of which is 120 bits long.

For organizations with a large budget, it is still possible to attack this system by analysis of multiple blocks, etc. It's just that low-cost additional coding steps can cause exponential additional effort to be required, which makes quantum computer resistant crypto systems secure, for all practical purposes.

Conclusion

While mainstream algorithmic coding systems are vulnerable to near-term quantum computers, it is possible to design coding systems which are more secure than current practice. The most promising designs involve the use of multiple valid keys.

The 21st Century Hacker Manifesto

by Prisoner #6
http://ebony.gomen.org

1. Hackers are no longer anonymous independent operators or groups: We are now a known and calculated factor in the machinations of the most powerful individuals, groups, mega-corps, governments, cartels, mafias, etc. on Earth... except for the very best - and even then, for how long?

2. Being a hacker is no longer synonymous with: "phreaker, inventer, tinkerer, genius, security expert, oddball, eccentric, helper, trickster" or any other benign adjective. Let's not fool ourselves. Our new titles are: "terrorist, threat, intelligence agent, anarchist, snitch, gov/mob recruiter, honey trap, fool, mentally disabled, sociopath, psychopath, career criminal, desired asset, puppet, and similar.

3. Hackers are being treated by all global-scale organizations as "natural resources." History shows quite clearly how these organizations treat "natural resources" - raping, pillaging, fighting for ownership, using each skilled hacker until they are burned out, used up, dead, or otherwise disabled.

4. The new global arms race is no longer about who controls the most atomic bombs. It is about who controls/owns the most hackers, botnets, and exploits (zero day and otherwise).

5. Being an elite hacker with current knowledge of the *actual* state of global dynamics (aka "politics, news, propaganda"), the kind never released to the public, may make one feel very "kool," but attempting to inform and/or discuss any of your very real privileged information with, basically, any other non-hacker will not result in praise. Just the opposite. We are disbelieved, mocked, and even scorned. Being a member of the new digerati may be intellectually gratifying, but ultimately only isolates us from the majority of other humans.

5a. This isolation serves the interests of global organizations by offering us a "place among peers," "a chance to work with tech only dreamed of by most isolated civilian hackers" and non-obtainable otherwise, the possibility of having our genius *rewarded* and *recognized* and "the chance to use our skillz to help change the world." Though *some* sizable truth exists to these claims, the fact is that once employed by any of these global elites, we immediately become slaves (rather than "valued operators," as in the sales pitches), where traditional rules of espionage reign supreme and *not* the "corporate ethic" most of us expect and are used to.

5b. Espionage rules dictate that all hackers are "assets to be controlled by any means necessary." Sadly, but quite seriously, this includes torturing, killing, threatening, pressuring, etc. of family, friends, and loved ones; public exposure of our "shameful secrets" or, if none exist, simply creating them; unlawful criminal prosecution ensuring little possibility of other "straight" jobs; and worse.

5c. Once an asset of any global organization, it is extremely rare to ever be allowed to leave. Any of us that seem to be "former-blanks" are to be treated with extreme suspicion.

6. World War Three has been going on for some time now and its battlefield is cyberspace. By labeling yourself a "hacker," you are now volunteering as a *combatant*.

7. The "Internet" is not now, nor has it been for some time, a "simple network of computers." With smart phones, iPads, Wi-Fi, NSA-everything, IPv6, Botnets, etc., it would be far more accurate to call it a "four dimensional tesseract hypernet." It's a completely chaotic clusterfuck, basically. As per beginners' network theory: a device or program existing on a network is accessible by *anyone* with network access. What NSA can do, so can the Yamaguchi-gumi, with the *same tools!*

8. As a simplified model, there are essentially no more "governments" or "countries" with any true global power anymore. The world, as we elite hackers know it to be fact, is comprised and controlled purely by:

A) Multinational corporations (including NSA, CIA, etc.)

B) Organized global "criminal cartels," including the previously Russian "Brother's Circle;" the Japanese Gumi's and Kai's, the largest and most powerful of which is the Yamaguci-Gumi; the Chinese Hong and Tong societies (who, along with the respected Japanese "Yakuza" are actually quite formal and completely *legal* components of their country's government; traditional "Mafia families," such as the respected Sicilian, Colombian, Mexican, etc....

8a. What remains as the "public face" of the United States and other governments is a mere

public relations shell which exists solely for the purpose of continuing to extract and export all remaining possible valuable resources from the ignorant hardworking wage-slave public and placing it permanently into the hands of the globals.

8b. For the time being and in the near future, there are plenty of resources being extracted from the public for all the true global players to be perfectly happy with the arrangement and, as such, very little actual conflict or competition exists between them. This is why there are no obvious large scale violent conflicts (outside of propagandized isolated incidents) to indicate this new global "arrangement," as fairly accurately predicted and described by such authors as William Gibson, Neal Stephenson, Marshall McLuhan, and others.

9. Be aware that as a "natural resource" and "desired asset," many, if not most, modern "hacker spaces" quite suddenly appearing in major cities everywhere are either openly (more often secretly) funded and controlled by DARPA and/or aforementioned organizations with the primary purpose of counting, monitoring, investigating, and eventually recruiting you.

10. If you are one of us - a young or older, yet-unknown hacker - the smartest course is to *stay that way*. An author in a previous *2600* article was foolish to say that "hacker nicks" were a thing of the past. I honestly (though respectfully) think he was being egotistical to publish articles under his *real name*. Respectfully, because his "point" was sort of later proven by Snowden and others: *any* well known hacker is probably also well known to the NSA, nick or no nick.

10a. The best policy in these interesting times is to:

I] Stay alone.

