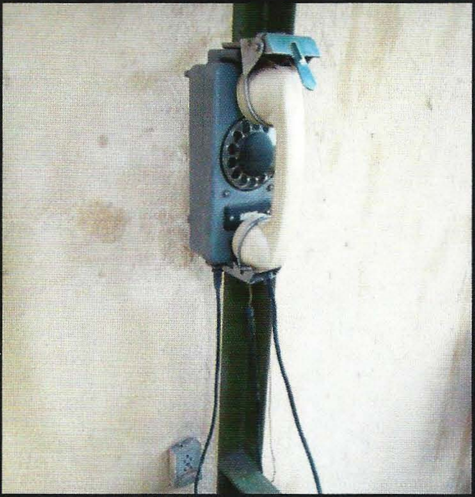
Volume Thirty, Number Three
Autumn 2013, $6.95 US, $7.50 CAN

2600

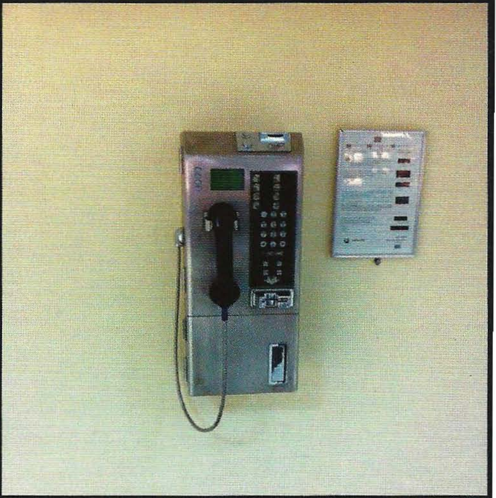
The Hacker Quarterly

Awkwardly Sized Payphones



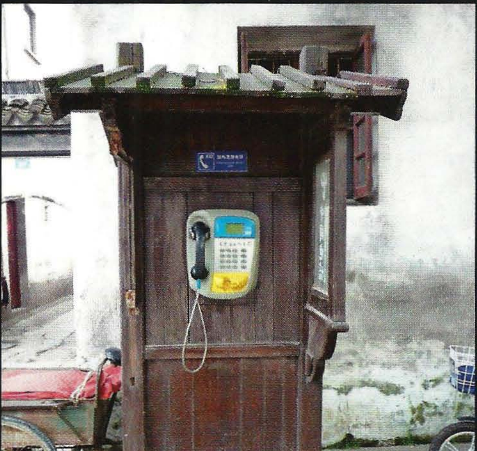
Russia. Found at the Tagansky Protected Command Point in Moscow. It's technically not a payphone and the site is technically no longer a secret military complex, but a harmless museum. The weird-sized phone still scares us, though.

Photo by Ashes



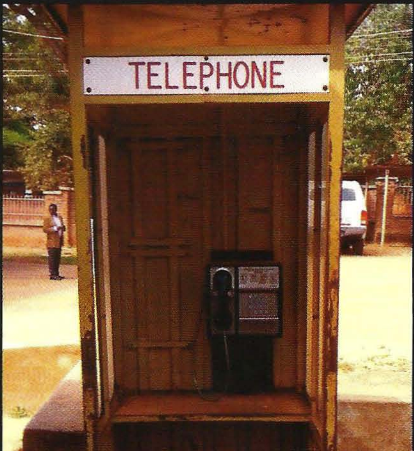
Azerbaijan. Located in the Heydar Aliyev International Airport in Baku, this phone and its instruction plate have an awful lot of white space surrounding them, making them stand out even more than the presence of a payphone normally would.

Photo by J.P.



China. It seems like this booth was constructed for a somewhat larger model of phone than the current resident, found in the ancient canal-networked town of Tongli.

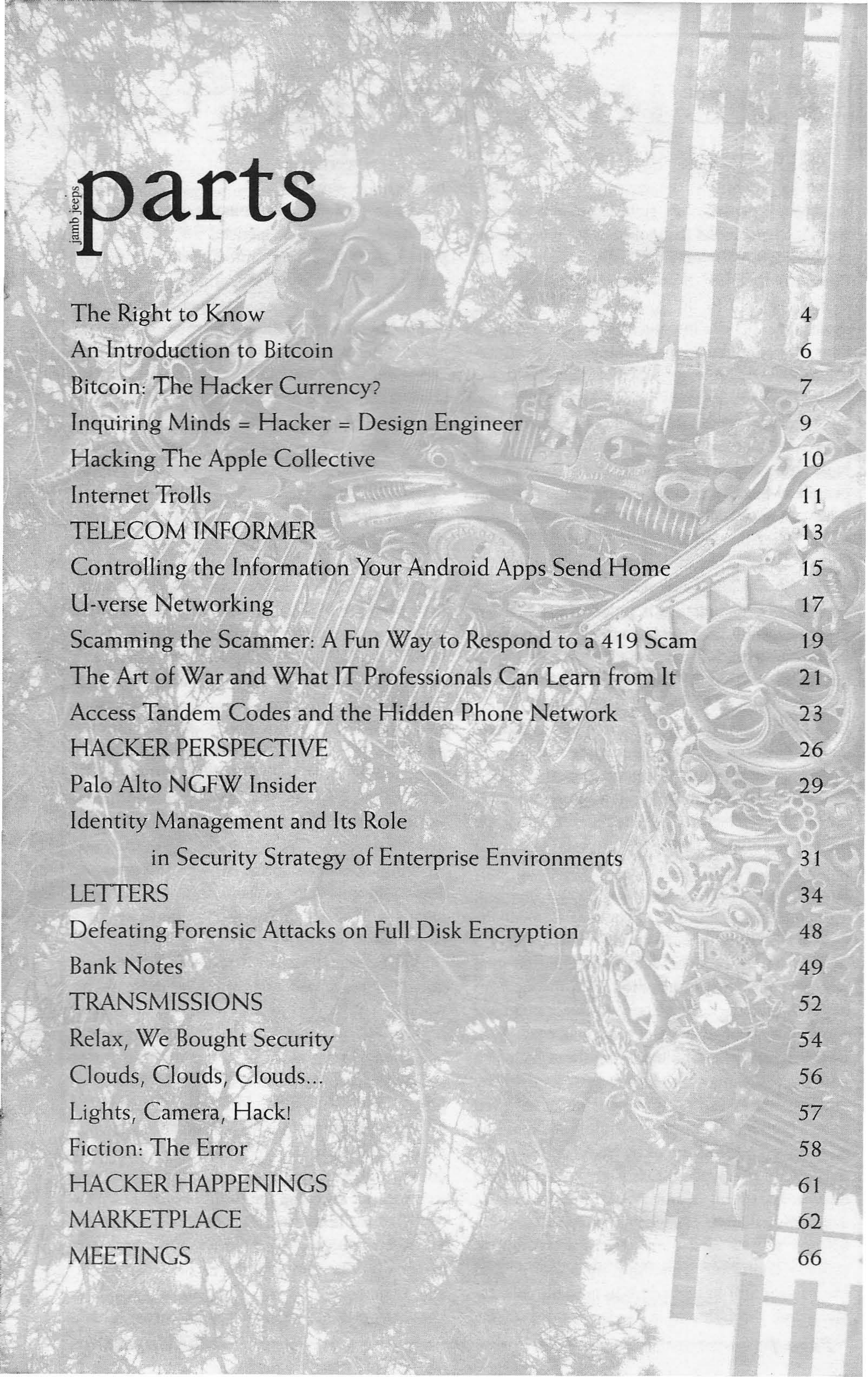
Photo by Joy Lockhart



Malawi. Found on the grounds of Ekwendeni Hospital in Ekwendeni, this fairly modern phone also doesn't seem to match its home.

Photo by Kevin

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 (Do not send us links as photos must be previously unpublished.)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



jamb jeeps

parts

THE RIGHT TO KNOW

One of the most important tenets in the hacker community is the sharing of information. We believe we have the right to see how things work, to learn what technologies are in place in our world, to ultimately understand the way it all functions together. Sometimes this knowledge is inconvenient to the powers that be. In fact, usually it is. Those in control generally preserve their power by keeping certain things to themselves. Secrets are a huge part of their world.

We've seen so many instances of this battle taking place in the nearly three decades that we've been around. Hackers around the world have revealed inconvenient truths and been penalized heavily for them. Often, these revelations are inspired by a simple and sometimes naive belief that information should be free by default. Other times, significant thought goes into it and the information revealed carries far more weight, as consideration is given to concepts of justice and full disclosure. Each of these reasons for sharing such information gives a black eye to the status quo, but the second one can be viewed as truly dangerous, since the revealing parties have actual knowledge of their subject matter - and its most relevant and interesting aspects.

What we've witnessed this summer is nothing short of unprecedented. The intrusive actions of the National Security Agency can't really be seen as surprising to anyone possessing even a passing familiarity with the American surveillance program. But having it laid out in black and white for all the world to see is a monumental embarrassment to the NSA and those who support its policies. Edward Snowden, the man who revealed this information, is someone who has exhibited the convictions we celebrate in our community, but at a great personal cost. And, whether you believe that sharing these facts is a good or bad thing, it would be very hard to say that Snowden wasn't following what he believed to be a high moral compass. While some may say he betrayed his position as an NSA contractor, he most definitely lived up to his job as a concerned citizen. This kind of individual sacrifice is rare and commendable. It's what so many of us strive for, yet so few find ourselves in a position to actually contribute something meaningful. And even fewer still in that position are able to actually come through and stare down some of the greatest powers ever to exist. How can such spirit not be admired?

We saw a similar spirit in the case of Bradley Manning, recently sentenced to 35 years in prison for revealing information from his vantage point in the U.S. military. We learned of completely unjustified civilian deaths at the hands of our own soldiers, information that was being suppressed and kept out of the public eye. We heard what governments were really saying about each other and saw ample evidence of lies and hypocrisy from all corners of the earth. There were no governments anywhere that didn't feel nervous about what the public might find out about them. And this is a good thing. We all have the right to know what is really going on. Yes, it can be said that some things need to be kept out of the public eye for the sake of security and diplomacy. But every secret is only a secret for so long and, if that's all that's holding up a regime or policy, the foundation will collapse at some point. It's even been said that Manning's revelations helped lead to the Arab Spring. If true, this would almost universally be seen as a good thing. Yet, a severe punishment was inflicted for sharing the information which so many feel has benefited the world and the ideals of freedom, far more than any harm and inconvenience that may have been caused. That shows us what the priorities of those in power truly are. Keeping the secrets and knowing one's place are way more important to them than openness and idealistic acts which could pave the way for a better world.

We've seen the evidence for this better world already. People are *talking* about these issues whereas before they would have had no knowledge at all to consider. We're thinking about our privacy a lot more now and are a bit more hesitant to believe what we're told by those in power. We've even seen changes in policy as a direct result of the NSA revelations, which never would have occurred otherwise. Education comes from knowledge and we can't honestly be free without knowing the truth.

What we need are many more Mannings and Snowdens who occupy a place in unique corners of society who can educate us on what's actually happening. And yes, we *do* have the right to know these things. A society whose government spies on its citizens and expects no objections is a society that will cause immense harm and/or self-destruct. When policies are based on lies, as we have seen in everything from legislation to wars, they spread a sickness that can be so much more destructive than any revealed truth.

We have learned a great deal in watching the reactions of our various leaders. We see how the surveillance of so many aspects of our lives is supported by politicians of both parties and how deep the cover-up goes. We also see how they have no problem changing the rules behind our backs to make these inexcusable actions "legal." Shining the light on their subterfuge is about the most patriotic act we can think of.

But this goes way beyond government. We've also seen how so many technology giants are working hand in hand to destroy any privacy we have left. The biggest have already been implicated in the NSA's PRISM program, the true extent of which has yet to be revealed. Other companies and individuals with a semblance of integrity have a unique opportunity to come forward and not play this game. Such moves, obviously, don't come without risk, something the big moneymakers aren't likely to embrace.

This episode has also taught us a great deal about the integrity - and lack thereof - in the journalistic world, a forum where this sort of thing shouldn't even be a question. When information of this sort is leaked, it needs to be reported on accurately and fairly. The world of journalism has obviously undergone tremendous changes in the past few years, but the overall values remain the same. While people like Julian Assange of *Wikileaks* and Glen Greenwald of *The Guardian* have more of a say in how their stories are reported than the hierarchical reporters of the past, what they are revealing is what is the story, not their personalities or the way they operate. So much time has been wasted on character assassination that the story itself is in danger of being lost completely. This distraction makes it easier to threaten and harass those who put themselves on the front line by daring to touch this material in the first place. We've seen a few despicable instances of this already and, no doubt, more are in the planning stages. Journalists need to be in the foreground of those who object to this sort of thing, yet too many are instead playing right into the hands of the authorities, no doubt out of fear for themselves or for losing their prized connections. Those are the ones who are in the wrong profession.

The hacker spirit must thrive in all of these environments. When policies or incidents that are unjust occur, they need to be revealed. Too many times, the excuses of just following orders or company policy or not making waves have been used. Those days have to end. The truth, though sometimes messy, will come out at some point and it's far better for us to deal with it together than to live our lives in ignorance and realize far too late what we were complicit in.

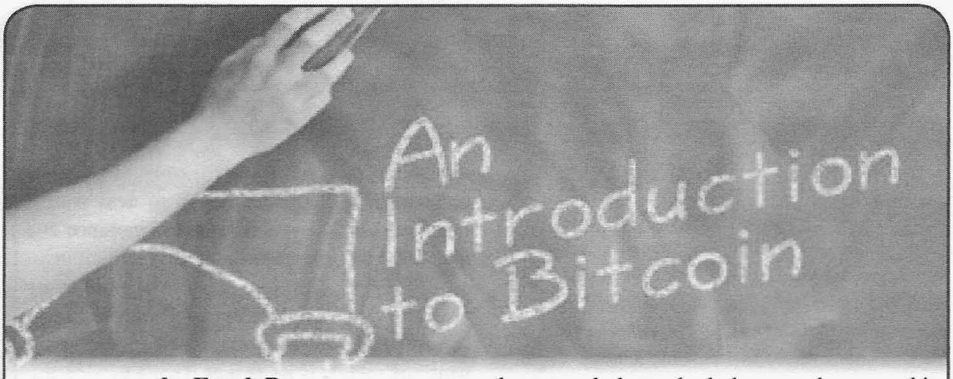
Of course, this flies in the face of every powerful entity on the planet and we can expect severe reactions from those who realize their world of secrets is in danger. That's why courageous people like those named here are so valuable and must never be left unprotected. Once it becomes clear that information will indeed be free by default, meaningful dialogue and actual change will become possible. That simply cannot happen in the current covert atmosphere.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for October 1, 2013. Annual subscription price $27.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, St. James, NY 11780.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780
4. The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.
6. Extent and nature of circulation:

	Average No. Copies each issue during preceeding 12 months	Single Issue nearest to filing date
A. Total Number of Copies	33063	31750
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4356	4255
2 Paid In-County Subscriptions	0	0
3 Sales Through Dealers and carries, street vendors, and counter sales	27506	26500
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	31862	30755
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	147	145
2 In-County	0	0
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	1054	850
E. Total free distribution	1201	995
F. Total distribution	33063	31750
G. Copies not distributed	0	0
H. Total	33063	31750
I. Percent Paid	96	97

7. I certify that the statements made by me above are correct and complete.
(Signed) Eric Corley, Owner.



by Frank Buss
fb@frank-buss.de

Bitcoin is a digital peer-to-peer currency, created in 2009 by Satoshi Nakamoto. Or, as Dan Kaminsky phrased it in a good *Wired* article: "Bitcoin's a dollar bill, with a teleporter built in." [1] Payments are made to addresses, a 33-letter length public key. You can send money from address A to address B, if you know the corresponding private key of address A.

Compared to paper money, it has many similar features. First, you really own your Bitcoins, like money in a wallet. The standard Bitcoin-Qt client program has a virtual wallet, which you can backup to a thumb drive or upload to some Internet server (the wallet can be encrypted with a passphrase). A wallet is a set of addresses, with the associated private keys.