II] Stay unknown.

III] Repeat after me: "Me, a hacker? Ahahahahaha! I wish! Nah, I just keep up with tech stuff to help my parents protect their desktop and hopefully get a decent job one day. I love computer tech and all, but I've *never* been smart enough to be a hacker! I just don't have the time to study and keep up with all that stuff. I do have a life, you know!"

11. Linux is the only "safe" OS left (if one exists at all!) and then only when heavily modified and encrypted. Really, NetBSD and/or custom kernels are required even to *imagine*, arrogantly, that you *may* be "private."

12. Public key encryption *may* (I say with heavy doubt) be the one last hope we have and then only with ridiculously huge prime numbers. At least for the time being, where *public* tech is concerned; math still beats tech.

Shouts out to: The Mentor (for his first one, thanks and luv for inspiring a generation); Kevin Mitnick's Latest Book "Ghost in the Wires" (best of his, by far!); Patrick McGoohan's TV series "The Prisoner" (Oh yeah, global village? You'd better believe it!); The United Socialist Republic of Barrett Brown's (all of them, even the one I trash I like and best MySpace group ever!); "Best Truth," a Princeton study in intelligence agencies by Berkowitz & Goodman (speaks for itself); and Adrian Lamo (Mucho amo amigo! A most misunderstood hacker and excellent case study of "the path to Hell is paved with good intentions.")

P.S. Wasn't "Emmanuel Goldstein" a fictional character created by the global intelligence agency to *capture* people who were too smart? Trust *2600*, do ya? Lolllzzzz....

EFFecting Digital Freedom

by Vera Ranieri

The Internet has been an amazing driver of innovation. New companies have sprung up seemingly from nowhere to deliver new and useful services. Important to that ecosystem is the idea that all traffic on the Internet is generally transmitted without unfair discrimination based, for example, on the identity of the sender or receiver of the information or the protocol being used. It is this idea that we refer to as "net neutrality."

As an Internet subscriber, you don't expect your ISP should care about what bits are transmitted across its lines. A bit from your favorite social media website generally costs just as much for your ISP to deliver to you as a bit from your favorite pizza parlor does. As an entrepreneur hoping to become the next best social media website or pizza parlor, you're glad that your ISP doesn't care: you have just as much access to the consumer as the next guy.

Unfortunately, ISPs have already indicated they are more than willing to abandon net neutrality by discriminating against certain types of traffic. In 2007, Comcast was caught interfering with their customers' use of BitTorrent and other peer-to-peer file sharing systems. More recently, in 2012, Verizon was fined for charging customers for using their mobile devices as a mobile hotspot.

Of course, Internet providers have long offered different levels of service to consumers for varied pricing. For example, a small business that makes extensive use of video conferencing has the option of paying more for more bandwidth, and that's fine. Problems arise, however, when ISPs use their position as gatekeepers to play favorites, provide faster or slower connections to certain websites, and charge website owners for access to the ISP's customers. At that point, user choice becomes a smaller and smaller driver for innovation.

The History of the FCC and Net Neutrality

Thus, the fear is that without net neutrality rules in place, ISPs act in ways that threaten innovation culture. Recognizing this risk, the Federal Communications Commission (FCC), the agency tasked with overseeing telecommunications, has twice tried to enact net neutrality rules. But each time, the rules were struck down by the courts.

Why? The FCC, as an administrative agency, can only do what Congress has given it authority to do. And if it tries to do something that goes beyond that, a challenger may be able to get the rules struck down in court. And this is what happened to the FCC.

Because of a decision made by the FCC in 2002, the FCC hasn't classified cable-based ISPs as a "telecommunication" service (something that would mean classification under Title II of the Telecommunications Act). Instead, the FCC determined that such ISPs were "information services" and therefore outside the scope of Title II.

But the FCC saw the need for net neutrality, and attempted to bring that about using authority other than Title II. The FCC first tried to enforce net neutrality under its "ancillary authority." Comcast challenged that authority, and in 2010 the FCC's rule was struck down. The FCC also tried to bring net neutrality by using its authority under "Section 706." This time Verizon challenged that rule and in early 2014 it succeeded. The reasons why the courts struck down the rules are complicated and mired in technical legal details. But the basic point from each case is this: because the FCC tried to make rules

where Congress hadn't given it authority to do so, the rules were not allowed.

What Now?

Today, the debate centers around whether the FCC should "reclassify" ISPs under Title II or continue to try to use Section 706 (even though using that section has already been rejected by the courts). Many people believe that Congress gave the FCC authority to enact net neutrality under Title II if it determines that ISPs are, in fact, a telecommunication service.

But there are those (ISPs in particular) that are against Title II reclassification, as they fear it will impose a whole set of rules that were developed for telephone service. Most of those rules just don't make sense when we're talking about Internet infrastructure. For example, there are rules about obscene phone calls, rate schedules, telephone operator services, etc., which are unnecessary to net neutrality.

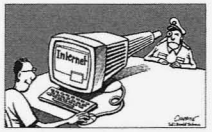
ISPs and those against reclassification aren't telling the whole story. An important aspect of Title II regulation is that it allows the FCC to "forbear" from full regulation - that is, decide not to apply all the rules that would normally come with Title II. This forbearance is a formal process, and a future FCC would have to go through an onerous process to reverse a decision to forbear. Because of forbearance, the FCC can choose to not enforce a given rule if it is not necessary to promote good practices, or to protect consumers and the public interest. Forbearance is crucial to net neutrality because it helps to limit FCC regulation. If the FCC reclassifies broadband as a telecommunications service, which it must if it is going to do its part to protect an open and neutral Internet, then it should also use its ability to forbear to ensure as little regulation as possible to enact net neutrality.

How You Can Help

The Electronic Frontier Foundation (EFF) has created a simple form that you can use to submit comments to the FCC, available at `www.DearFCC.org`. Already the FCC has received over three million comments from Internet users regarding the new rules. Use this website to add your voice and let the FCC know what you think about net neutrality and the importance of keeping the Internet free and open. Let the FCC know that we want the Internet to help, rather than hurt, innovation, creativity, and freedom. We don't want an Internet that is controlled by gatekeepers who can use their position to extract more and more tolls from those who seek to use it.

SUPPORT THE EFF! Your donations make it possible to challenge the evil legislation and freedom restrictions we constantly face. Details are at https://supporters.eff.org/donate.

Are You the Consumer, or the Product?



by the Piano Guy

Do you pay to use Google? Do you pay to use Facebook? If you don't advertise on these services, the answer is probably no. That then means that you are the "product," rather than the "consumer," even if you think you're just a consumer.

Why does this have hacker ramifications? Because to be something worth being consumed by the people who are buying the product (the advertisers), you have to give up privacy. This is probably apparent to most folks that would read this fine publication, but it isn't apparent to your friends and relatives, and you may want to give them this article so you can say that you are not the only person who is concerned about these issues (since they may think you're paranoid already). Further, you may not be aware of the depth to which this goes, which may make you rethink some of your practices - or at least tell those you care about.

"But I don't do anything illegal, why should I care about my privacy?" might be what you hear back from some people. You may even think it yourself, especially since knowing how to do things that are illegal doesn't mean that we actually do illegal things. As an aside, I'd be curious to know how many of us subscribe to the motto "just because you can doesn't mean you should." My hunch is that it is a much higher percentage than what general society perceives.

The reason to be concerned about privacy is because what is legal and reasonable today may not always be. Google will hold on to your data forever, and there is no guarantee that they will be able to keep it from being used for purposes we would consider evil today, either by computer-savvy villains or governments.

Allow me to use myself as an example. The Creator of the Universe gifted me with many things, but in this go-around heterosexuality was not among them. I've already received government-sanctioned discrimination based on this; I was denied a top secret clearance in the 1980s because I was perceived as a blackmail threat. The laws have changed, but they could change back. And they could get worse. Things could degrade in society to the point that I could have a similar issue of being blackballed because I write for this fine publication, or you could be for having read it at one time.

In the United States, our government, for all of its flaws, could be a *lot* worse. There are elements in our current government that are trying to take it in that direction. If enough wise and thoughtful people don't get out and vote (hint hint), it could go there. Think about this: George Bush won by 538 votes in Florida. Think of the wars, the financial ruin, and the many dead worldwide that ensued because of this man's policies. 538 people made the difference, and we're still paying for it.

If you live outside of the United States, but in a country where you can read this magazine, your government too, for all its flaws, could be a *lot* worse.

Having established why privacy is important to everyone, let's discuss how Google violates your privacy on a regular basis.

Recently, a man was arrested because while Google was searching through his Gmail for keywords to know which ads to push to him, they found child porn in his email. Google goes so far as to have staff look at every picture in email, and also has a hash of previously found porn to aid in flagging potential offensive content. They report it, as they should.[1]

Now please know that I am glad that they caught a consumer of child pornography, and that I never endorse illegal activity. I don't even endorse engaging in "victimless crimes" or "things that should be legal anyway." That's not the point. How comfortable are you with having every single thing you send be reviewed and stored forever?

"But the NSA stores everything anyway, so what's the difference?" It is the difference between crossing the street in front of your home at 2:00 am after looking both ways and dancing drunk and naked on the freeway during rush hour. You're much more likely to get "hit" if Google is used to find you.

"OK, so I'll encrypt my emails." That will guarantee that the NSA stores them forever[2].

"I'm careful, and I know what I'm doing." Do you love your parents? Your siblings? Your friends who aren't as 1337 as you? Do you take time to teach them how to protect themselves?

Will they do so? Do they get the cost/benefit here that you do? Help them do the simple things, like not using Gmail or Google Docs for anything that they would not want to be permanently archived and analyzed, potentially even after they are dead and gone.

The level of surveillance is increasing all of the time. Facebook has a similar business model to Google in that they are both advertising companies that use the Internet to provide information to their customers (the advertisers) about their product (that would be you). Facebook is trying to force everyone to use Facebook Messenger. I don't know if/when they will remove messaging functionality from the phone app, and I don't know what they are going to do on the desktop, but if you read the TOS for the Messenger app, you'll most likely not install it.[3] But, your relatives and friends will. Smile, as you will potentially be on candid surveillance.

Ultimately, if we don't get out the vote, and keep it out, we won't keep our government. If we don't keep our government, "tools" like Google and Facebook will be used against us in more insidious ways than we can imagine. With computer-savvy villains on the loose, we have even more reason to be concerned, even if we keep our government intact. Beyond voting, the only thing we can do is use safer services in more appropriate ways, to be less of a "product" for the "consumers."

References

http://www.telegraph.co.uk/technology/google/11010182/Why-Google-scans-your-emails-for-child-porn.html

http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/

1. http://www.huffingtonpost.com/sam-fiorella/the-insidiousness-of-face_b_4365645.html

GENERATING PHONE NUMBERS

by Samuel A. Bancroft

It's no secret that many people use their phone number as a Wi-Fi (WPA/WPA2) network passphrase. Two factors contribute to this. Firstly, WPA/WPA2 requires a passphrase that is eight to 63 ASCII characters long. A phone number, being ten characters long, is simple to remember and to type. Secondly, oftentimes ISPs will configure the home's wireless network to use WPA/WPA2 using the customer's phone number as the passphrase. Customers infrequently change it.