There is no central authority who can stop you from spending or receiving money like we've seen for bank accounts in the Cyprus crisis. And, like paper money, Bitcoin transactions are non-reversible. If you buy a hot dog, usually you can't return it and get your money back. The same is true for Bitcoin. If you transfer Bitcoins to someone, you can't get them back (unless the receiver sends it back to you). This is different from PayPal or banks, who can chargeback money. As with real money, this has its pros and cons.

But there are also some differences compared to paper money. All Bitcoin transactions are known to all nodes of the Bitcoin P2P network. So there is no anonymous coin. Nevertheless, it is pseudo-anonymous, because common practice is to use a new address for any Bitcoin transaction. So, if Bob wants to send money to Alice, Alice should create a new address for him. When the money is sent to this address, the transaction is distributed in the network, but nobody knows who owns this address nor the reason for the transaction. A Big Brother needs to monitor all links between addresses and people to reveal the identity, like all email traffic, HTTPS shopping sites, currency exchange sites, etc. But for even more privacy, there are Bitcoin mixing services. [2]

Another important difference is the limited amount of Bitcoins. In the year 2140, all 21 million Bitcoins will be mined. Until then, there is a steady stream of new Bitcoins - currently 25 Bitcoins every ten minutes, created by the miners. The network and protocol guarantees that no more Bitcoins can be mined. This is like gold, which can't be printed by the government for free, but needs to be mined. And Bitcoin is based on cryptographic proofs. You don't have to trust someone like you have to for fiat money.

How to Use Bitcoin

First, you need a way to manage your wallet. You can use a software, smartphone, or web wallet. [3] One of the first clients, and still widely used, is the Bitcoin-Qt software. It is easy to use and available for Windows, Mac, and Linux. With a software wallet on your PC, you don't have to trust a company like with web wallets or, for example, Apple, who could delete your web wallet program from your iPhone. Once you have a wallet manager, you can create an address and receive money. Services like `mtgox.com` or `bitcoin.de` helps to find people who want to sell or buy Bitcoins. Another way to trade Bitcoins - more in the spirit of Bitcoin - but not as easy to use, is #bitcoin-otc on Freenode, where you can have a nice chat, too.

Once you have Bitcoins in your wallet, you can buy services with it, like a WordPress account or premium Reddit services. Or you can provide services for Bitcoin. No one can stop the payments, like Visa did for WikiLeaks when the U.S. government asked for it. If you transfer money, the transaction has to be integrated in the next block and verified by at least six other clients, which needs some time, usually at least the block issue time of ten minutes. You can speed it up if you add some fee to the transaction. The miners who create new blocks get the fees and the higher the fee, the faster your transaction will be processed. I've set the fee to 0.001 BTC per transaction in the settings of Bitcoin-Qt and usually I get six confirmations within half an hour.

Novel Concepts

Another interesting application is to print your own money. You can create a Bitcoin address and transfer some money to it. Then print the public address and the private address on a piece of paper. With the public address, the receiver of the paper can verify that the money is still at this address [4] and the private address can be used to transfer the money to another Bitcoin address. You should fold the paper so that the private address is not readable until unfolded. There is already a website, [6] which creates some nice bills for you. Pay attention to the implementation, because if the website receives the private key, it can steal your money. Best is to open the website, which is implemented in JavaScript on the client site, then disconnect the Internet before generating the paper wallet, then clean the cache and close the browser before reconnecting. For more paranoid users, or for larger amounts of money: Copy the JavaScript website to a thumb drive, start a read-only Linux system without an Internet connection from a CD, and then use the JavaScript program.

The same website provides another interesting concept: brain wallets. As noted before, you create your own Bitcoin addresses to receive money. The private key is a long sequence of gibberish characters nobody can remember. A brain wallet is a passphrase, which is converted with hashing algorithms to this address. So you just need to remember a passphrase and then the website creates the public and private key for you (again, you should use it offline). Send your money to the public address and, with the private key, you can send it again to another address, once you need it. This is useful for long term storage. But you should be careful with the passphrase: Everyone who can guess it can steal your money. And even more scary: Someone could create a rainbow table of all sentences of Wikipedia and, as soon as a new transaction in the Bitcoin network is generated, a table lookup can give a thief your private key immediately. So use a long passphrase, easy to remember, but not written somewhere on the Internet or in some book before, maybe with grammar or spelling errors, or names, dates, special punctuation, etc. I've created a brain wallet with this passphrase: "Frank test for 2600" (without quotations). This is a gift for the reader of this article, whoever is first. Importing a private key in Bitcoin-Qt is possible with a command line interface, and more easily with a wallet, [4] or with the more advanced, but still experimental, client Armory. [5]

But keep in mind: Bitcoin is the first P2P currency and still a big experiment. Never invest more in Bitcoin than what you can afford to lose. If someone detects a major flaw in the protocol or the cryptography concepts, all your money could get lost.

1. http://www.wired.com/➥opinion/2013/05/lets-cut-➥through-the-bitcoin-hype/
2. http://en.bitcoin.it/wiki/➥Mixing_service
3. http://bitcoin.org/en/➥choose-your-wallet
4. http://blockchain.info
5. http://bitcoinarmory.com
6. http://www.bitaddress.org

Bitcoin: The Hacker Currency?

by Variable Rush

Bitcoin is a decentralized, non-fiat currency. There is no distributing authority. It has worth and value because a group of people believe it has worth and value, the same as nearly every other currency system that has ever been devised on this planet. For example, the U.S. Dollar ceased being backed by gold in 1971. Instead, it is now backed by the "full faith and credit" of the U.S. government.

Unlike the U.S. Dollar, which only goes to two decimal places (like $0.00), the Bitcoin goes to eight, so your Bitcoin wallet could have as little as 0.00000001 BTC in it. If you convert that to USD, that would be zinc shavings from a penny.

Bitcoin is an anonymous currency and the protocols associated with its creation and distribution help facilitate anonymous transactions. Each Bitcoin user uses a wallet program. This wallet can be from a dedicated wallet program such as Bitcoin-Qt or another such as MultiBit, or even a website-based client such as the one found on `blockchain.info`.

A Bitcoin user is not limited to how many wallet programs or wallet addresses they can use. Actually, they are encouraged to use many such addresses. If a person uses a single wallet address for all of their transactions, then it could be easily seen where that person has sent their money to and from. If a person regularly creates a new wallet address, or uses a different address for every transaction, their privacy will increase since the only people who know a transaction took place would be you and the person to whom you sent Bitcoins.

Wallet addresses are a series of 34 alphanumeric characters that look like this: `16F8sVDtyGeFTjSSaSr4mwqTCgVBq82BMb` (that's one wallet address that I personally use, so if you want to throw me a few Bitcoins, knock yourself out).

How do you get Bitcoin? First, you should install at least one of the various Bitcoin wallet programs (or create an account on `blockchain.info`). I like MultiBit, as it's a lightweight client and does not have to download nearly 5GB of every previous Bitcoin transaction to date, unlike BitCoin-Qt, which downloads a month's worth of previous transactions upon first installation.

Once you have a wallet address, you can purchase BTC from an exchange such as Mt. Gox, accept it as payment for services rendered, or, if you're desperate, there are a lot of "Bitcoin faucets" and other grunt work sites that make you answer questions or watch a video or some other small thing to gain a reward of a really, really, small amount of BTC, sometimes as small as 0.00000009 BTC. Trying to earn BTC from these kinds of sites is extremely tedious and not really worth it in the long run.

The other way to earn Bitcoin is to mine it. In Bitcoin mining, you install a mining program on an extremely high-end computer and essentially have the computer crunch numbers trying to solve Bitcoin algorithms. Around the world, these algorithms are solved nearly every ten minutes and a new block is created. As these algorithms are solved, the Bitcoin network increases the difficulty of mining. Many would-be miners team up in mining pools. These pools split the BTC reward dependent on each member's computer's contribution to the number crunching.

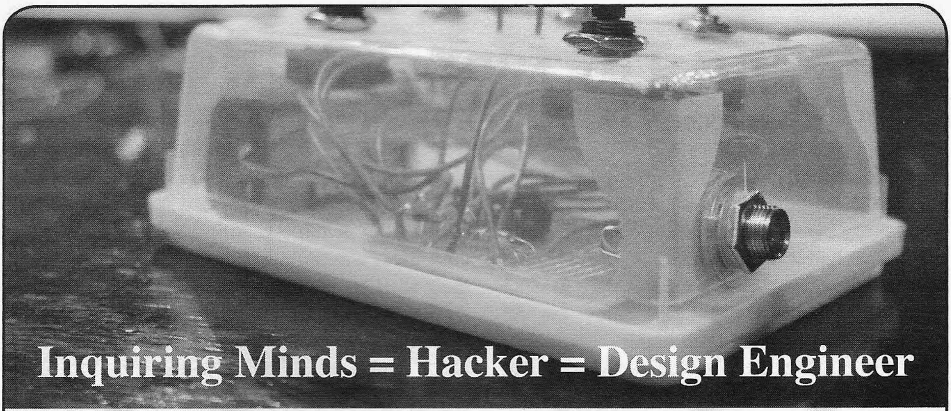
The reward for creating a new block is currently 25BTC. This amount halves every four years. When Bitcoin was created in 2009, mining would yield 50BTC per block. In 2017, the reward is due to drop to 12.5BTC and on and on until the year 2140 when the last Bitcoins will be able to be mined. There will only ever be 21 million Bitcoins. Of course, Bitcoins can be lost forever if a computer containing a person's Bitcoin wallet were to crash and there were no backups of that wallet.

The market for Bitcoins has been fluctuating wildly for the past several months. In August 2012, the price was $10 per Bitcoin. This later went up to $15 per Bitcoin. In March 2013, the exchange rate skyrocketed to an all-time high of $260 per Bitcoin before falling to around $150 as a large group of people sold their Bitcoins to take advantage of this bubble.

And that brings another negative to light. If someone had sold, say, 25BTC when the price was $260, that would have yielded that person around $6,500, a pretty impressive amount. However, the transfer from anonymous BTC to cold hard cash deposited into a bank account costs the person the anonymity Bitcoin is known for. An amount as significant as this (and perhaps even lower) when it hits a bank account can send up red flags that will put you under the suspicion of the IRS, and perhaps even the Secret Service and FBI.

Even if you manage to skate by with no problems there, your bank will report your account activity to the IRS at the end of the year for tax purposes. Whether or not, or even how, you report this income is up to you. So far, no documentation exists on any Bitcoin user that has been collared by the Feds. As even cursory readers of this magazine are aware, the less government intervention in your life, the better.

Will Bitcoin last as a currency? Who knows? Other virtual currencies may be created in the future that will replace Bitcoin's supposed dominance in the marketplace. But for right now, Bitcoin seems to be on top.



Inquiring Minds = Hacker = Design Engineer

by sarlacii

I favor hardware over software when it comes to hacking. In the commercial work of design engineering, this is often while trying to find a solution to a problem. For PJs (private jobs - anything not work-related, really) it may be hacking in a more *2600* sense. Of course, nowadays it is vital that any engineer understand how to work with software too... from high-level, OS-specific stuff, down to low-level firmware. But you can still favor one over the other!

Software hacking appeals straight-up though, as the development interface is so familiar to all of us (PC users) - another window on the desktop. The tools are also readily at hand - available for download, with examples and tutorials that you can use immediately. You install your stuff, and away you go. It's also easy to experiment, as failure is just a compilation error.

Hardware is that incremental step removed. You need physical components, small hand tools, a soldering iron, and multimeter perhaps. Printed Circuit Boards (PCBs) make entry even more difficult, unless you restrict yourself to generic project boards from EIE, Farnell, RS, or your local electronics store. You will also need to learn some theory of electricity... and how the resistors, capacitors, inductors, and transistors etc. all interact. It may seem that software hacking is easier. Initially. And only if you remain a script-kiddie.

Let's compare the two disciplines. Both fields are based on theoretical knowledge. How deep you choose to go is up to you however, as you can interact with either with only the barest knowledge - like pushing a button to make a call. Both fields make use of "blocks" to simplify the program or circuit. They can be "black boxes" too - where you have no knowledge of the inner workings, only the boundary conditions and input/output functions. Both can use PC software to aid the design process - e.g., software IDEs (Integrated Development Environment) versus electronics CAD (Computer Aided Design) packages. There are emulators and debuggers for one, SPICE simulations and hardware debugging ('scopes and instrumentation) for the other. The parallels are obviously manifest.

So, yes, there is an explosion of software driven technological change in the world today, and rooting your cell phone is made "easy" (not forgetting the skills that created the howto)... but it can be just as rewarding to hack the hardware, too. So before opting for the alluring software route, consider the shortage of hardware hackers - it can be a sweet payoff!

However, the growing prevalence of projects like Beagle Board, Arduino, and the numerous development ("dev") boards of the various IC manufacturers is, I believe, rekindling an interest in hardware. Such projects effectively provide the user with generic hardware and a simplified, "high-level" programming interface... yay for the black box approach! Invariably, however, and before you know it, you're extending the original capabilities, and you have to hack the hardware.

So, hardware is not necessarily "difficult," and neither is the learning of it more demanding than becoming a decent programmer. Besides, don't forget that the software cannot run without the hardware! Try hacking your hardware.

Hacking The Apple Collective

by Ronin

I'd like to take this opportunity to thank Big Bird for lighting a fire under me so I would express my views on the current Apple environment. I've had a lot to say and it's about damn time I said it. He wrote a great article in 29:3 about his experience with the "Genius" bar. As great as the article was, I felt like it was missing something: an inside perspective. My goal in writing this is to share with you a bit of knowledge on how Apple runs their shop, and why the retail stores make the decisions they make. I am certainly not defending Apple. I thought it would be nice, however, to have a different perspective on the mystery that is Apple Retail.

Part I: Joining The Collective

I joined Apple in November 2006 as a Mac Specialist (a sales guy) and spent two years preaching to the public about how much safer Apple computers were and how they made life *so* much easier. I quickly decided sales was not for me, but I was stuck in the position for the time being. Luckily, a "Genius" position opened up at the store I was located in. I applied and knew I was a shoe-in. I had the highest scores on the pre-test and had more technical knowledge than anyone else on the team. I worked hard to prove my worth but, alas, I was not chosen. This was the first time, but certainly not the last time, that I had a carrot dangled in front of me to make me work harder for less pay. That single instance shattered my fan-boy status about Apple. From there on out, it was a job like any other. I realized that Apple didn't care about putting the right person in the right spot. They cared about how much work they could get done with a minimal amount of pay.

Part II: The "Genius" Bar

For the record, I hate the title "Genius." It asserts the arrogance of Apple to a T. The worst part about being a "Genius" is the constant barrage of angry customers who feel like they're entitled to having something fixed or replaced free of cost. Now, this is where I would like to offer some insight on Big Bird's experience. At the Genius Bar, we are under strict orders that are issued each quarter. Those orders usually have a one or two word summation. For example: Wait Time, where our orders specifically focused on how long a customer was waiting to be seen. Another example (and my favorite) is "Getting to Yes." This gem of a slogan pretty much summed up the majority of my time at the Bar. Apple's feedback from customers was showing that customers wanted their stuff fixed, but fixed for cheap. This led Apple to drop prices of parts (which were priced at the time of manufacturing, so if you had a four year old Mac, you still had to pay $900 for a part that should be $150). This also meant that what was a clear cut price for a repair now could vary depending on how much of a hassle a customer gave you. If you quoted a customer $1000 and the customer flipped his or her respective shit, then the "Genius" was OK'd to negotiate a price that the customer felt comfortable with ("Getting to Yes"). I spent a little under three years as a "Genius" with these collective orders changing from quarter to quarter. As I was getting ready to part ways with the technology giant, orders came down again, as usual, but this time completely reversing the previous order. Instead of "Getting to Yes," it was now "Resetting Expectations." So now, instead of giving the customer the benefit of doubt, Apple didn't want to have anything to do with "Getting to Yes." The price negotiation stopped almost overnight and repair costs were lower than they were, but locked into place now. Just imagine all the happy customers *that* would bring in!

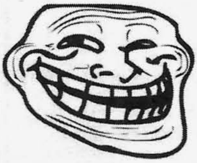
Part III: The Brain Wash

It was about halfway through my time as a "Genius" and I was burnt out. I hated the ignorant public, I hated fixing n00b problems, and, more importantly, I hated working my butt off for half the pay I should have been making with my skill set. My manager at the time pulled me aside and asked if I wanted to go to Core. Now, Core is an interesting place. Core is Apple's training camp. It's usually local to the market that the retail store is located in and the physical location is kept secret to all but those who are driving the cars full of eager fan-boys and -girls. Inside of Core is a magical world: one filled with good feelings, stories that make you laugh and cry, and an overall feeling of friendship. As a seasoned vet of the Apple Retail environment, I knew what this meant. It was time for a bit of attitude adjustment with a page taken right out of *1984*. We were fighting a war! And everyone, and I mean *everyone*, in the store had to be for the war. If not, you ran the risk of being sent to Core for an adjustment. If a manager wasn't on board, they suddenly disappeared for a weekend, only to come back with a smile on their face ready to fight again. I reluctantly agreed, knowing what this meant for me. I won't go into detail about what they did but, needless to say, when I got back to my job Monday morning, I was ready to fight for Apple again.

Part IV: The Afterlife

I left Apple because they dangled one too many carrots in front of my face. Even another Core couldn't fix how bitter and jaded I was. I was overworked and underpaid. I often compare Apple to the Borg, and myself as someone who was initiated into the collective and then successfully separated again from it. I've been out of Apple for two years now and I still catch myself saying "we" when talking about Apple, like I'm still working there. That just goes to show you that this is no joke. Is there a part of me that still wishes I was there? Sure, I miss the collective from time to time. But I've grown to think outside the Apple box. I have moved up in the world of tech, earning my Network+, Security+, and my Certified Ethical Hacker - all of which Apple did not support me learning. I have moved on to a pen testing position and use my newfound powers for good (not casting judgment here, just saying how I chose to use my skills that Apple did not support). Is there life after Apple? Absolutely - just make sure you don't spill anything on your laptop....

I hope this helps shed a little bit of light on how Apple works their magic. The reason they can afford to pay their employees the same as a Costco employee is because people *want* to work there. Some of them are so hopelessly devoted to Apple that they'd work for free if they could (I wish I was joking about that). In some ways, it makes me sad to think that the company that dared to defy a growing industry, and was a poster child of "Think Different" is now thinking just like everyone else.



INTERNET TROLLS

by Sam Bowne
samsclass.info

I was recently asked to help a colleague who had been receiving threats by email. The exchanges resulting from that, and many similar situations, led to this article.

What is a Troll?

In face-to-face discussions with friends, coworkers, customers, and sane strangers, people speak with a purpose - to deliver information, make a request, or to express an emotional connection. Civil adults learn to consider the needs of others, respecting their privacy, time constraints, and feelings. So most people are not prepared to understand trollery, and misunderstand it, because it does not occur in normal conversations.

One way to understand trolls is to think of a toddler, just learning to speak, who has discovered that repeating the question "Why?" over and over again causes an adult to keep talking forever. Another example is a filibuster, in which a legislator reads the entire Sears catalog just to give the appearance of engaging in debate. These are denial-of-service attacks - consuming the time and energy of the target pointlessly is the attacker's goal.

There is a level of good faith in normal conversation - the parties are expected to speak honestly and to have good intentions. Trolls do not have this good faith; they exploit it to harm others. A troll may ask for something, but if their wish is granted, they will not stop asking for things. They may ask a question, but they don't want an answer. Trolls are attackers, and the goal of their messages is to harm the recipient.

Defense

The only defense I know of is silence. Don't get hurt or angry and, as much as possible, give no response at all. Trolls are gratified by protests, angry denials, and counterattacks. They poke you, hoping to get a response. If they get no response, they will stop having fun, and go torment someone else.

If you must answer because the troll is a colleague or someone else you cannot completely ignore, delay the answers as long as possible. This is a "tarpit" defense and also reduces the troll's gratification from the exchange.

Notifying Police

I don't think law enforcement can do anything to stop most trolls, but there is one exception. If the troll has found your physical location and begun stalking you in real life, painting messages on your house, stealing your car, visiting your workplace, etc., then you may be in real direct physical danger. Police, restraining orders, and private investigators may be helpful in that situation.

But the actual physical danger from trolls is small. I think most of them are shy, timid, lonely recluses in real life, and wholly unprepared for real physical combat. Consider Jennifer Emick - she exposed the identity of some people in Anonymous and endures an incredible flood of trolling, including numerous threats to kill and torture her, yet none of the trolls have physically attacked her.

Getting Even

Some victims of trolling want to convince the trolls that they are wrong, or punish them. Please utterly eradicate these concepts from your mind. Trolls are failed personalities, like failed states. They have no decency, honesty, or goodness. Trolls have tormented people until they are dead, and the only remorse they show is that their toy is broken, and now they need to find a new one.

Conflict Management

A student introduced me to this excellent concept. With trolls, conflict resolution is impossible - you can never win. There is no way to make them stop, or admit you are right, or grow up, or to arrest them (except in very rare cases). However, conflict management is an achievable goal - limiting the harm the trolls do to you. That is the best goal to strive for.

The fundamental reason resolution is impossible is a lack of respect. In order to influence someone, you must respect them, and they must respect you. Trolls regard targets as contemptible and disregard everything they say. You cannot possibly gain their respect, and any respect you grant a troll just makes you a more entertaining victim.

It is essential to understand that you are at war: a malicious enemy is attempting to destroy you. Do not imagine that you are having a dispute over an issue with a potential friend. Any attempt to meet demands, soothe the troll's "feelings," or elevate the tone of the discussion will only expose you to more attacks.

The Biggest Risk

The most dangerous thing you can do when trolled is to fight back. I have been called in to help several victims of trolls, and some of the victims have hurt themselves far more than the trolls ever could. One victim resigned from employment and became a paranoid wanderer, hiding on the couches of friends while compiling large quantities of "evidence" from email headers and websites, abandoning all normal life to track down largely imaginary tormentors. Another sent death threats to the trolls, got a gun, and became the subject of police investigations rather than the victim.

Trolls love such overreactions - if they see your arrest or dead body on the news, they will laugh and say it proves they were correct all along, and seek fresh victims with renewed vigor.

The most important thing you can do is protect yourself and not overreact. Block all troll communications. Use Twitter blocks, email spam filters, etc. Maintain your own self-esteem. Ignore all troll accusations. Refuse to blame yourself.

Don't give anything the trolls say the slightest credence. They are subhuman biting pests like insects. Nothing you can say or do will gain praise from them or stop the abuse.

Just ignore them, laugh at them, and remember that they act this way because they are broken people. Trolling is their problem, not yours.

References

- http://gizmodo.com/5914671/this-is-what-happens-when-anonymous-tries-to-destroy-you
- http://www.heraldsun.com.au/news/victoria/torment-too-much-for-bullied-teenage-schoolgirl-sheniz-erkan/story-fn7x8me2-1226242170733
- http://www.theatlanticwire.com/national/2010/10/gay-teen-suicide-sparks-debate-over-cyber-bullying/22829/
- http://abcnews.go.com/Health/gay-buffalo-teen-commits-suicide-eve-national-bullying/t/story?id=14571861

Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! Another quarter brings another continent and I have now, in addition to visiting all seven continents, circumnavigated the globe counterclockwise. After a brief stop in the U.S. where I spoke at the bSides Las Vegas conference, I am writing to you from the Central Valley of Costa Rica. This is where I will call home through Christmas. My yearlong experiment in preparing for senior management has reached the two-thirds mark. When the opportunity to study somewhere with better weather than the Netherlands for the final months of my degree program arose, I jumped at the opportunity! The curriculum may be equally soul-draining here, but at least the food is better.

I have been staying in hotels a lot lately - in Brussels when visiting the European Commission, in Dusseldorf prior to catching my flight to the U.S., and in Las Vegas attending bSides and Defcon. Even my new student housing is like a hotel. The campus where I am studying was built as a resort property, but the resort failed. The student houses were originally constructed as resort villas, and there was even a hotel switchboard. This means that every student house is equipped with a phone similar to a hotel phone, in my case a Siemens Euroset 3005.

This got me thinking a lot about PBXs, and the current massive shift away from them. Have you ever noticed that phones in offices, hotels, and other institutions look different from ordinary telephones, and have features that aren't available on ordinary telephones? This is because they aren't ordinary phones. Institutions will typically install a phone system called a PBX, or Private Branch Exchange. These can provide a large number of extra features that you won't find on a regular telephone, and the list of features has grown a great deal since I last wrote about PBXs in the Autumn 2007 issue. Back then, we were starting to see VoIP based PBXs and "unified communications" entering the mainstream, but it was all very cutting edge at the time and not widely adopted. In that column, I mostly looked at the past of PBXs. This time, I'll look into the present and future.

Historically, PBXs have been sold as integrated, proprietary solutions. You would buy the PBX itself from a vendor such as Nortel, Siemens, or Alcatel-Lucent, load it up with the appropriate modules and cards providing the features you want (enabling services such as voicemail and connectivity to the phone company), run ordinary internal telephone wiring, and hook up proprietary telephone sets. These sets could run on up to three pairs each (although typically two pairs) and proprietary digital signaling would provide features such as message waiting indicators, Caller ID, and so forth. These kind of PBXs are still around, and you can still buy them. Just about the only thing that has changed is that instead of leasing a circuit from the phone company, you'll hook up your PBX to a fast Internet connection and route calls via a VoIP provider.

These days, a PBX is just as likely to be an ordinary computer as a machine that you buy from a vendor. Proprietary handsets are still around, but these have rapidly gone by the wayside in favor of SIP phones, which you can buy from any vendor because these operate according to a published standard and provide all of the functionality that most users could possibly want. Telephone wiring has yielded to Ethernet cable, and even Wi-Fi in some hard-to-reach locations. Even extensions - the tried-and-true way for decades to reach people in the bowels of corporate cubicle farms - have yielded to direct inward dials. When you can give every employee their own phone number for less than $1 per month, what's the incentive not to do it?

It's easy to wrap your head around a PBX (or any telephony solution) at the size of one site, especially if it's small to mid-sized and you don't have to worry about trunks or tie lines. Now consider the problem of large multinational corporations (such as banks) with tens or hundreds of thousands of employees and offices all over the world. Linking enterprises of this size in a secure and reliable way, while avoiding being eaten alive by circuit charges and toll charges, has always been an intractable problem. In the past, you couldn't realistically keep everyone in a company in the same telephone system or directory. Dedicated circuits to places like India and China weren't necessarily even possible to purchase (let alone cost-effective). Making matters worse, the architecture of PBX systems was generally hub-to-node rather than peer-to-peer (meaning that one site calling another site would have to route through headquarters, even if this wasn't the most efficient or cost-effective thing to do). Additionally, with very large corporations, finding PBX systems that could scale to the number of sites and employees involved could be exceptionally challenging - in many cases, impossible. Most companies ended up with a mix of different systems that varied depending upon the site, resulting in big integration headaches for telecom managers.

Meanwhile, the Internet solved most of these problems a long time ago for corporate enterprises, leaving the IT guys smugly rolling their eyes at those old crusty telecom guys who "just didn't get it." However, their smug attitudes were quickly corrected by rolling out "VoIP pilots" and making IT departments be early adopters. Until recently, the technology just wasn't good enough. VoIP was immature, not user-friendly, and didn't integrate well into existing environments (with the exception of long distance and wireless carriers, who have quietly replaced circuit switched trunks with much cheaper VoIP while raising prices in the process). Microsoft, for its part, has quietly gotten into the telecommunications business in a very big way. They have achieved a surprising degree of success selling Lync, its unified communications play (formerly known as Office Communicator) and it's becoming more and more common to see it deployed in corporate environments. Companies running Microsoft Office, Exchange, and Outlook can now add a Lync server which (more or less) seamlessly integrates with the rest of the environment. This can entirely replace an office's existing telephone system with a SIP-based solution and integrates with the existing corporate email and directory services solution (so, for example, users receive their voicemail as a transcribed email). While Lync is compatible (for now) with SIP-based phones, most users run the Lync client on a PC and talk using either the PC microphone and speaker or a headset. Proprietary handsets that break often and cost a fortune to replace are now a thing of the past.

The Lync feature set is incredibly rich, much more so than I'll detail here. These days we expect voicemail to arrive in email already transcribed and, of course, Lync does this. Sure, you can dial in to a Lync system to listen to your voicemail, but Lync can also read messages from the associated email account over the phone. Lync users calling one another (obviously) don't incur any telephone charges, because calls are routed over the Internet (or corporate WAN). Conference calls can take place over VoIP, but a DID can be assigned to the conferencing system allowing conferences to be accessed via a PIN using a regular telephone. Users (provided the administrator allows it) can very easily configure their number to simultaneously ring a variety of devices, both traditional telephone and Lync VoIP, and located anywhere in the world - making it easily possible to be reached no matter where you happen to be in the world. Administrators can select from any SIP-compatible VoIP provider and (with some help from their SIP providers) can configure preferential routes based on cost, quality, or a combination of these. Private routes can even be configured via a corporate WAN; after all, it's not technically necessary to drop off calls to the telephone system in the same country where they originated. The solution is fully video-enabled and, most interestingly, allows for remote desktop sharing.

By default, Lync users can contact one another even if they do not work for the same company - the directory is open and connected to the Internet. In fact, if a Lync user accepts your directory request, you will appear in their directory alongside all of their other contacts and Lync won't effectively flag or differentiate you as a user that definitely shouldn't be trusted. The Lync user will see all the same warnings associated with your requests as they will for anyone else. Other "stupid user tricks?" Many Lync users never dial in to listen to their voicemail (since they listen to voicemail through their email account), so they never reset the default passcode assigned by their administrator - potentially leaving the tremendous power of Lync in the hands of adept phreaks. Typically, Lync is integrated with a corporate email system and will use an email address as the contact, so a curious phreak might go "Lync scanning" for contacts. Social engineering takes on an entirely new meaning when it can include video, multinational corporations with hundreds of thousands of users, and - with the right user at the other end - taking direct control of computers (with all accompanying phun).

Microsoft, for its part, has never cared much for open standards and recently bought Skype, which is based on proprietary (but admittedly superior) technology. I expect that over time, Lync and Skype may eventually merge into a single "cloud hosted" product, which gets even more interesting. Many companies are offering "cloud VoIP" products where IT departments can outsource their entire corporate phone systems along with other IT infrastructure. For those systems hackers who have never gotten into phreaking because it's just too different, we're starting to see a convergence that might be really exciting. It's not just non-critical (or too often critical) data moving into the "cloud" (whatever that is). Entire corporate phone systems are migrating too! The opportunities for phun and mischief and exploration are already incredible and it's only just beginning.

I write a lot about older systems and how things worked in the past, in part because I think that telecommunications history is interesting and surprisingly often still relevant today, but also because engineers always seem to repeat the same mistakes in implementation. PBXs are still being produced, used, and sold more or less in the same way they always have (and they have all of the same problems), but the market is shifting rapidly (in telecommunications terms) to solutions that look more like Lync. Google isn't doing Google Voice and GChat for fun; I expect they have very big plans in the enterprise space and are still working to get the technology right.

And with that, it's time to enjoy some beer and tacos. Mexican food is popular in Central America too. Get out and explore - the world becomes a lot more interesting when you truly become a part of it!

Controlling the Information Your Android Apps Send Home

by Aaron Grothe
ajgrothe@yahoo.com

I have my Android phone set to auto update all my apps, so I know when I have to manually update an app there has been a permission change. This has never been a good thing. For instance, a game about mad avians decides that it needs to be able to read my Device ID and contacts. An application for playing music suddenly needs to be able to take screenshots of other apps. I'm already using and like these apps, so I consider this to be a sneaky way to make a land grab. What to do? For some apps you are forced to upgrade if you want to continue to use the service, as in the case of the music app. For others, you can keep running the old version until the next time you replace your phone. Another answer is to try and grab some permissions back from these apps, hopefully in a way in which they will continue to work.