WPA/WPA2's shared-keys can be brute forced, but the time involved is a major obstacle. A dictionary attack is more practical and a phone number dictionary attack may be the most practical of all due to its high yields and simplicity.

Many people use wordlist generators such as Crunch, a wordlist generator that produces large word/number lists with specific patterns, to create a "phone number" dictionary using the pattern <AREA CODE>%%%%%%%.[1] Others create scripts to do something similar to the pattern above.[2] This method of creating a phone number list is inefficient and ignorant.

The North American Numbering Plan (NANP) is a telephone numbering plan created by AT&T in 1947 and put into operation in 1951. It serves 20 North American countries.[3] The NANP dictates the rules for area codes, exchange numbers/prefixes, etc. For example, exchange numbers ranging from 000-199 are not used within the NANP plan. Knowing this, we can see that generating numbers using a scheme such as <AREA CODE>%%%%%%% creates a lot of waste. Just knowing that the NANP does not use prefixes 000-199 means that the above scheme will create 10,000 numbers per invalid prefix for a total of two million invalid phone numbers.

There is another consideration. Various prefixes within a valid range are not used and this varies throughout different area codes. To illustrate, area code 906 (Marquette, Michigan) contains 305 valid prefixes while area code 212 (New York, New York) contains 778 valid prefixes. If we use the Crunch scheme we discussed for area code 906, we would produce 10 million numbers while only 3.05 million numbers are valid for this area code. As can be seen, about seven million invalid numbers would have been created.

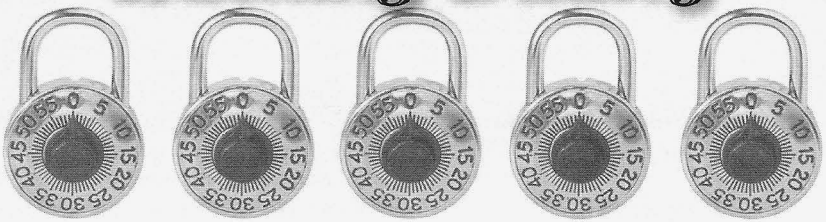
Below I have included a Python script that will generate every valid phone number within a specified area code. It accomplishes this by scraping valid prefixes from

http://www.allareacodes.com and producing valid phone numbers from it. The numbers are saved in a text file. Take look at the bash script f0ne.sh by DERV if you are looking for something with more bells and whistles.[4] Help save the planet - do not generate millions of invalid numbers.

```
#!/usr/bin/env python3

import urllib.request
import re

def main():

    ac = input('Enter the area code to compute: ')
    url = 'http://www.allareacodes.com/%s' % ac
    body = requestPage(url)

    # Find the region we are intreasted in.
    findStart = re.search(r'Area Code ' + ac + ' Prefixes', body)
    findEnd = re.search(r'Most Searched Numbers', body)

    try:
        startSpan = findStart.span()[1]
        endSpan = findEnd.span()[0]
    except AttributeError:
        print('Error: Area code is not valid.')
        quit()

    getPrefix = re.findall(r'\(\d{3}\) \d{3}', body[startSpan:endSpan])
    prefix = cleanList(getPrefix) # Removes '(305) '

    makeFile(ac, prefix)

def requestPage(url):
    req = urllib.request.Request(url)
    response = urllib.request.urlopen(req)
    return response.read().decode('utf-8')

def cleanList(getPrefix):
    prefix = []
    for fix in getPrefix:
        prefix.append(fix[6:])
    return prefix

def makeFile(ac, prefix):
    textFile = open('%s_numbers' % ac, 'w')

    for x in prefix:
        for i in range(10000):
            textFile.write('%s%s%s\n' % (ac, x, str(i).zfill(4)))

    textFile.close()
    print('Done. Area code %s had %s prefixes' % (ac, len(prefix)))

if __name__ == '__main__':
    main()
```

[1] http://packetfactory.wordpress.com/2012/06/29/generate-10-digit-phone-numbers-using-crunch-in-backtrack/
[2] http://www.josephlandry.com/2011/01/phone-number-dictionary-file-for.html
[3] http://www.nanpa.com
[4] http://pastebin.com/v2jJHYZ2

Hacking Dudley



by David Crowe

Officer, I swear I didn't mean to hack it, but it was either that or be thrown out on the street in skimpy shorts and a thin, sweaty, t-shirt.

I don't know whether to start this story at the end or the beginning. If I start at the end, I have to tell you of my shock when I opened my gym bag and found inside two identical Dudley combination locks. How could this be? I only owned one because I get easily confused and two identical locks with different combinations would mean I would be forever getting flustered. Were they breeding, or was someone playing a trick on me? Was it magic, or was it the NSA?

Suddenly, I remembered the beginning of the story (although I didn't realize it at the time). A couple of days before, I had returned to the locker room after my workout and couldn't open my lock. For 15 minutes I swore under my breath, trying the combination I had known by heart for months to no avail. I checked the not-so-secret place I had it written down; it was as I remembered, and still it wouldn't open. I cussed the lock that I assumed must have malfunctioned. Just in case the lock was misbehaving, I was adjusting each number up one, down one, and then, just about when I was ready to give up, the lock opened.

I was glad I hadn't called the locksmith to cut it off. How could I have explained that I was locked out by my own lock? Would the fitness center believe that I wasn't just trying to break in to Mr. Big's locker and steal his stuff? What the heck was wrong with *my* lock anyway?