Options

If you have a rooted and unlocked phone, you have several options to pull back some permissions from your apps. In this article, we're going to talk about three methods: Cyanogenmod 7's Permissions Management, PDroid, and OpenPDroid ROM modules and custom patches against the Cyanogenmod source code tree.

There are several different ways of altering the information that an app running on a smart phone makes available. Typically, you will either deny the access or alter the data that is sent from the phone. An example of altering the data is sending a random Device ID instead of your real Device ID or a fake latitude/longitude instead of your real one. You can also have the system block the access.

Cyanogenmod (CM) 7 provides an easy way to revoke privileges through the Permission management. This feature has been removed from CM 9 and later. Many poorly written apps will do a Force Close after being denied a privilege, so this feature is not being brought over to newer versions of Cyanogenmod.

PDroid and OpenPDroid offer you a bit more control over permission management than Cyanogenmod as they intercept requests and for many of them, such as a Device ID request, can either return a random or user chosen value. Returning a value allows a lot of apps to continue working instead of just doing a Force Close. You'll need to create a custom module for the ROM you have installed on your phone. You'll also need a GUI for controlling the module. The preferred GUI for controlling permissions is PDroid Manager.

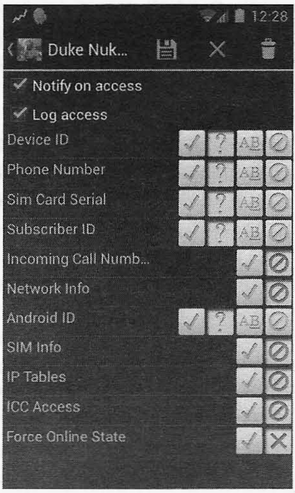
Cyanogenmod's source code is also available and there are patches out there that allow you to modify the source code tree to do things such as return random Geo location, Device ID, Android ID information, and so on. After incorporating these patches, you can build your own custom ROM and install it on your smart phone, and the phone will always return either random or user chosen values compiled into the ROM. The major problem here is most of these patches are all or nothing. Having mad avians not know your latitude and longitude is fine, but for Google Maps it is kind of a pain for them to think you are in Forman, North Dakota unless you are.

Example

The following is a quick example of restricting an application's permissions using OpenPDroid and the PDroid Manager. The app chosen was Duke Nukem 3D. This was chosen because it is a game I play every now and then, and it shouldn't need to know my phone number anyway.

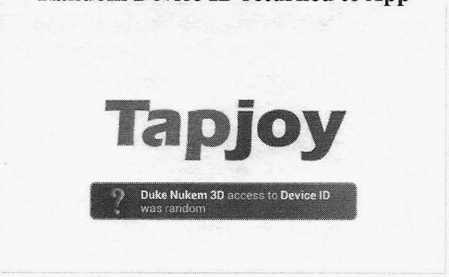
For this example, I used a pretty simple policy. If it is possible to set it to random (Device ID, phone number, etc.), set it to random, otherwise set it to deny. I also set it to log and notify for access requests. Here is a quick screenshot of the full permissions for the application.

With this policy, you'll see several notices as the application starts up as follows:



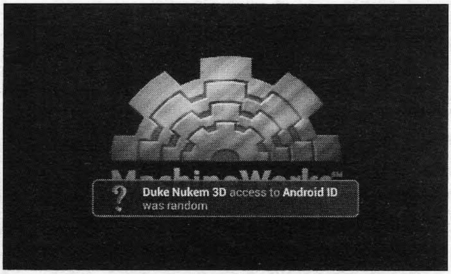
☑ Notify on access
☑ Log access
Device ID ✓ ? AB ⊘
Phone Number ✓ ? AB ⊘
Sim Card Serial ✓ ? AB ⊘
Subscriber ID ✓ ? AB ⊘
Incoming Call Numb... ✓ ⊘
Network Info ✓ ⊘
Android ID ✓ ? AB ⊘
SIM Info ✓ ⊘
IP Tables ✓ ⊘
ICC Access ✓ ⊘
Force Online State ✓ ✕

Random Device ID returned to App



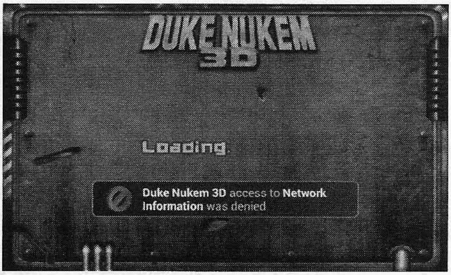
Duke Nukem 3D access to Device ID was random

Random Android ID returned to App



Duke Nukem 3D access to Android ID was random

Network Information access denied



Duke Nukem 3D access to Network Information was denied

After this, the game seems to run pretty well, with minimal information handed over!

Hints

The following are a couple of hints that will hopefully make your experiments go better. These are all based on my personal experiences and your mileage may vary:

- Use a Cyanogenmod ROM instead of trying to use the ROM that came with your phone. I've been able to create modules for some stock ROMs, but have had better luck with CM ROMs.
- If you use Cyanogenmod's Permission Management to remove privileges from your phone, a lot of your apps might do Force Closes. This is why PDroid/OpenPDroid tends to be a better solution.
- Use ClockworkMod ROM Manager to flash/backup/restore your phones. This will save you countless time.
- Every five minutes spent in the XDA forums will, on average, save you an hour of frustration later.
- If you have an HTC device, you can unlock it using the HTCdev site. It is a lot easier than having to downgrade your phone to a vulnerable ROM to get root access on it.
- Use auto_patcher to generate modules for PDroid and OpenPDroid. You can do it by hand, but it isn't worth the pain, except as a learning experience.
- Permission restriction can be a bit of trial and error. Start with very strict and, if the app Force Closes, you can give it back a few permissions until it works again.
- If something goes wrong on your phone when you install your PDroid or OpenPDroid patch, you can either use the restore zip file or just do a fresh reinstall of the original ROM.
- I prefer OpenPDroid as I have had better luck getting working modules with it than PDroid. Your mileage may vary, though. Depending on what Android version you are running, you might have to use one or the other. They both largely work the same, so if one doesn't work for you, try the other one.
- If you want to get a quick summary of the permissions that you have given away on your phone, I recommend you give PermissionDog a quick install. It provides a high level summary of some of the more dangerous permissions you have already probably allowed apps on your phone to have.

Conclusion

The next major step in terms of privilege control on smart phones will probably be done using virtualization. If you run Android inside a VM, you can intercept the calls to the hardware and provide the guest operating system whatever values you want, with the guest operating system being none the wiser This is going to require more power than most smart phones have today.

The design of Google's Android with its relatively granular permissions and open source nature allows for people to get some control over what information is sent from their phones. This is by no means a foolproof way of restricting apps from sharing your information, but it is a very good first step and hopefully these solutions will continue to evolve and get better.

Resources

auto_patcher - http://forum.xda-dev➥elopers.com/showthread.php?t=➥1719408 - tool that makes it easier to generate zip files for installing PDroid and OpenPDroid. It can also do a lot more. Well worth a look.

ClockworkMod ROM Manager - http://➥www.clockworkmod.com/ - makes doing restores/backup/updates as easy as it can be.

Cyanogenmod - http://www.cyanogen➥mod.org/ - alternative firmware for Android phones and tablets based upon the Google Android releases.

HTCdev - http://www.htcdev.com - HTC is allowing people to unlock the vast majority of their phones. If you have an HTC phone, this is very nice.

OpenPDroid - http://forum.xda-dev➥elopers.com/showthread.php?t=➥2098156 - developers of the OpenPDroid kernel module.

PDroid - http://forum.xda-dev➥elopers.com/showthread.php?t=➥1923576 - developers of the PDroid kernel module.

PDroid Manager - http://forum.➥xda-developers.com/showthread➥.php?p=34190204 - GUI front end for managing permissions with PDroid or OpenPDroid installed.

Permissions Dog - https://play.➥google.com/store/apps/details?➥id=com.PermissioDog&hl=en - great app that provides a lot of information about the permission settings on your phone.

XDA Forums - http://forum.xda-dev➥elopers.com - the place to go for more information and troubleshooting on issues with permissions.

U-verse Networking

by Uriah Christensen

I work in technical support for AT&T Business U-verse. I switched from working with consumer accounts to business accounts because I like solving real problems. I was also burned out of having to tell someone to change the input settings on their TV to get the U-verse to "work." The technology and the way U-verse works is quite interesting and has much potential for the future of Internet-based media. However, this article is not about that. This article is a basic description of how to set up a network and correctly configure it to connect to U-verse.

The reason for this is that I have found many IT personnel are clueless when it comes to connecting a network to an Internet gateway. I'm not sure how many people in the IT field that this article refers to will actually read it. If you have used U-verse as your Internet provider and have no issues with setting up your internal network, feel free to skip this article. Or you can keep reading and may learn something that didn't occur to you before. I find this info will be considered Networking 101 for most, and am shocked with the IT people calling in and saying AT&T messed up their connections, when just about ten minutes of configuring would get them back up and running.

The first thing I would like to let everyone know is that U-verse is a VDSL connection. Basically, it is a different frequency that allows for more data to be sent down the line then traditional ADSL, and an ADSL modem will not work or authenticate. Also, the authentication is different with U-verse. Traditional ADSL uses PPPOE, while U-verse Uses 802.1x certificate authentication. The modems cannot be put in bridge mode, and the DHCP cannot be turned off.

So how does a person connect a router to the modem? Simply put an Ethernet cord from the modem's built-in four port router to the Internet/WAN port of the router. Simple, right? Not quite. The next thing you need to do is set up the subnet correctly. Many routers (including the U-verse modems) have a default private IP address range of 192.168.1.0/24. The default gateway on most routers is 192.168.1.1, and the default gateway on the U-verse modem is 192.168.1.254. Now, if your devices see a gateway of 192.168.1.1, and the router sees one at 192.168.1.254, then the router will look for that IP on its subnet, and the router will also get two IP addresses on the same subnet: 192.168.1.1 and 192.168.1.64, for example. Since these are showing the same subnet, where will the traffic be sent? This will cause some major routing issues, so we need to set things up differently.

Since I hate to tell customers to reconfigure their entire network, I have a simple solution. If you have ever done some checking on a cable modem's connection settings, you know that they usually have a private IP address of

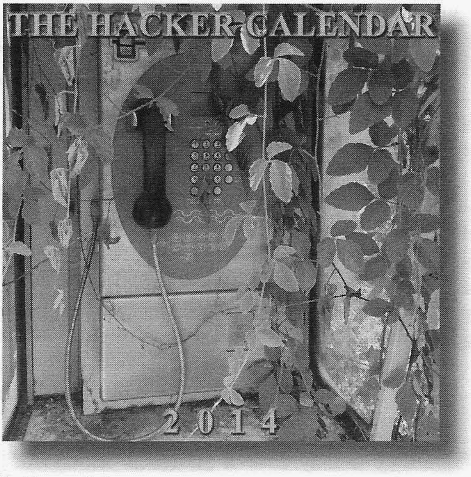
192.168.100.1. This corrects the IP address issue. I simply have the customer log into the modem and have them change the default DHCP to 192.168.100.0/24. This two minute fix corrects most of the issues that come my way.

The next complaint I get is that there is no bridge mode on the modem. Due to the authentication, you cannot have bridge mode because the device that you would bridge to could not authenticate on AT&T servers (I know, don't make an argument about how one could technically do it if they wanted to. I have also come up with some ways, but that is not the point of this article.). The question is, what is the point of bridge mode? Well, it's to give your router the WAN IP address and let your router handle the routing down from there. This can be done by either using DMZplus mode on the 2wire models or IP Passthrough on the Motorola models. Bridge mode is not needed to pass the WAN address. Bridge mode is needed to pass the ADSL signal to a second device that can handle the authentication. Unfortunately, many seem not to understand what the difference is.

The last complaint I get is that you cannot turn off DHCP. I get this so much that I really would like to tell them to hold, then throw myself out the window and plummet to my death! One IT person told me that she needed to turn off DHCP on the modem. I just blinked (I wish they could see my face over the phone) and asked a question: "Why?" She actually thought that the modem would hand out IP addresses to the devices on her router's subnet. I had to explain that the modem will hand out IP addresses to the devices connected to it, and her router would handle the addressing of the devices connected to it. To have to explain this to IT professionals is one of the most annoying things to me. Certification is no substitute for competence!

There is one other topic I would like to discuss. That is static IP addresses. You can have a block of static IP addresses for a low monthly cost. The first thing I would like to say is that I have no idea why AT&T calls them "static." These are assigned by the DHCP server in the modem and are dynamic by default, unless you statically assign them on the device you want to have it on. They are public IP addresses, and you set them up as a subnet in the modem. Once you assign the IP to a device, you can go to `http://whatismyip.com` and you will see that IP pop up. Also, since it is a subnet, the WAN IP assigned to the modem is different than the default gateway address for the public block. This confuses many customers, but when you explain that the same thing happens when you see a WAN IP of, say, 68.2.135.x and a gateway address of 192.168.1.1, as you would on most routers and that it's the same thing with the public subnet, the light dawns!

My hope is that this article will help with understanding basic networking and how to implement this with a U-verse connection. It isn't that hard, but for some reason I get calls from IT professionals that have no idea of basic networking concepts. My rant is this: I don't care that you crammed for a week to get certified! I don't care how long you have been in the field posing as an IT professional! I'll say it a second time: certification is no substitute for competence! Play with the equipment! Learn the equipment! *Hack* the equipment! Only then are you qualified for the job! I spend my time practicing these basic concepts, playing with my routers, and writing programs. I hack so I can do my job better, and so should you!



CENTRAL BANK OF NIGERIA

PRESS STATEMENT ON ADVANCE FEE FRAUD/SCAM

DON'T BE FOOLED!! MANY HAVE LOST MONEY!!

IF IT SOUNDS TOO GOOD TO BE TRUE THEN IT IS NOT TRUE!!!

[illegible]

CENTRAL BANK OF NIGERIA

[illegible]

Scamming the Scammer

A Fun Way to Respond to a 419 Scam

by the Piano Guy

I had an experience today that may be instructive on how to deal with scammers. Someone tried to make me the victim of a Nigeria 419 scam. I didn't fall for it, and instead got to scam the scammer. As a student in IT security and information assurance, this felt good to do.

As you would expect, all names have been changed to protect the privacy of everyone involved. My friend's name isn't Matt, my folks weren't prescient enough to name me Piano Guy, and the scammer wasn't named "[Scammer Replaced Name]." Prosecutions are underway through Homeland Security (no joke), so privacy is required.

A few days ago, I was asked by a friend to re-friend him on Facebook. I figured that he had a problem with his account, so I did. The next day, I saw a post from him wondering why he had been getting questions from people about him re-requesting to be Facebook friends. Now, I like this guy, but it isn't like we talk every day, so I didn't make the connection. In reality, I should have questioned the re-friend request. The lesson I learned from this is that if someone you think you are friends with on Facebook re-requests your friendship, look them up and see if you're currently in their friends list. If you are, that second request is from someone else who has cloned their account.

Today, while sitting home looking for more computer clients, I got a chat from the scammer.

12:00 pm
Hello Piano Guy
how are you doing today?
12:00 pm
I am doing well. How are you doing today?
12:01 pm
I'm okay but not too well here.
I am sorry I didn't inform you about my traveling for a Program called Science, Health and Environmental Reporting.
It is currently held in Nigeria, Sweden and Kenya. I am presently in Nigeria.

At this point, I knew for sure someone was trying to scam me. This friend in no way, shape, or form would be in a position to do this. I looked up his number so I could call him and confirm he was home.

12:01 pm
Seriously?
I had no idea.
12:02 pm
Yes!!!
It has been a very sad and bad moment for me because i got robbed on my way to the hotel where i lodged.
My ID, cash and other valuables i have with me got stolen, I contacted the embassy here to help me out but it will take some time to get back to me.
12:02 pm
Really? Are you there alone?
12:02 pm
yes
12:03 pm
Wow. That's horrible.