But now I realized what had happened. I had picked up someone else's lock and put it on my locker, which is how two got in my gym bag. But how had I opened someone else's lock with *my* combination?

I started to think about it, and do some investigations. This style of Dudley lock has 60 numbers on the ring, so theoretically there are 60x60x60 combinations - or 216,000. What are the chances of me getting a lock with a combination anywhere close to mine with those odds?

But I've observed that these locks don't require precision. I found that the first number could be off by three and still work - six different numbers would work. So there are effectively only ten possibilities for the first number in the combination. The second number in the triplet is even more permissive. I could be off by five and still open the lock, so there are only six possibilities here. And the third number is also permissive, but it actually doesn't matter. If you get the first two correct (or at least close to correct), you can simply twirl the dial slowly with a little pressure until it opens. So that means the two locks I have really only possess 60 different combinations.

My chances of getting a compatible combination lock were therefore one out of 60. I still wouldn't bet on those odds (I don't bet on any odds, actually), but it's a whole lot more likely than one out of 216,000. I would love to know what the owner of the lock thought when he couldn't find his lock. "What kind of idiot would steal a lock not knowing the combination?" But no locks were reported missing at the gym club (he was perhaps as embarrassed as me), so I had no chance of finding him and returning it. Now I am the proud owner of two locks that can be opened with the same combination.

The normal disclaimer implies. Use this to get yourself out of trouble, not to get yourself into trouble.

I'm not a lock picker; the only thing I'd picked before was my nose. It's probable that experts know even more tricks with these locks, in which case they are pretty useless. Good for protecting clothes at the gym club, but don't fill your locker with gold bars and expect them to be there when you get back.

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

by Andy Kaiser

Chapter 0xB

My client Oober had just disappeared on me. P@nic, the missing hacker, was involved in a hacking competition which held some connection with the Naked Princess picture, but she and the picture weren't talking. Both were hiding more effectively than an Easter egg in N64 Goldeneye.

Even still, there were a few logic gates I could slam through: I needed to talk to Oober. I knew his name - his own mother had dropped him off at my office. He might not want to meet in person again, but maybe I'd do it anyway if I couldn't ping him in digital form.

As for P@nic, I'd realized she might be operating under an alt, also hacking with the handle "Chixor Zed." My conversation with Lynx had told me that Chixor Zed hadn't been responsive, but I had an in. Hopefully.

It took a while of scanning forum postings and IRC chat logs to find Chixor Zed. The timing seemed to fit my theory - Chixor Zed had appeared out of nowhere - just after the AnonIT hacking competition was announced, and long after P@nic had a solid online presence.

I saw too that P@nic herself was all over social media. Or she was, until just about a year ago, after which the handfuls of anonymously-maintained social media accounts just stopped posting, stopped updating. That date didn't correspond with anything else I knew about her, Oober, or AnonIT, so I saved that for later compiling.

Since she'd gone off-grid and had stopped social media involvement last year, I had no clue if any of her accounts were maintained, but I knew how to find out.

I looked at the list of social media sites that she'd been a part of, and got to work.

I began with a deep sigh. Then I signed up for FriendyFace, SyncedIn, Twitchat, and far too many more of the social media heavy hitters that P@nic and everyone in civilized society seemed to care about except for me. Social media made me want to lurk, not like.

Being Dev Manny and the Information Technology Private Investigator that I was, I had little to brag about. My lack of effort at social media was probably why I had close to zero clients. I resolved to someday throw a new title on my business card and recommit myself to sales. Something like "Best Damn Social Mediator," only with a more family-friendly acronym.

While signing up, I used a temporary email address and fake account info. My highly developed paranoia smiled and gloated just minutes later, as my inbox began to explode with spam spawning from those who thought it ethical to sell my information to scammers. I watched in real time the flood of unsolicited friend requests containing cute/funny/adorable pictures of cats/dogs/penises.

I ignored it all and planned out the only other action I wanted to take on each site. The point of all this was to send P@nic a very specific message, and it had to be crafted. The message had to let her know I knew about her double identity and her involvement in the AnonIT hacking competition, and that I was friendly with Oober - and do it all in a way that wouldn't be understood by anyone intercepting the message.

After trying a few variations, I copied and pasted to P@nic's year-old accounts:

"Don't panic. Need to have an uber-talk, from Anon to Zed."

Then I waited.

Not long after, my inbox incremented by one. There was no cute/funny/adorable picture, just a one-sentence response from the P@nic account holder:

"I Retire Chixor right now."

I stared at the message, wondering at the weird phrasing and capitalization. After seven blinks, I understood and scrambled to get on to the IRC channels where I'd last seen Chixor Zed.

That's how I made contact with the missing teenage female hacker and Oober's obsession. I was finally talking with Chixor Zed, also known as P@nic.

Chapter 0xC

P@nic: *?*

Me: *I'm a friend of Oober: Dev Manny, Information Technology Private Investigator. Oober's worried about you. I've been sent to find you.*

P@nic: *i'm in deep water and he's a little fish. staying off grid to keep him safe, to keep family safe. parents are out of country anyway. they know nothing. keep oober out of this, get me?*

Me: *Might be hard to do. He's my client. He likes you.*

P@nic: *yeah, i get that. so if you care about him, help me. i can't go home, but i need hands onsite to access something important.*

Me: *Why me and not Oober?*

P@nic: *because you have a car.*

P@nic: *because i care more about oober than you.*

P@nic: *because i will pay you a lot of bitcoins.*

P@nic: *and because i said please.*

P@nic: *please.*

Logic, loyalty, and bitcoins. I did like this girl.