I reached the friend on the phone. He told me about having had his profile stolen on Facebook, and that they could do nothing about it. He was fuming.

I decided to see if I could roll with it, and eventually turn it around on the scammer. Now, this is a dangerous game I chose to play, because the scammer could decide to target me and my friends next, but I use real passwords so I feel somewhat safer than maybe is justified.

12:03 pm
Yes, i'm in a critical condition here right now
I urgently need your financial assistance of $600 to sort-out my hotel bills and get myself back home.
I will really appreciate your help and i promise to pay you back immediately upon my return.

No one is getting from Nigeria to the U.S. for $600, let alone sorting out hotel bills as well. Further, my friend is a grammatical purist, and I would never see an "i" from him in any correspondence. I'm still playing along....

12:04 pm
I know you're good for it.

12:04 pm
you could have it sent via western union now so i can pay off some old bills and get myself back as soon as possible

12:05 pm
I suppose I could do that. What do I need to know?

12:06 pm
all you need to do is to look for the nearest western union agent close to you and have the money sent from there
okay?

I wanted to see if I could get his contact information.

12:06 pm
I suppose I could do that, but I don't know where to send to YOU. I can't just tell them to send to my friend Matt because he is in Nigeria.

12:08 pm
okay, i'll give you my friend info here to send the payment to now. okay? he'll help me receive and give me the cash because my id and other valuables got missed too. Okay?

12:09 pm
Okay, but I'm going to want to call your friend on the phone, so I'm going to need a phone number to reach him at.
I'm concerned about you.

I'm stalling for time and trying to get more information. My friend calls back, and tells me that if I look at the profile I will see that it is really https://www.facebook.com/Scammer.ReplacedName.5, which has nothing at all to do with my friend's name. I realized that I could see this myself if I clicked on the link on his name that was in the chat window, so I checked and, sure enough, that was the URL.

12:10 pm
i know, it's just a young college boy in school here, just borrowed his computer, he doesn't have a phone because i just asked him now.
I'll be fine...Okay?
here's the info ...

I should have waited here for him to give me the information, but I jumped the gun a bit.

12:11 pm
Also, what hospital are you staying at? And, what is their phone number? I'll wait. I know it will take you some time to track down a nurse to get that information. Get the international code too.

12:13 pm
i'm not in a hospital now....i wasn't hurt bad at all, just stole everything from me. I'll be logged off soon so please we need to make the fast how soon would you be able to send it to me?

12:14 pm
I can do it this afternoon. It's already after 12 here. I need to have some kind of other verification. If I send the kid the money, what's to say that he won't just keep it, and then you're still screwed?

12:15 pm
trust me, he won't..okay? you can mark my words on this

12:15 pm
Okay, what is his contact information?

12:15 pm
wait please
Receiver's Name: PETER KEN
Address: 32 araromi street
City: Ojota
State: Lagos
Country: Nigeria
Zipcode: 23401
did you get it?

I had the information I wanted, so it was time to lower the boom.

12:17 pm
I got it. I do have a question for you.....who is [Scammer Replaced Name]?

No response for four minutes... it was a long four minutes for both of us.

12:21 pm
have to go now, not mentally balanced here

That was an understatement.

12:22 pm
wait please
i should be able to get back online as soon as possible, need some rest here. Okay? As soon as you have it sent, you'll be given some info, kindly reply back with the Full Sender's Name, MTCN, Text Question and Answer used and the Amount Sent. As soon as i get that, i'll be able

to make communications and get back to you immediately.
Okay?

Now that he had the nerve to come back, it was time to scam the scammer. It is okay to lie to a liar....

12:23 pm
What does MTCN mean?
I gotta come clean with you. I'm also from Nigeria. I'm scamming The Piano Guy, just like you're scamming Matt. How many people have you gotten to send you money on this account?
12:24 pm
what do you mean
12:25 pm
I know you're not Matt. I can see it from your web name. I dropped a big hint when I asked you who [Scammer Replaced Name] was. That's YOU. How much money have you made off of those American suckers?

Shortly after that, I went to put in a fraud complaint (which can be done with the gear in the chat message). I couldn't. He had already deleted the page.

Problem solved. But, we're not done yet.

I decided to look up that name. [Scammer Replaced Name] isn't exactly John Smith. It turns out that there is a person from Jackson, Mississippi that has that name, and no one else in Facebook or Google does. This led me to call the detective bureau there, which led me to the Attorney General's office. They have directed me to the Department of Homeland Security (DHS), who is processing this. I do understand that this person could either be a perpetrator or a victim of identity theft but, either way, the matter should be investigated. All they have to do is look at this person's computer logs, and we may have taken a scammer out of the Internet pool (if they are the scammer), or may lead to logs that will help DHS find the real scammer.

Lessons to Learn

- Don't re-friend someone on social media sites that you are already friends with unless you check it out carefully.
- It is okay to get information from the scammer to try to figure out what is going on, but do not give them more information about you, no matter what. And, if your own systems aren't secure, expect to be attacked back by someone like this, so don't play in that arena.
- Realize that there are people out in the world like me who will see this as an extra credit school project or others who will see you as a person to target back. Knowing how to hack, understanding how things work, and the like is very cool. Using these skills for bad purposes can get you hurt and can land DHS on your doorstep. Just as Spidey's uncle said, "with great power comes great responsibility." Play safe and legal out there.

The Art of War and What IT Professionals Can Learn from It

by Rick Conlee
rick.conlee@gmail.com

Having been in the IT community and its seemingly infinite capacities for the better part of 12 years, I can say that I have seen my share of triumphs and disasters. I run a small IT management company in Albany, New York - and I have between two and three subcontractors working for me at any one point in time. Our footprint compared to the larger MSPs and VARs in our area is comparatively small. When we sign on a new customer, they always ask how we are still around - referring to the large shadow cast by our competition.

When I was a student in college, one of my favorite books that has shaped who I am today both personally and professionally was (and still is) *The Art of War* by Sun Tzu. There are hundreds of translations and variations of this book, but the core text written by Sun Tzu himself back in 500 B.C. is very short and simple to digest. It is divided up into 13 chapters detailing the key aspects of warfare and how one might employ tactics and strategy.

The author fought in the Wu-Chu war back sometime around 500 B.C. and was given a small fighting force of around 30,000 to 40,000. His opponent, Nang Wa, was able to field forces of one million or more and had a huge manpower and financial advantage. Think of Nang Wa as your largest competing MSP or VAR. They are big, well-funded machines that could seemingly curb stomp you in one business quarter. Sun Tzu won that war and, in doing so, he demonstrated a principle that he documented in his writing, and was studied by many famous battlefield commanders. That principle was his emphasis on light forces being able to maneuver. In the 20th century, that principle was put into play by people like B. H. Liddell Hart, Heinz Guderian, Erwin Rommel, George Patton, and Norman Schwarzkopf. Liddell Hart wrote a study on the usage of mobile armored forces being able to maneuver rapidly against larger forces. He wasn't taken seriously in Great Britain, but two people who did take him seriously during the 1930s between World War One and World War Two were Heinz Guderian and Erwin Rommel. Blitzkrieg as we know it was born during that time. When the Germans took on the stronger, well equipped Polish and French forces, the world stood in absolute shock while the sound of squeaking tank tracks and the spine chilling air horns fitted to Stuka dive bombers screamed out of the sky on targets all over Europe. It must have been a horrifying experience. Since then, there has been an emphasis on teaching maneuver warfare at military academies all over the world. Innovative ideas, rapid decisive movement, and cutting edge technology win battles and wars. But what about small IT companies? How can they benefit from the teachings of Sun Tzu's *The Art of War?*

The passages in the book have a very general appearance and can be seamlessly applied to just about anything. One example comes from the "Tactical Dispositions" chapter in the D. E. Tarver version: "What the ancients called a clever fighter is one who not only wins, but excels at winning with ease." Notice how it is short and sweet, but yet so powerful and wise in its delivery. The slant from that passage can be applied universally throughout your life and dealings. In the case of being an IT pro, that passage can mean many things, but where you can apply that wisdom with great success is being able to take a disastrous situation (the infamous BSoD on a desktop/laptop) and turn it around, all the while making it look like a cake walk. You probably do that already on a day to day basis. In doing so, you just became a god to your customer/user/brother-in-law and they will praise your skills to their associates, thus generating some great word-of-mouth and, in many cases, more income.

The world of IT is much like war. You spend time fighting problems, clients' poor technology decisions, and other firms trying to invade your turf. By being a smaller IT shop, you can be more dynamic. Your business decisions are put against real time where bigger firms can sometimes have leadership teams that will go back and forth on critical business decisions, sometimes for days on end. Sun Tzu says: "the good fighter will be terrible in his onset, and prompt in his decision." If a business decision takes more than a day, someone else has taken the initiative so, as in the previous passage, you must be deliberate and timely in your decision making process, and rapid in execution.

Another great passage worth including is: "Let your rapidity be that of the wind, your compactness that of the forest." Equipping yourself with tools like VNC, SpiceWorks, or Splunk can give you rapid easy-to-deploy access to a client with the ability to collect intelligence on a remote system and will allow you to resolve problems quicker than having to go on site, driving down service delivery and resolution, therefore leaving more time in your IT shop to focus on the core business, and expanding your profit margin. Mobility in service delivery is a must and cannot be overemphasized.

In conclusion, if you don't already own a copy of *The Art of War*, I highly recommend you get it (there are free versions of just the core text in epub and mobi formats, as well as online at `http://classics.mit.edu/Tzu` `➡/artwar.html`). In my humble opinion, if you are starting an IT business, this book is a must read.

Access Tandem Codes and the Hidden Phone Network

by Brandon

There are many, many secrets in the phone network, but few as well kept as the access tandem codes. These date way back - maybe even to the time when direct dialing first appeared.

So what are access tandem codes? Simple! An access tandem is a machine in the local phone network whose main purpose is to connect you to long distance networks or other local offices with subscribers. So an access tandem code, quite simply, is a code that points on that equipment. The format is pretty straightforward. For example, a call to the access tandem in Des Moines, Iowa is reached by dialing 515-089 and any last four digits. So basically, an access tandem code is a phone number beginning with zero. Since this is supposed to be unheard of, dialing can be a bit of a challenge. So we'll cover some of the ways we've found to circumvent the traditional restrictions.

From a mobile perspective, AT&T's non-prepaid network or a Sprint phone will usually just place the call, no questions asked. If you happen to be using Sprint, regardless of the kind of phone you have, sometimes they'll route your call to things within an access tandem code other than what you intended to call.

Dialing these codes is also a pretty straightforward task on a landline, but how to go about doing it depends on the kind of switching equipment that runs your phone line. A switch is a host to a telephone; all your phone does is convert audio into something you can use. Everything that makes your phone a phone is part of the switch. Anyway, DMS-10s and EWSDs will occasionally just let these calls go straight through. Fortunately, if you aren't served by one (`http://www.telcodata.us/➡search-area-code-exchange-➡detail` will let you know with reasonable accuracy what's running under the hood) or if your switch isn't cooperating, there are a few ways of circumventing the block. The first method has the most success on DMS-100s and GTD-5s; if you know what the carrier access code is for your carrier, stick it in front of the call. For example, if you were using Sprint, dialing 101-0333 before the number would get you around the restriction. Your switch tacks this code onto all your long distance calls, so it's something that'll be part of your phone account. It's not known exactly why this is, but a GTD-5 is known to block access tandem codes on three-way attempts.

The next way is a little weirder. Some carriers have long distance equipment that's programmed to allow you to get a dial tone from it if you're a customer. Using Sprint as an example again, dialing 101-0333# will give you a 400 hertz tone from the equipment. From there, you're free! Your switch has no say in what you're calling. Well, for the most part. A lot of the long distance network isn't provisioned to directly deal with toll-free or some other numbers, so if you choose to try anything that isn't a normal number, some odd things can happen.

Some Voice over IP providers do allow this sort of traffic to slip by - more specifically, some of the shadier ones. Let me explain - when you make a long distance call, your carrier has to pay termination fees for every minute you're connected. In rural areas, this can be higher then a couple of cents per minute, so they could be losing money every time you call rural America. To get around this, some of them buy minutes from people who literally just have a bank of phone lines with unlimited long distance accounts. That way, the carrier who actually connects the call is stuck paying those fees, and sometimes they just happen to let these slip by. Since routes are different for different areas, this doesn't work consistently, but it's common for routes to change frequently, so you could get lucky. Occasionally, some Voice over IP routes will work with Centurylink's 958 codes, but you may hear an error message before they go through. Just keep waiting - if a route to them is available, you'll get it eventually.

If all else fails, the absolute easiest way to dial access tandem codes is to just get a calling card. The AT&T ones sold at Shell stations work pretty much universally for access tandem codes. The 959 codes near the bottom of this article also work on AT&T cards. The one thing to watch out for, though, is the fact that instate calls will cost more (the polar opposite of IDT's cards actually, which we'll cover in a sec). You might want to have an out of state friend three-way it in occasionally.

The other card I've found that works is anything from IDT. So long as you get something with their logo on it, I don't think it matters what you get; it all goes to the same platform. This company is so shady, it's hilarious; they're the ones with machines in airports peddling ten dollar cards worth 20 minutes. For those of us not trapped in an airport, the price is reasonable, but the caveat for these cards is they work pretty much like the Voice over IP method; they're simply just hit and miss. My experience has been they change their routes almost every week, though, so it could be worth a shot. Dallas (214-040-xxxx) is the one exchange I've seen work most with these cards. IDT cards do, as of the this writing, also work with Centurylink's 958 codes, covered near the end of the article.

So what do they actually hide on an access tandem code? Perhaps most ubiquitous (and rightfully so, it's one of the most used things in an access tandem code) is the inward operator. An inward operator is just what it sounds like - an operator for operators. Technically speaking, the console they're using is exactly the same, but their main function is to butt in on phone calls. Not for surveillance (CALEA equipment pretty much covers that), but like an aggressive form of call waiting. Here's how an average conversation will go when you want to perform an intercept on, say, a call in Seattle:

(dials 206-033-1210, the routing code for Seattle inward)

"Inward"

"Yes, can I have an intercept on 206-555-1212, please?"

"Certainly, could I get your name?"

"Bob"

"Please hold" <as the operator calls out to the distant number, you can hear a blip of their call before silence>

Then the operator will ask the called person if they want to interrupt their conversation in the name of Bob. If there's silence or a sound other then a person talking, the operator will let you know what's going on before telling you to try again later.

Easy, huh? You can also ask them to do busy line verification! Sounds exciting, I know, but if you're up for a challenge, there's another thing these operators can be used for: phantom traffic. I'll leave it to your imagination as to how you ask for this, but when you make a phone call, there's a *lot* of data that's sent with it; your number is sent in two different fields, the switch that makes the call inserts a number to identify it with, the kind of phone you're calling from, where your call was forwarded from (if applicable), and if any more forwards are acceptable - basically, it's a mess. Phantom traffic is the phone equivalent to Tor; the only thing associated with the call is a destination number.

Another thing you'll find a lot of are 10x tests. When you find these in the wild - on access tandem codes at least - they're laid out very evenly; the last four digits will usually be xxxy, where y can be any number, and x corresponds to the test number. Like a lot of things run by phone companies, the names of the tests make no sense, so let me explain.

100 - Starts out with a 1004 hertz tone and goes straight to silence.

101 - Rings a phone inside the switching office.

102 - This one is like the 100 test line, but after a few seconds of silence, the tone repeats. And goes back to silence. And repeats....

103 - These generally are only accessible in very rural parts of the country, like towns with populations in the triple digits, or Alaska. It's otherwise known as a supervision test; it picks up and hangs up the equipment making your connection repeatedly, often making what's referred to as bit robbing noise as it does.

104 - To be honest, I'm a little in the dark as to what these do. They pick up like 105 tests and wait for two digits, but the only thing I've seen them do in return is hang up. Here's how AT&T describes them:

"104-type transmission measuring and noise checking provides a test termination for 2-way transmission testing, a near-end noise measurement and far-end noise checking. This termination may be used to test trunks from offices equipped with automatic trunk test frames. It may also be used for manual 1-person 2-way transmission measurements from a test position."

105 - These are kinda neat. It'll pick up with a 2200 hertz tone, and start waiting for digits. Different digits will give you different combinations of tones and noise back (protip: try one digit at a time). There's a lot of different variations from one manufacturer to the next, but 0 universally indicates a request to hang up. Some of these are run using real hardware, and will break in interesting ways - 928-055-1050 is a good example of this.

108 - Echo test, or loopback, as it's officially called.

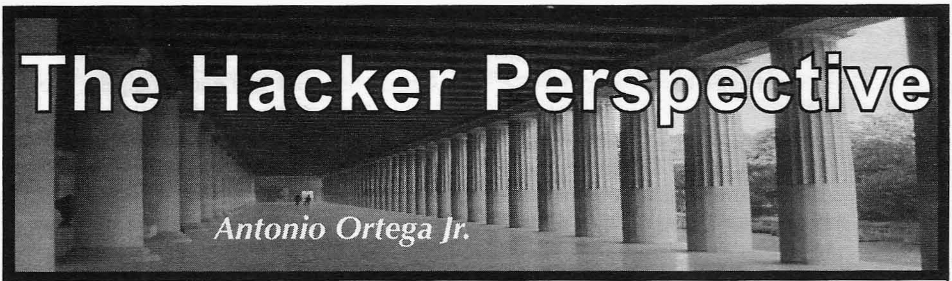
Lastly, you can find recordings. Sometimes you'll find a recording meant to indicate a dialing error, like 612-076-1259 or 602-051-5200. Other times they'll be things meant for employees, like 410-040-9400. In this case, a gruff voice simply says "Non verifiable." If you stay on long enough, you'll also get an all circuits busy recording. Nothing is actually busy - in fact, it's pretty normal. The Nortel DMS family of switches (excluding the DMS-10) has a bad habit of sticking you on here whenever it feels like it.

Moving on, here's a slightly different flavor of hidden number: 958 and 959 codes! These are different in the way that as far as the public network is concerned, they don't actually exist; they're a product of the long distance equipment your provider runs - so it's a pseudo private network. The first one I'm going to talk about is also the easiest to get onto just by the way long distance carriers do business. When someone buys minutes from a provider, they're not always their first routing choice. They may not even use them for every route, so it's just stuffed into a list of networks the switch has at its disposal. When a number that's invalid is sent, some equipment will cycle through the networks, looking for one that'll accept the traffic. Lucky for us, these test exchanges are eccentric enough that there's only one that'll accept it! So the short answer is you can go ahead and dial it, and it'll Just Work. Centurylink's network has a pretty self explanatory way of routing these internal codes; for every city they have a switch in, they assign its area code and the exchange 958 to the switch. For example, they have a switch in Denver, so if your call wanders its way onto their network, 303-958-xxxx addresses the Denver Centurylink switch. Their network is relatively small, so aside from Denver, there's Seattle (206), Minneapolis (612), Salt Lake City (801), Phoenix (602), Chicago (312), Kansas City (816), Atlanta (404), Charlotte (704), Tampa (813), Los Angeles (213), Newark (201), and New York (212).

Centurylink, like any good company, most definitely has nothing to hide. Not in the 958 exchange anyway, so there's usually just one of two things you'll find there. The first is an announcement that repeats over and over to help their Voice over IP customers check for packet loss. The second, well, I'm not quite sure how to explain. A Nortel DMS switch will ring once and pick up silently. The moment that call goes off-hook, the DMS starts counting up to two minutes. If you stay with the silence for those two minutes, it'll hang up and the call will end normally. But if you hang up, that timer keeps going. If you call back before two minutes are up, it'll ring a few times and then send a message back on the call signaling channel saying the call is busy. Subsequent attempts don't ring - it'll just send back a similar message. Once those two minutes are up, though, it goes back to picking up silently. These can usually be found on the lower end of the 7000 block (7000, 7100, or 7200), while the VoIP announcement is typically towards 7600, 7700, or 7800.

I won't dwell on this much since it's been covered before, but AT&T also enjoys hiding numbers. Kinda like an Easter egg hunt! Just without any rotting if you miss something - which is an especially good thing, since this is a great example of a time when you need to balance between painstaking levels of detail and just enjoying what you hear. The AT&T network is *huge* and has more hiding places than a drug smuggler's car. So for now, let's just cover the basics. Pick almost any American area code with a 1 or a 0 as the middle digit, and then dial 959-6904. Chances are, if AT&T is handling the call, you'll probably get a scratchy recording telling you an earthquake stopped your call. Welcome to the weird, weird world of the 4ESS; AT&T's brand of long distance equipment. There's too many to list here, but for every state in the U.S., there's at least two of these, and a good number of them let you hear the strange local varieties of disaster messages among other things. These usually gravitate towards 959-6900 through 6920, while some of the tests described above sit near 959-10xx.

So there you have it! Whether it's been an excuse to kill some time on a gray day or a primer to exploring some of the other hidden parts of the phone network, I hope you enjoyed reading this.



The Hacker Perspective

Antonio Ortega Jr.

In the 80s, my mother brought home a Commodore 64. Cutting edge external 170K floppy drive technology and commands in basic introduced a ten-year-old kid to the world of computers. Reading and math were no longer new to me, but this box upset the "normal" order of numbers and letters. Commands in basic were disruptive. The promise of video games was the entire motivation of unraveling this new language. This was not only the most effective way to force a ten-year-old into typing, but gave me a clear goal. Still typing `Load *` was not hacking. It was, however, the beginning of a curiosity on the secrets and limits of what a few keystrokes could unlock. What followed was an exploration into the exciting world of making words run down the screen, having other characters run down the screen, and other thrilling combinations of white and blue results.

Finding my own way to get results was just how computers always worked in my world. They didn't do a whole lot practical except for some games. The promise of networking to BBS games was interesting as it took computers to a more social level. As fun as it was commanding a spaceship I couldn't see to a fake planet for the mining of a material I could then sell to someone I didn't know (and all in text), it did lead to boredom. Here we have my introduction into hacking. Cheating at games. Harmless and fun at first, it soon became apparent that these hacks ultimately led to me not having to play at all. Then *Doom* came and WADs went flying. Diving into mods was more interesting than the game itself. Understanding what was going on behind the graphics was part of the game experience. The BASIC code of the Commodore was gone, but the curiosity was there. The results were typical. More explosions and finding what would crash a 486.

It wasn't until the mid 90s that looking at everyone's code become an interest. Talking with the world at large about HTML code and protocols for the first time showed me that most computer users weren't interested in learning how to utilize their computers to a fuller potential. The curtain pulled back by the Commodore and *Doom* mods for me still hung for most. Interest in the enlightenment that comes with hacking through yourself was minimal. People still wanted results, but with a shortcut. For those willing and able to hack through the chat rooms and under construction banners, there was still little left to gain. The beginnings of the Internet offered little reward for hacking other than exploration. Pushing what you knew and could do with these languages and systems was its own reward. What it meant to hack for the sake of hacking, to explore how far we could impose our commands, became public. The Internet finally offered something many of those who hacked felt they never had: recognition. The awkward and nameless nerds that went to your high school had used computers to fetch a result they had little of and always wanted. Recognition for their work. Even if they only vandalized your Angelfire and Geocities sites. You knew there were hackers out there.

The term hacking was gaining ground in pop culture with the release of the 1995 Jolie movie and came to mean cheating the system or breaking and entering with a computer. This never seemed accurate to me. I was 19 and the heater core in my car broke, spilling radiator fluid everywhere and stranding my girlfriend and myself. Having only a few tools, rerouting the radiator hoses to bypass the heater core got us home just fine. I was seen as clever. Rerouting any capabilities from one computer to another was seen as a hack and shady. Obviously hackers had created all computer problems. From Michelangelo to Melissa - and clearly hackers caused your screen savers to freeze. Solutions in real life were not hacks. My applying the same logic to any problem on a PC or in my car only meant I was clever enough to be a mechanic. Computer hacking was seen as being done with malicious intention and would only result in trouble.

Hacking had a name and I didn't want anything to do with it. I still hacked. I just wouldn't draw attention to it. There was never a need to. Exploring different hacks was just what I had always done. It was a normal and entertaining way to solve problems. The self-described hackers I had contact with were searching for an identity. Even if only "cyber bad boy," it was something. If being a hacker meant some kind of computer thug or a malcontent with an agenda, then it was not what I had been doing. Finding potential and resolving issues within everything I came across was what hacking meant to me. It was a way of looking at behaviors and a deeper understanding of their ability to furnish a result. Being a hacker should have been seen as resourceful and inventive, but instead viruses and misunderstanding resulted in fear.

The stigma attached to hacking survived into the 2000s. Threats of cyber crimes like information stealing and identity theft had everyone worried about hackers and the media played up those fears. My interest in being known as a hacker were zero. My interest in hacking and the utility I gained, however, was steady as ever. My landlord kept forgetting to authorize my MAC address on the apartment Wi-Fi. The Wi-Fi was included in the rent, so I was without a service I was paying for. Some packet sniffing and spoofing my MAC address seemed the logical solution. Nobody thought me clever. Rather, I was a hacker and dangerous. The fact that I only accessed a service I was paying for meant nothing. It was a hack. What that meant to me was that I now had the Wi-Fi access that was promised me. I told my landlord I had broken in and I would cease my spoofing when he authorized the MAC addresses of my devices. After an explanation of what all that meant, he asked if I could optimize the struggling Wi-Fi network. Short of blocking MySpace, there was little to be done with his wireless network, but for once someone saw positive potential in hack. There was even talk of a small discount in rent. This resulted in my interest in being known as a hacker equaling more than zero for once.

In my life, the title hacker has meant more to those with little to no computer skills than those who could hack into a network. It means more to the ignorant public. The people I have known to perform a hack of any sort were more interested in the hack itself. "Can I" was the question asked in a hack. Can I crack my own passwords? Would this run in Wine if I did this? Could I get OSX on my PC? The general populous, meanwhile, saw hacks as a "Will they" as in will they get me. Most anyone I know, from those who know a few simple hacks to those who can get machines and software that were never meant to cooperate to play nice, have no interest in "getting" anyone. Also, the people I have known with this fear have often had nothing to "get." It's only within the past few years that anyone seeing me as a hacker has become positive. A growing number of people see the ability to hack anything as being a part of a secret world. The world exists behind a Windows logo and is only accessible in a text prompt. Movies and television reinforce this idea and the final result is me being asked if I could remotely blow up the computer of this jerk on Craigslist.

I like hacking. I have hacked into networks and hacked into accounts. I have hacked software and hardware. Never with any malicious intent. To this degree, I am a hacker. It means exactly what it implies. I am one who hacks. Never will it mean I am out to get anyone as a result.

A new generation of hackers is out there hacking away. It has been said that knowledge not earned will ultimately be abused. Jeff Goldblum's rant in *Jurassic Park* will remind you. Those with little skills and understanding beyond the use of YouTube are now able to perform hacks in minutes and on a whim. In no time at all, anyone with the motivation and an hour's patience can be a hacker on the Internet, building on information and techniques laid out before them. Having the Internet as a starting point, hacks with childish vandalism are often the results.

The power behind that label has gained value, however. More and more are willing to pay for the skills of a hacker or for protection against being hacked. In a time where your formal education level is the biggest indicator of the income you will receive, computers remain result-oriented. If you have the chops to hack or stop a hack, there is value in your skills. In my hacking to solve my problems - and often a friend's problems - potential employers have taken notice. The ability to go beyond what software Best Buy has and to get more utility from the machines and software a business already has is appealing to small business owners especially.

I have never been more encouraged to hack. Employment is finding me and friends are seeing the ability to do more with their devices - even those looking to start something new. Buzz phrases like "going viral," "Internet startup," and "search engine optimization" have planted the seed of enterprise in many and, while they dream big, they hack small. From web development to system networking to hardware maintenance, employers are looking for more than just a one trick pony.

Hacking has come around and found a new legitimacy that makes the idea of being a hacker acceptable - and in some cases even marketable. I'm now able to share the ideas of how to hack, free from the suspicion of the 90s. It means something new to be a hacker. Finally, the stigma is falling away and the truth is coming out. Hackers in general are resourceful, clever, and often very helpful. They are also a useful ally in our lives which are ever-increasingly involved with technology. Sure, there will always be punks and vandals, but the same is true in almost any group.

With new legitimacy, hacking has found new voices. Ever vigilant in her nerding, once again it's my mother showing me the way, this time turning my attention to the publication *2600* - hacking out in the open and accepted. Over 25 years after being introduced to computers, I can say I hack. After all the exploring and hacks I have attempted, admired, and had success with, it's OK to tell people. Not everyone gets what it means to be a hacker yet. Not everyone needs to. It's enough to have a place to enjoy it out in the open.

The world of hacking into anything on the screen is still as challenging and engaging as that blue screen with the white letters from the 80s that I would try to get to react in an interesting way. Knowledge is scary for some. To others it is a liberating way of life. I'm not a hundred percent sure my mother had the goal of raising a child with a tendency to hack his way through obstacles in life. I have solved problems for myself and others by knowing a few simple hacks. I have amazed and frightened others with the possibilities of a few more complex hacks. I have admired the elegance and intelligence of hacks I would have never dreamed of. All of these results are what keeps me and other hackers going. It has proven to be a better way to live.

Antonio Ortega Jr. reads comic books and codes in his spare time. He is currently working as IT support for a software company in Eugene, Oregon.

HACKER PERSPECTIVE Submissions Are OPEN!

It's been a couple of years since we've had openings, so you'd best make your submissions as quickly as possible. Hacker Perspective is a column about the true meaning of hacking, spoken in the words of our readers. We're interested in stories, opinions, and ideas.

The column should be a minimum of 2000 words and answer such questions as: What is a hacker? How did you become one? What experiences and adventures did you live through? What message can you give to other aspiring hackers? These are just suggestions - you must choose your own points.

If we print your piece, we'll pay you $500.
Submit to articles@2600.com or the mailing address on page 65.

Palo Alto NGFW Insider

by]{nightVision

With companies moving toward Next Generation Firewalls (NGFWs) and all their new capabilities, I was curious as to what really makes this different. As a hacker, the first thought is "Let's void the warranty and take a look inside!" Luckily, I was able to get a hold of one through a friend who was willing to let me find out how secure it would be for his company. To inspire others to "void warranties," I'll explain the entire process, as each investigation becomes a learning experience.

Before starting, here are some initial observations that led me down this path. The firewalls are sold as appliances and closer inspection shows it's simply some type of Linux. The standard access you have is through a console port, ssh, or a WebGUI. The console port and ssh logins give you a limited shell, apparently locked down to a set of commands you are shown. One of the commands gives you a pretty standard TOP output for CPU, memory, and processes, so it's looking more like a Linux system beneath the shell.

Let's Check Out the Internals

First, I upgraded the system to the latest version of software (5.0.2) to make sure I was looking at the most up to date code they had available. I have the smaller model, so I opened the system to see what trouble I could get into. There are basically two other ways to attempt to get access to the system. On the motherboard itself is a JTAG connector, and the hard drive appears to be a standard SATA hard drive. So to begin with, I removed the hard drive and attached it to my forensics hard drive controller. Granted, any USB to SATA controller would work. The next question became what type of OS was I going to connect this to.

So my system happens to be Windows, and the drive is formatted with more standard Linux partitions, which normally isn't compatible. However, people have made programs you can install to let you read these types of partitions. I'd recommend one that reads but doesn't write to the disk. Most won't guarantee they won't corrupt the file systems on writing, but reading is pretty safe. So I copied all of the files from the individual partitions onto my server, and started poking around. It turns out this isn't a perfect solution, as I'll cover later.

Initial Observations

Looking at the file structure shows this is a flavor of Linux.

```
Linux version 2.6.32.13mp5.0.2.0
➥.11 (build@engbf01.paloaltonet
➥works.local) (gcc version 4.3.3
➥ (Cavium Networks Version: 2_0
➥_0 build 99) )
```

So there are a couple of areas we can look at on the file system to learn more about the system and determine what other "opportunities" we might have.