She then relayed some very simple instructions, an address, and what to do when I got there. We broke contact and I headed out, hoping my car would beat its current 30 percent chance of starting.

I made sure my car doors were locked. I didn't like driving to this part of the city. Part of my worry was the state of the houses themselves, their conformity, the visual display that might as well have screamed how the homeowners lived quiet lives of quieter desperation.

The deeper I drove into this community of despair, the more out of place I felt. I took too long poking at the GPS and missed my turn. It took me several tries to convince my car to shift into reverse, but eventually the transmission rolled the right dice, ancient gears slammed into place, and my car lurched in the direction I wanted it to go, punctuated with an angry cloud of black smoke.

P@nic's house wasn't a mansion, but it was close.

The three story house was all brick and stone and modern elegance. A canopy of cheerfully leafed trees covered the neighborhood and cradled above the house like a beautiful green umbrella. The nearest house to this one was hundreds of yards away. All houses here had wide lush yards with bushes so carefully shaped they almost looked plastic. Even with all the trees, not one leaf was out of place.

All in all, this was a perfect place to live, a shiny close-knit community just outside of a big city, full of wealth, safety, space, and beauty. A dream house in a dream location.

I hated this part of town.

My own office - with its coffee-stains-where-there-should-never-be-coffee-stains, the evolving funky smells, the building electrics more temperamental than a rabid dog - that was more honest than the "perfect" home in front of me. I didn't care about comfort. I dealt with the truth about reality instead of trying to hide from it.

I pulled into the driveway, though my car didn't want to. Intimidated by pavement somehow free of cracks and oil stains, my car sneakily dropped into neutral and tried to roll back down the inclined driveway. I sensed that if I shifted into reverse and floored the gas, my car would find its way out of this place without me even needing to drive it.

I set the emergency brake, killed the engine, waited for the car to cough itself to death, and got out. I walked up to an entranceway so large, welcoming, and column-filled, I felt like I was stepping into a movie set.

There was a doorbell, so I pushed it. A faint *BONG-bong* echoed through the house.

I stood and waited.

When I was reasonably sure that no one was home, I followed P@nic's instructions - there was the fake rock, just under the leftmost bush. The key fit the front door. There was no alarm system. I was amazed at the trust and lack of security. Like building a wireless network with WEP encryption... you just don't *do* that.

I pushed into the house. The foyer was big. The adjoining rooms were big. The stairs were big. The only thing out of place was the small human looking around the place: I was alone.

Where I needed to go wasn't far. I climbed to the top of the stairs and turned into a long hallway that sprouted bedrooms and offices along its length. On the hallway wall was the row of pictures P@nic told me to look for.

I saw P@nic for the first time.

She was an only child. The first picture leading the mounted row in front of me was that of a happy-looking couple on a palm-tree-studded beach. Must be the parents. They wore outdated clothes, and the photo print was taken with an early generation digital camera, grainy and a little off-color. That told me something interesting: This was a tech savvy family, early technology adopters, dating from before megapixels killed film. That mentality might explain P@nic's head start in hacking.

The next photo was of a beta version of P@nic - what normals called a "baby." Wavy dark hair hung close to bright, eager brown eyes. Looked like a cute kid.

The next picture was her a few years older, wearing a pink dress, a wide grin on a face almost hidden by a massive armful of stuffed animals. Her brown hair was longer, with pink bows. Cute.

The next picture was maybe around nine or ten. She was intentionally posing like a model on a runway, with a self assurance rarely found in any adult outside of Hollywood or politics. Her hair was even longer, double-braided, hanging down almost to her waist. She had serious eyes that tried but failed to hide a shining joy in whatever it was she'd been doing at the time of the picture. Cute.

The last picture in the row wasn't cute. It wasn't of a child.

It was P@nic in her early teens. Her long hair was gone, cut choppy at her jawline. Her hunched posture indicated frustration, irritation, a desire to be anywhere else than where she was. There was no pink in her outfit, just dark colors and simple clothes, a fashion afterthought. The worst was her eyes, which had darkened to something sullen and suspicious. Angry.

This last picture was so different from the others, it took me time to figure out why it was even there. Maybe it was something about kids getting older, and the parents would take what pictures they could get. I didn't have kids. I didn't know how they worked. But I remembered enough of my teen years to know they sucked. Maybe that's what this was - P@nic criticizing the rest of the world until she found her place in it.

At a second glance, I knew I was wrong. I leaned in and looked closer at the picture. The eyes....

The eyes told me more than they meant to. They were cautious, almost feral.

Something in her had been hurt. Injured. Broken.

Lost in analysis, I remembered what P@nic had asked me to do.

I flipped the picture around. I gently detached the image from the frame. Between the thick cardstock backing and the photo was a piece of folded paper. I took it and put it in my pocket, but not before first opening it, verifying what I thought it was, and taking a cellphone shot of the contents.

I began to repair my permitted vandalism and put the photo back in the frame. While doing so, I checked the back of the photo. It had been professionally printed, and I read the imprint of the printing company and the date stamp.

The picture had been taken one year ago.

P@nic had quit all social media about a year ago. She'd later won the AnonIT competition, and part of the winners' booty was the Naked Princess photo. The piece of paper I held was linked to the AnonIT competition.

The data bubble-sorted in my head, and certain events began to line up with others.

P@nic was tied to the Naked Princess photo. Whatever had happened with it had changed her life enough to turn treasured family photos from light to dark, and had caused her to sever all ties with social media. She then later inserted herself into AnonIT, in order to do something with the photo... or despite it.

As proof, I'd seen P@nic's childhood pictures, with multiple pointers to some significant event happening a year ago.

As proof, I was in the middle of a very strange case, between P@nic, Oober, the AnonIT competition, and the Naked Princess - a picture so horrible it had terrified and disgusted all who saw it.

As proof, I had a piece of paper in my pocket.

The paper was a note from P@nic. Her meticulous and careful handwriting held what she'd asked me to get: A hand-printed encryption code. It was a 384-digit key needed to open up her cloud-based storage locker.

I knew it was important, so much that P@nic had risked exposure by asking me to get it.

I had no idea yet what it would reveal.

The key word being "yet."

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.

January 16-18
ShmooCon
Washington Hilton Hotel
Washington DC
www.shmoocon.org

March 20-22
CarolinaCon 11
Raleigh, North Carolina
www.carolinacon.org

April 3-6
Easterhegg 2015
Kinder und Jugendzentrum Mühle
Braunschweig, Germany
www.easterhegg.eu

April 25-26
Maker Faire U.K.
Life Science Centre
Newcastle upon Tyne, England
www.makerfaireuk.com

May 14-15
THOTCON 0x6
Chicago, Illinois
thotcon.org

May 16-17
Maker Faire Bay Area
San Mateo Event Center
San Mateo, California
www.makerfaire.com

June 3-5
RVAsec
Richmond, Virginia
rvasec.com

June 12-14
CircleCityCon
Indianapolis, Indiana
circlecitycon.com

June 12-14
NolaCon
Crowne Plaza New Orleans
New Orleans, Louisiana
nolacon.com

August 6-9
DEF CON 23
Paris/Bally's
Las Vegas, Nevada
www.defcon.org

August 13-17
Chaos Communication Camp
near Berlin, Germany
www.ccc.de

September 26-27
World Maker Faire New York
New York Hall of Science
Queens, New York
www.makerfaire.com

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

Marketplace

For Sale

CLUB-MATE is now easy to get in the United States! The caffeinated German beverage is a huge hit at any hacker gathering. Available in two quantities: $36.99 per 12 pack or $53.99 per 18 pack of half liter bottles plus shipping. Write to contact@club-mate.us or order directly from store.2600.com. We are now working to supply stores nationwide - full details at club-mate.us.

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.

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.

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.

BLUETOOTH SEARCH FOR ANDROID searches for nearby discoverable Bluetooth devices. Runs in the background while you use other apps, recording devices' names, addresses, and signal strength, along with device type, services, and manufacturer. Handles Bluetooth Classic and Bluetooth LE (on LE-equipped Android devices). 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.

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. Only $24.95 each if you order two or more. Add $4 S/H per order. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas, Box 410802, Crc, Missouri 63141.

Announcements

JOIN THE MOVEMENT! Help us expose the Justice Department's political agenda against hackers! We are blowing the Ghost Exodus case wide open and exposing the perpetrators responsible for manufacturing and slanting his case in favor of the prosecution, ironically, the same prosecutor residing over the case of Barrett Brown and Matthew Weigman. Find out why Jesse McGraw's lawyer refuses to file his appeal, and what one rogue prosecutor is trying to cover up. Help us to distribute pamphlets at hacker conferences and visit our legal fund to donate to the cause. Free Ghost Exodus! Free Jesse! Fundraiser: http://tinyurl.com/freeghostexodus Contact: freejesselegalteam@hush.ai Main Site (still under construction): http://freejesselegal.wix.com/freejesse

THIS IS SHIMSHON ALPERT and I am (BE"H, with G-d's help) on the way to becoming a Minister of Knesset (parliament) in Israel. I'm also a *2600* subscriber. Now that I have your attention, here are the details. I am currently in the process of putting my name on the Bayit Yehudi (Jewish Home) party list to be voted for in the primaries. This will determine my ranking and chances of entering the Knesset in the next general election. By the time you read this ad, the Bayit Yehudi party primaries may already be over. I am reaching out to the *2600* community for moral support. You don't need to do anything. Just keep me in mind, and if you know anyone in Israel, tell them about me. That was easy, right? In an ideal world, people should automatically know who I am and support me because they are not going out and attempting to become Ministers of Knesset. You're either part of the problem or part of the solution. I don't really like campaigning. I like getting things done. This ad is part of my compromise between a silent and "out there" campaign.

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

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.

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!

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 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.

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/

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!

Personal

BEING CLOSE TO RELEASE IN 2016, I am looking to brush up on what's been going on in the hacker world. I would be interested in discussing topics, getting articles mailed in, or book recommendations (or donations). Some topics I am familiar with include SQL, PHP, Wi-Fi, and pen testing. I am also interested in any info anyone will provide about speaking topics at events like Defcon or HOPE. I've been locked up since 2009 so any info, articles, or speaking topics anyone wants to send, or anyone just wanting to chat with me, would be greatly appreciated. I can be reached through Jpay.com using my DoC #339317 in Washington State or via mail at Chris Berge, 339317 10-G31, Washington State Penitentiary, 1313 N 13th Ave., Walla Walla, WA 99367. Please note that book donations must come from a company and have a receipt. Happy hacking!