`SDA2/etc/mtab` documents how these partitions are loaded so that we know where to look for configuration info:

Normal Operations

```
sda2 /
sda5 /opt/pancfg
sda6 /opt/panrepo
sda8 /opt/panlogs
```

Maintenance Mode

```
sda3 /
```

Maintenance Mode can be entered upon startup to reset the system and do limited recovery work like fsck. This mode is another interesting area to research in the future.

`sda2/var/log/dmesg` is the file saved from the system startup. Much of this can be seen if you login to the serial console when you power this on. This also shows on startup that an internal flash drive was mounted, which appears to contain the /boot information, since I didn't find that on the hard drive partitions.

`MIPS` - a flavor of Linux being run to handle the CPU on the motherboard. This causes some challenges for us as these aren't as common and documented, much less than Linux on Intel processors. There is shellcode for exploiting MIPS systems, but I'm sure this would take quite a bit more investigation to take advantage of. Conversely, the same challenges it presents us leads to a more secure platform for a security device.

`/etc/passwd` and `/etc/shadow` - good news as an owner, there appear to be no backdoor users, you appear to only have the PA accounts enabled, all the rest appear to be expired so you can't use them. For Root, they expired the password, and further set the `/etc` `➥/security/access.conf` file so you can't login as root. Now, looking at the login shell for all other enabled users, they are defined to use /usr/local/bin/cli as their shell. In looking for the CLI, I found a limitation with using Windows to look at the Linux partition. The Linux partition software didn't know how to handle links, so it ignored them. Later, while looking at the actual RPM for CLI, I could see it created a soft link to pan_cli in the same directory.

WEB GUI

sda2/var/appweb/htdocs is the root directory for the main web application. Looking around shows you what lies beneath the surface, something I don't think they wanted you to know. These URLs are pointing at the Management interface, leaving it at the default IP address.

```
https://192.168.1.1/php/utils/de
➥bug.php
```

Whoops, they left a Console Debugging application on the system. Login to the interface and open this link in another window. Click the debug checkbox. Now when you go back to your GUI and do anything, all the underlying data is captured in the debugger. This includes cookies, data sent and received by the GUI, etc.

```
https://192.168.1.1/php/readme.
➥txt
```

Come on developers, a little cleanup couldn't hurt you.

Under appweb, you'll also see the directories used for GlobalProtect (their VPN portal) and CP (their Captive Portal). These are less interesting, as they are relatively simple sites.

Content Updates

To me, the value in an NGFW is the combining of AV, IPS, and botnet detection to the standard firewall and URL capabilities. For a lot of companies, this is their "secret sauce" that they want to keep private to show their value. Looking around, I found the content updates stored in SDA5\mgmt\updates. So looking in the subdirectories, you find the content files. Looking at them in a hex editor, you can see the .db files are actually SQLite databases. Loading up SQLite DB Browser, you can look at all of the data.

curav\botnet.db - tables - malware_domains, ddns_domains (malware and dynamic DNS).

curav\virus.xml.db - virus information number, name, description, and severity.

curav\virus_signatures.db - virus name, action, signature (looks like mostly pattern matching).

curcontent\global\threats.xml ➥.db - IPS threats, references, actions, categories. Interesting for threats - they actually stored the signatures in an xml file.

curcontent\global\global.xml and some more interesting xmls to check out.

If you search other directories under SDA5\mgmt\updates, you'll find other .db and .xml files that store configuration or interesting information.

Brightcloud URL database seems to be done differently, probably due to the sheer number of URLs and performance concerns. This looks to be a nonstandard database showing category names, but all of the URLs are hashes. I'm sure this makes the URL checking much quicker and happens to hide this information from us. PA has now come out with their own PAN URL database, but I don't have a license to pull down those update files.

Interesting Finds

/etc/yum.repos.d/panos.repo - Yum Package Manager Repositories. Shows the IP address of their internal repo server.

```
##
PanOS repos
#
[core]
name=PanOS $
releasever PanOS
Base Repo
baseurl=http://10.0.0.226/pub
➥/repository/panos/os/$basearch/
enabled=0
gpgcheck=0
```

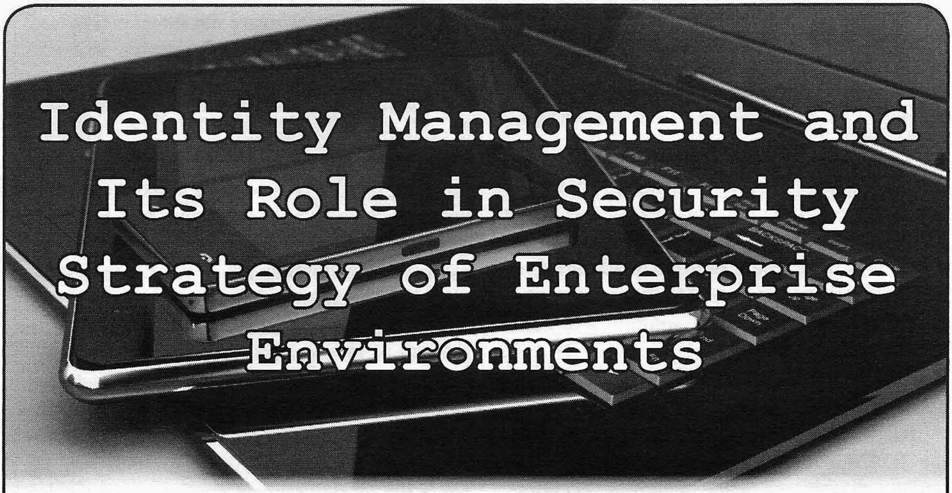
(so if anyone ever visits Palo Alto corporate, check out this server!)

Future Work

From this, there are a couple of "opportunities" I plan to explore for a Part Two:

- The JTAG connection looks interesting, but may be of limited use.
- Looking at the Flash ROMs to learn more about the system itself.
- Document installed packages and determine if they are all up to date, or, if there are older ones, are they vulnerable?
- Use write access to drive to re-enable the Root user and/or create another user and change the passwd file to give them a standard shell.
- Maintenance Mode - are there more options or possibilities here?

and many more... the more I dig, the more ideas come to light.



Identity Management and Its Role in Security Strategy of Enterprise Environments

by Patric Schmitz

Enterprise environments are usually anything but homogeneous. So IT folks get confronted with many different operating systems, and often many of them are not using the same user and group databases or any compatible processes for configuring for access control. This is a reason why Identity and Access Management, IDM, or IDAM is a term that we run into quite often and that companies are spending a lot of money on.

Why do I think this is worth being an article in *2600*? We are all interested in IT and security and, in my humble opinion, everyone at least should have a little background knowledge on what the whole thing is about and why it should be part of a complete and efficient security strategy.

Identity management sees the whole identity of an employee, instead of a single account within a system. Important information about an identity stored in various, independent places is not easy to consolidate and report on, so several data stores make it hard to control who has access, where, when, to what, and for which reason. This is the reason why IDAM should be part of security strategies, not only in enterprise environments, but in any heterogeneous environment. The more different systems there are, the harder it gets to keep track of user entitlements and accounts. Having different data stores for user accounts requires several administrative interfaces to manage them, which might require additional resources for account management. Now picture this in a bigger company and mostly we will find departments being responsible for one system each: Windows, Active Directory, UNIX, Linux, SAP, and so on. All the IT personnel is responsible for creating and managing accounts in the different systems, but the data within the systems is mostly not owned by IT, but by other departments. In many companies we will find a huge variety of process landscapes built around how access rights are being granted and created. Wouldn't it make life a lot easier and the whole account and entitlement administration more secure if all actions could be done through one single interface, which can be operated by anyone in the business? The data owners could decide, approve, and manage who needs access, recurring attestation for user entitlements could be automated and again be handled by the accountable employees without having to involve IT. This not only improves efficiency, but also security because there are no processes involving more people than necessary and we have a single source of information. This way reporting on access rights becomes child's play.

This is where IDAM kicks in. A basic IDAM solution will be the single point of administration for all accounts and access rights of an identity. Of course, it is necessary to have connectors to each and every target system which will ensure the IDAM solution will be able to take the necessary actions within the target systems and directories. Basic connectors to the most common systems and directories usually come with the IDAM solution either included right away or as add-on modules. Connectors to non-covered systems can be created either via external APIs or even from within the IDAM solution itself. The complexity creating connectors is not only based on the IDAM solution, but also on the API and documentation that comes with the target system or directory. A very rudimentary connector could just import a text file on a regular basis.

With the most basic IDAM solution, the challenges of several administrative interfaces has been removed, but most likely this won't help with the involved processes and the fact that it will most likely be mainly administered and maintained by the IT department. So, taking it a step further, the solution will come with flexible role-based access control (RBAC), automation, workflows, and modules that will allow self-service and delegation.

RBAC will allow you to define roles within the IDAM solution, entitling users to create, update, disable, or delete identities, accounts, departments, groups and equivalents. Roles allowing you to create other roles and assigning them to users, populate departments and groups. Roles defining workflows. Roles, roles, roles. You now realize that this doesn't have to be done by the IT department anymore, right? Parts of it, of course, will remain in the responsibility of IT and that should never change. Many duties and responsibilities can now be taken over by other departments. Not IT, but Business. Those are the people who know which user should be granted access to R&D, financial, manufacturing, or other data. How would someone from IT know if Debby still works in HR and therefore still needs access to the employee database, or if Alan, who is a contractor, hasn't already changed projects, but is still able to VPN into the company's network? IT usually doesn't know, Business does. Direct reports, sponsors, project managers, supervisors, team leaders. Those are the people who know who is still working in their projects, departments, or manufacturing sites. So shouldn't those be the ones to decide who is able to access the network, systems, files, or folders?

No, they shouldn't. Why? Because they don't necessarily see, realize, or understand what networks, systems, files, or folders are. But what they understand are job titles and departments. They know their direct reports and who is working for them. Now, let them decide and attest who is still working in their team, who is still involved in the project, and therefore who needs to be in their groups. We see that this is an important chapter of an IDAM solution as well. Translating access rights to something that is recognized and understood outside of IT, even by those who are not interested in how it all works. A good IDAM solution will take care of this and will even go one step further by: automating processes like adding all users in a department in the appropriate groups, granting all access needed for people with a specified job title, like VPN access for consultants often working from remote locations, etc. Basically granting as many rights as needed, but as little as possible to do their job. This is a basic principal in IT security.

A well-known example of what is common practice in enterprises: Bob moves from Helpdesk to Datacenter Operations. He already has several entitlements like updating user accounts within AD, resetting passwords, etc. One of his colleagues in Datacenter Operations is Jim. He has a list of entitlements needed to get the job done. If there is no definition of what access is needed, someone will most likely request the same access rights for Bob as Jim has. No one remembers to remove all the rights Bob still has from his position in Helpdesk. Jim retires a couple of months later and a new colleague, Tony, joins the company. Well, Tony will most likely get all the entitlements Bob has, including all the stuff Bob used to have working in the company's Helpdesk. This is not needed for Datacenter Operations though, but who knows this?

Managers, supervisors, and other data owners should review access rights on a regular basis. This way, even without an automation engine, it is more likely to find and eliminate wrongly assigned entitlements.

There are IDAM solutions out there that will even automatically manage assets like mobile phones, computers, desks, or wastebaskets, setting off an order as soon as someone new joins the company or changes jobs. Not exactly a security feature, but still a very nice functionality feature improving efficiency.

Another aspect which should be considered during a complete IDAM strategy is data governance. Data owners, retention policies, and access rights are important and should be known, managed, and reportable. An IDAM solution should support the business and employees by data- and role-mining. Finding out who has access and who actually accesses data regularly helps to determine ownership. Data owners are important as they are responsible for deciding who should have access and who shouldn't. Supporting data owners by reminding them to check access lists and retention policies will help to meet internal or legal regulations. This is nearly impossible to automate completely.

Let's look at another challenge which often is forgotten when planning IDAM strategies: generic accounts. Many generic accounts are high privileged accounts, but since there is no identity connected to them, they are hard to handle and manage. Frequent password changes and control over passwords spreading is not easy when there are no efficient and reliable processes in place.

Picture the following scenario: Bob knows some root passwords and passwords to service accounts from his job in Datacenter Operations. Root passwords are not changed frequently, even worse are the passwords to service accounts that haven't changed throughout the last few years. It's just too much effort changing the passwords on all machines the service actually runs on. Bob leaves the company for whatever reason. All of his accounts get automatically disabled and deleted after a while, as they are managed by an IDAM solution. But no one changes the passwords to all of the root or service accounts Bob still knows. Some of the system owners don't even know that Bob knows the password as they changed into the position after Bob joined the department. There is no guarantee that all of the passwords can be changed when Bob leaves and shouldn't be able to access any system in the network anymore. And, on top of that, he still knows the root password to some R&D workstations from his time in the Helpdesk.

We all know this is nothing we would like to account for, right? And this doesn't fit into the only as many privileges as necessary, as few as possible principal described earlier. A proper delegation model, not only for roles but for generic accounts' privileges as well should be implemented. This is just as important as a working, reliable strategy on handling generic, privileged accounts and their passwords.

Not only RBAC is important to become compliant to rules and regulations, but segregation of duties. Making sure the one who requests access isn't the one approving it. This would defeat all principals of the best RBAC design. And wouldn't it be nice of the IDAM solution to check on compliance during request time already? As always and anywhere in life there are some exceptions. These should be covered in the workflows as well. Maybe with an extra approval by a CIO or a security and compliance officer or both in a four eyes principal having to re-attest the exception after a given time so the exception won't be a constant temporary arrangement.

Some comfort making the user's life easier comes in the form of Single Sign-On (SSO). Users have to remember a lot of passwords and keep track of changing them as well. Not only passwords used at work, but also their personal ones. This is not only stressing the users themselves when having to login to several systems each day, but as well the IT (Helpdesk) staff who have to reset forgotten passwords, reactivate expired accounts, and so on almost daily. It is so much more comfortable to log in to your workstation, then be able to use any system you need without having to enter your password another time. For sensitive systems, SSO might not be the best thing, but then a strong authentication solution using Tokens, SmartCards, biometrics, or something similar is always better than just entering a password. Users tend to write down passwords and hide them in easy-to-find hideouts. During my time in Helpdesk, I've really seen PostIt notes under keyboards and yes, even sticking to the screen! In addition to that, a self-service portal for password resets will ease users' and IT staff's lives a lot.

Last but not least, logging and reporting should not be neglected. In combination with alerting, it's not only used to reconstruct what happened, but also to limit the damage that could have been done. There are not many people I know who like reading log files. Being able to easily filter line noise and making the log human readable is just as important as creating customized reports for auditors or anyone else who needs to audit what's going on. Alerting on changes of attributes that shouldn't be changed will enable you to prevent worse things from happening afterwards. Some changes won't have an immediately obvious impact, but might just be the precursor to a real problem. When alerted right away on the change, instantaneous actions can be taken.

There are a lot of aspects that should be understood when thinking about a complete Identity and Access Management Strategy. Most of them are not even new, but being looked at from another perspective, more connected, and more integrated than in the past.

I hope I was able to draw a picture about IDAM and what it means to the security strategy not only in enterprise environments.

Random Bits

Dear *2600:*

Love your great magazine. In college, I was a very conservative law and order type of guy. Since then, I've developed a serious interest in computers which led me to your magazine. I'd been reading it for about a year when the NSA scandal broke. I must admit that I look at things very differently now. I've long thought that hackers played a role in the evolution of better software. Now I see them playing a role in keeping the government honest. Take the case of Ed Snowden. Thanks to his leaks, I now know that we are well on our way to being completely screwed when it comes to privacy. I have become more pessimistic than ever about the future as far as privacy is concerned. Technology (the kind that invades privacy) is everywhere in our day to day world, and data from disparate sources will soon be linked together in real time. It seems that the younger generation doesn't care at all about privacy as they willingly spill all the details of their lives on Facebook for the world to see. The most recent poll numbers tell us that the NSA's domestic spying program is no big deal to many people. I just don't understand why more people are not outraged over it. The other day I took my morning jog and the following vision of the future started to take shape in my mind. I hope it is just a paranoid waking nightmare, but I felt compelled to share it with your readers.