I AM TRYING TO GET A STEM-PROJECT GROUP in this prison, where men can study advanced topics and apply the concepts in a hobbyist-type makerspace. The University of Wisconsin at Oshkosh's math and science departments have shown an interest in volunteering to do instruction. Books, zines, and equipment are needed to fill it out. I also really need the community to tell the prison's administration that it is a good thing to allow inmates to engage in STEM studies and experimentation, what resources and support are out there, and that such a group should be started. Warden: judy.smith@wisconsin.gov, Edu. Director: david.hines@wisconsin.gov. I can accept new (or like new) publications from any organization, with a receipt, at: Jason Glascock #342498, OSCI, 1730 W. Snell Rd., Oshkosh, WI 54901. Letters, printouts, and zines can be sent to: PO Box 3310, Oshkosh, WI 54903. I am open to any correspondence, and will try to respond to everything. My interests center on applied tech in anything from agriculture to robotics to data. Used publications (or things in electronic format) should be sent to: "Ms. Chaney - Library" at the street address above. If you have equipment, please contact Mr. Hines, the Edu. Director, and send me a record.

OPERATION PRISON PIRATE needs your help! OPP Media started as a hobby in 2012 to provide uncensored information and entertainment to various prisons in the U.S., but we've hit the limit of what we can do by ourselves. We really need donations. It costs us about $50 per broadcast, all out of pocket. Recently, our main transmitted was damaged, and we can't afford to replace it. We are also looking for engineers, producers, voiceover talent, or anyone who can help us in any way. We'd like to expand to cover even more prisons, but we need some help. E-mail us at OPPmedia@hushmail.com, and send bitcoins to 1J34tpXw84qM39LEZRtnUiVVpmuU6oxQJE.

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 Spring issue: 2/21/15.

Did you miss HOPE X?

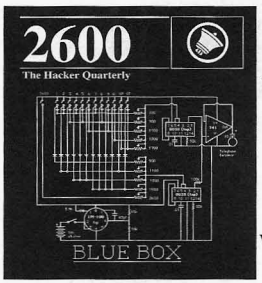
Or were you there and now you miss it because it's over? Either way, we're here to help.

We have HOPE X leftover shirts with the snazzy HOPE X badge design in the front and the colorful artwork on the back, all on a charcoal gray colored shirt. $20 each while supplies last - store.2600.com/shirts.html. Did you somehow manage to miss one of the 100 talks that were presented? DVDs of ALL of the three speaker tracks are available for only $5 each, $399 for all 102 DVDs. We can't possibly print all of the talk titles here, but you can see them at store.2600.com/hopex2014.html and select the ones you want. And for the first time ever, we' offering all of the talks on flash drives (either two 32gb or one 64gb drive). Much higher quality than what' s online, no DRM, easy to copy, sharing encouraged.

Only $99 for the entire set at store.2600.com/hofldr.html

This just in: We now have a HOPE Number Nine 64gb flash drive containing ALL of the talks from that conference for only $69! Look for details on our store.

NEW BLUE BOX SHIRT



store.2600.com
$20

We've retired the "blue" blue box shirts and have gone back to our roots with the traditional white on black style. Not only is it more readable, but it washes better and will last forever (we still see people with the ones we made over ten years ago). It also has brand new headlines on the back relevant to the hacker world.

"There will come a time when it isn't 'They're spying on me through my phone' anymore. Eventually, it will be 'My phone is spying on me.'" - Philip K. Dick, circa 1970s

***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); Winter 2014-2015, Volume 31 Issue 4, 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

Central Coast: Ourimbah RSL (in the TAB area), 6/22 Pacific Hwy.
Melbourne: Oxford Scholar Hotel, 427 Swanston St.
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: Cafe Monde et Medias, 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 Pansion and Stournari. 7 pm

IRELAND

Dublin: At the payphones beside the Dublin Tourism Information Centre on Suffolk St. 7 pm
Westport: Phone booth next to the library. 7 pm

ISRAEL

***Beit Shemesh:** In the big Fashion Mall (across from train station), second floor, food court. Phone: 1-800-800-515. 7 pm
***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

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: Upstairs at Tenders, 800 Holmes Ave NE. 6 pm

Arizona

Phoenix: HeatSync Labs, 140 W Main St. 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
Orange: Orange Circle. 7 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. 6 pm
San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

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

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

Delaware

Newark: Barnes and Nobles cafe area, Christiana Mall.

District of Columbia

Arlington: Rock Bottom at Ballston Commons Mall. 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: Ember Hookah Bar, 317 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.

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
Las Vegas: SYN Shop, 117 N 4th St. 7 pm
Reno: Barnes & Noble Starbucks 5555 S. Virginia St.

New Hampshire

Keene: Local Burger, 82 Main St. 7 pm

New Jersey

Morristown: Panera Bread, 66 Morris St. 7 pm
Somerville: Dragonfly Cafe, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 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: Cup A Joe, 3100 Hillsborough St. 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: Front of the food court fountain in Easton Mall. 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

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.

More Foreign Payphones

Malaysia. In addition to the stunning view, these payphones on Mt. Kinabalu happen to be 3.668 kilometers above sea level (a fact noted on signs inside the booths), making them the highest known payphones.

Photos by Bryan Rhodes

Switzerland. This phone is above Grindelwald in the Berner Oberland area in a cable car station at the summit of First. Now you know exactly how to find it.

Photo by Marcus

Portugal. This old school phone, seen in Vilamoura, is the basic coin model that has been tagged and stickered by many as a traditional sign of respect.

Photo by Robert Noack

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

Above: Now here is a building worthy of bearing our name. Spotted by **Gonadvs Maximvs** in Berkeley, California, this mighty complex looks down over the entire neighborhood.

Left: We've actually gotten a bunch of pictures of this locomotive recently, but we liked the one from **Jay Thomas** the best. The train is run by Roaring Camp Railroad and runs between Felton and Santa Cruz, California. As you can see, it doesn't move too fast.

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. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues) or a *2600* t-shirt of your choice.