Future scenario: a man walks down a public street and is scanned by facial recognition software and biometric readings are taken. The person seems anxious, angry perhaps. His heart rate is elevated. This is where our benevolent and all-powerful government enters the scene. Over the years, it has perfected its data collection to include real time electronic and biometric data integrated together so that no data is looked at in isolation. This suspicious person activates the monitoring software programmed to look for terrorists and other dangerous people (of course, all of this is done to keep us safe from terrorists). His facial profile is matched to a name and SS number in a government database. Now, the government knows that Mr. John Smith is upset this morning on his way to work. Time to do more digging. Does Mr. Smith own a firearm? Check the database. Better read his email to see if there is incriminating correspondence. Has he seen a shrink lately? Better check his medical record database. Check his Twitter and text messages too while you're at it. Has he had any unusual financial activity lately? Maybe he is in financial trouble or has been put on the payroll of a terrorist organization. We (your friendly government) will check that too. Now we check the correspondence of his wife and associates as well. Ah, it seems he is only upset because his wife caught him having an affair with a young woman in his office. Of course, we knew that months ago when she emailed her friends about it. Old news. Time to move on to the next suspicious looking person on the street.

I fear we will soon be told such action doesn't violate the Constitution because it is an old document written before email and computers. If the founders had known about terrorists and the Internet, they surely would not have written the Fourth Amendment without some exceptions for government snoops. And besides, as the Supreme Court will soon tell us - if you have nothing to hide, then you shouldn't mind government spying. Remember folks, freedom is seldom lost all at once, but bit by bit over the course of years.

Feel safer yet?

I don't.

Jim L

While this is undoubtedly a scenario that many in power would relish, we can take some comfort in the fact that the NSA story has not receded and, in fact, has gained much traction since it first broke this summer. While polls were quite disturbing at first, indicating that most people didn't really care if their privacy was being invaded since they had "nothing to hide," that initial lack of concern seems to be transitioning into indignation and a desire to learn how to keep our private lives private. Even *politicians seem to be getting the message, slowly voting to look into NSA violations after blindly accepting them. But we should not be fooled - those in power knew exactly what they were doing when they sold our freedom down the river and changed the rules so that all of these violations would be "legal." They should not be trusted again. Nor should we be doing anything at all to help make this easy for those who see our privacy and secure communications as some sort of a threat.*

Dear *2600:*

Pirate Bay and its affiliates are now blocked by all Internet service providers in Ireland. The court case was not defended. The European legislation requires the judge to recognize legitimate users' rights when putting in place such an injunction. Did anyone argue that Creative Commons material would lose an easy method of distribution? No.

Not that it can be proven, but it seems Ireland is hosting PRISM data under the umbrella of large U.S. corporations.

On the Snowden case, the Irish judiciary refused the U.S. deportation request, as they did not include the timeframe for the alleged crime.

Free Gary McKinnon
Garry Wynne

You have the Irish Recorded Music Association to thank for blocking Pirate Bay. But it's easily bypassed by using a web proxy or a mirror site, at least for now. But simply bypassing this idiocy isn't a solution - the idiocy itself must be defeated. As for your other points, Ireland's connections to the NSA PRISM program may not be provable at the moment, but that can change if someone with the access and a conscience decides to reveal the truth. We should consider how much has been revealed over the past few years by courageous people and feel optimistic that there are so many others out there who will do the right thing at the right time. And as for the Irish refusal to grant an arrest warrant for Snowden in July, this is widely seen as a technicality which the United States could easily fix. There are very few governments actually willing to stand up to the intimidating powers that are involved here.

Dear *2600:*

After years of wasting time playing high school sports because others wanted me to do so, after years of living in a household where the computer was seen by parents as evil because it distracted their offspring from the precious high school sports (you know, one of the things that don't have weight in the real world), I spent two months with my cousin in his Brooklyn apartment. He's a system admin for a company I choose not to name. Needless to say, my eyes have been opened to something I truly have interest in, and care for: computers. Is this enlightenment? Is the feeling of true awe, and a desire to learn as much as you can in what seems to be not enough hours in the day, what you folks at *2600* felt when you first discovered computers? Or "hacking?" My only regret is that, now, I am 19 years old, and have just finished my first year of university. I am changing my major to computer science. It sucks to know there are people out there who have been familiar with the world of hacking since age 13-14. They've got an edge I'll never have. Anyways - hope you guys at *2600*, and the entire reader base, immensely enjoy and make use of the rest of 2013. I sure as hell will.

lord.underdog

Yes, you nailed it as far as that magical feeling so many of us feel. But try not to think of it as a competition. There are people of all ages who are into this in one way or another. The time you've spent in other worlds isn't wasted time, but a window you've had into other perspectives that you can now bring here. Also, while majoring in computer science may be exactly what you need to excel and get what you want, it's not a requirement by any stretch. We know of many people who are hugely into hacking but have no technical training at all. All that matters is that you approach it in a way that's comfortable to you. There will always be people who do it differently and/or better. But nobody will be able to do it exactly like you.

Dear *2600:*

I have an interesting story and I am after advice in regards to whether it would make a good article. This happened recently - two weeks ago. I still don't know if I did the right thing....

To cut a long story short, I found an exploit in a live industry-regulated real money poker site. The exploit allowed me to download all players' hand history as well as see the last hands they mucked. It was bad JSON calls and I wrote a python script to make the requests and such I required. Obviously, with this information, one could do a great deal of evil things and really profit.... I thought, wow, this is my big break. Anyway, I didn't wanna be evil and there is no fun in cheating, so, really wanting to do the right thing, I decided to email them the exploit and hope they would... I don't know, offer me a job... or give me some money or something.

Anyway, I got an email back saying it was unreal and marvelous. They held an entire meeting to show their developers how something so simple could be such a bad mistake blah blah blah. They finished the letter giving me a 50 dollar no deposit bonus as thanks. This is a poker site with real money, regulated. This would have destroyed them. I mean, sure, they could have given me nothing, but for something so big, something of such great magnitude, I got $50. I could have played the poker on this site for years and years, fleecing every player and making a killing literally seeing their cards and the way they played. I could have loaded all of the data into software to analyze each player. I chose to do the right thing and that's my thanks?

I'm still in shock, to be honest. I thought this one was my big break. Obviously, I will write something up with full source and what they did wrong, etc. This was just a short explanation of what happened.

Scott

First, there's no such thing as your one "big break" if you have talent and ability, so you need to not think of this as a lost opportunity. More importantly, you have no way of knowing how someone will respond to a good deed. Returning a lost dog, performing CPR, or holding a door can all result in no thanks at all or something truly tremendous. You can't perform such acts with any expectation or you're doing them for the wrong reason and you'd also be a pretty shitty individual. So yeah, you probably saved their asses and they should have been more grateful. Perhaps they were scared you would really take advantage of them. In fact, some companies are so paranoid that they come after people who reveal such problems as if they were the ones who caused them! Our pages are often filled with such stories. We hope you continue to be honest and don't let this situation make you bitter or jaded. In the end, you're probably better off not working for them, as they don't seem to recognize the true value of talented people. We look forward to your article and have no doubt you'll find many more interesting exploits in the future if you keep looking for them.

Dear *2600:*

I work for a large web host provider and we have been migrating shared servers to Provo, Utah. It just all seemed a bit coincidental that news about the NSA started buzzing at the same time, so I did some searching. I discovered that the NSA had already invested a good chunk of time and money to build a data center in Utah. Another coincidence I find peculiar is that about 50 percent of the customers being migrated have complained of lower performance issues, even though this is "newer" hardware. Countless traceroute screenshots have flooded our support requests and there is sufficient evidence to say there are more hops between the customer and their migrated server. I just wondered if anyone else has reported similar experiences.

bob

If you truly believe traffic is being routed elsewhere, you can look at each of the hops in your traceroute for any smoking guns. But don't assume that just because your company is sticking servers in the same state as the NSA that there's any connection, online or off. Lower performance with new hardware is surprisingly common.

Dear *2600:*

What would happen if someone wrote a trojan that, instead of taking control of your machine to add to a botnet, simulated the Internet traffic of someone the government might want to keep an eye on. Such a trojan could potentially flood the NSA with so much dummy information that they might just give up on trying to make sense of it since it would seem like everyone in America is up to no good.

Pete

The trick would be making it unique and random enough so it couldn't be easily identified as "that trojan." This technique has been used in the past against totalitarian regimes to bog them down with erroneous data. No doubt it will be a strong tactic to use to confuse and annoy surveillance proponents in the future.

Dear *2600:*

A national radio program called *Radio Lab* did a segment on Joe Engressia (aka Joybubbles) and how he discovered 2600 hertz. It also touches on the rest of the early phreaking community and follows his life story even after he quit Ma Bell. The link to the story is http://www.radiolab.org/2012/feb/20/long-distance/. My local NPR station is doing summer reruns, though, so judging by the URL, you folks may have already heard about it. If you haven't, though, it's well worth a listen.

Nate Brown

Dear *2600:*

I just listened to the podcast of *Off The Hook* for Wednesday, August 21st, 2013 regarding the sentencing of Bradley Manning.

I am utterly disgusted to find that the U.S. government treats its own citizens who tell the truth no better than it treats "enemies" in other countries.

More Americans should be outraged at this behavior. I don't mean to be patronizing, but I feel so sorry for the American people because they are put in the same blame basket as their government.

The American government is their own worst enemy. They have either chosen or created their own "enemies" in this day and age by their bullying, strong-arming, and abuse of persons in other countries and the other countries as a whole. I can see this behavior is going to come back around in a very bad way unless Americans force their government to change their demeanors towards others and indeed their own.

Thank you for your time.

Neural Nut

That's basically what it comes down to - the people need to confront their leaders on these issues. If they don't - or they feel that they can't - then it's the same as giving their enthusiastic approval and, before you know it, the concept of "normal" has changed.

Contributions

Dear *2600:*

I've been an avid reader since the 1980s, and in the mid-1990s, I started making electronic music. I still do - check out http://distancetojupiter.bandcamp.com/.

During the interval of time between October 1999 and May 2000, I composed two tracks. There's a slightly weird history for both, which I'll get to in a moment. They were performed live using a Roland MC-505 Groovebox and recorded straight to MiniDisc. The tracks were never released as part of any of my Distance to Jupiter albums, mostly because they're pretty long and meandering (there was a lot of pot smoke in the room at the time, and well, that's what happens). I was listening to *Off The Hook* a few months ago and liked how you had these long electronic musical intros prior to the all the talky bits, and it reminded me of these two tracks - especially "Hacker Ethos" which was inspired directly by *2600*. So I spent hours searching my audio archives for these tracks, and dusted them off. I put a quick coat of mastering on them today and I present them here. If you like them, feel free to chop/edit/mangle for *Off The Hook* or just enjoy, or simply trash 'em. If you prefer the latter, let me first ask that you take a listen to the intro to "Channel 144" which contains a long sample of Morse code which I found, back in 1999, on Dish Network's channel 144. There was a really weird test pattern on screen at the time, and this endlessly repeating bit of code. I sampled it using a BOSS SP-202 sampler. This channel later vanished, but thinking back to those days when Dish Network was actually kind of interesting (and you could find really bizarre things on the higher-numbered channels), I've realized I'm still curious to learn what this was all about.

I may attend a *2600* meeting in Phoenix to see if anyone there knows Morse code or try to learn it myself. Anyway, these tracks form a hacker-themed pair, so I thought I'd relate the history and present "Hacker Ethos" as a potential intro for an *Off The Hook;* it was directly inspired by reading *2600,* as I said. Note that I'm not reserving rights on these tracks, and I'm releasing them under Attribution-Share Alike CC BY-SA (http://creativecommons.org/licenses/by-sa/3.0/).

The track "Hacker Ethos" has two flavors, AIF and WAV. Same goes for "Channel 144." I provide both formats because I know sometimes people have preferences.

https://www.dropbox.com/s/8vovcwbmx790n8f/Distance_to_Jupiter_Hacker_Ethos_%28c1999%29.wav.zip

https://www.dropbox.com/s/ex0xq2s6d5sb1ro/Distance_to_Jupiter_Hacker_Ethos_%28c1999%29.aif.zip

https://www.dropbox.com/s/v87qadwtrxarskc/Distance_to_Jupiter_Channel_144_%28c1999%29.wav.zip

https://www.dropbox.com/s/cx6xz0fy76u1b8c/Distance_to_Jupiter_Channel_144_%28c1999%29.aif.zip

Take care, and keep up the amazing work. I love *2600!*

Jim

In order to ensure that everyone gets to hear these great compositions, we're printing the direct links here. We also encourage readers to check out your other material. Above all, we want to thank you for thinking of us and for being creative - and especially for doing both at the same time.

Dear *2600:*

I'm mailing you to offer our services, pro bono, in the field of illustration, design, and image making. Although I love the look of *2600,* I'm thinking that it could be even more powerful - more up to date and layered without losing the brutality of the design you have had for a long time. If this in any way sounds interesting, get in touch and let's discuss further. We would love to make you a proposal for a redesign!

Rasmus & Hanna

We assume you're talking about the printed issues and not the website. Sometimes it's hard to tell when we get email. We're open to specific ideas and this goes for all of our readers (and website visitors). We're always looking to change things up a bit and to improve on what we've already got. Thanks for the generosity.

Dear *2600:*

I see cool art and images in the magazine and I don't know if you have a recommended way to send them in. I took a photo of a building in Barcelona, Spain recently that went crazy with the cameras, like an art project or something. When I snapped the picture, my first thought was "I have to send this in to *2600*."

I uploaded it to Dropbox here: https://dl.dropboxusercontent.com/u/52597040/DSC_1196.jpg

You are welcome to use the image any way you like. I'm a lifetime subscriber and I already have several *2600* shirts, so I don't really need anything in return.

Enjoy.

Tom

We don't want to get into the habit of printing dropbox links, but this image deserves to be shared far and wide. There are literally hundreds of "cameras" on that building and we'd sure like to know more about it. As for how to send us images to print, you can email us at articles@2600.com with any hacker-related or 2600ish images. Payphone photos, as always, should be sent to payphones@2600.com.

Dear *2600:*

I'm not sure what your submission policy is re: multiple publication, but I'm assuming it's lax so I'll just give you a link to a piece on my personal website that I think might interest your readers.

Jesse

And our auto-responder quickly dispelled that assumption.

Dear *2600:*

Amusingly, your autoresponse does enumerate your policy on duplicate publication, and it's not compatible with what I've done, so feel free to count my submission out. I send this email as a note that you might want to put that policy on your website somewhere that I can find it.

Jesse

Point taken and we will update that part of our website accordingly. Hopefully, you'll send us an article in the future.

Dear *2600:*

Knowledgeable colleagues tell me that my article "Extra Legal Harassment" has been published in the Spring 2013 issue of the magazine. Yay! I wrote that back when I was a political prisoner of the Feds in a facility in Beaumont, Texas, and I've been wondering what to do with it if you didn't find it to be useful for *2600*.

With Snowden now being perhaps the ultimate example of what I discussed in the article, it's a timely topic and I hope it can help other activists be prepared in the event they are targeted by corrupt law enforcement as a result of their efforts to encourage a better future for us all. With the rule of law largely in tatters in this country - I was recently lectured by a federal judge abut my (vocal and unchanging) unwillingness to follow the "spirit" of the law so I understand this quite well - it's imperative that activists be prepared for the full suite of tools used by the police state to cripple its opponents.

I've been working on some writing relating to tactical tools available to protect against illegal and unconstitutional NSA dragnet surveillance - if it's of possible interest, and the writing comes together well, I'll submit the result for consideration. If it sucks when I'm done drafting it, I won't waste your time.

Oh, and I've had the same aforementioned federal judge quote verbatim from my Last HOPE presentation, twice, in open court - is that some sort of record? He is quite obsessively interested in my assertion (paraphrasing, as I don't have the transcript handy) that "learning how to work around the rules, instead of breaking them, is both safer and far more fun." Which, I dunno, I always thought was a rather boring statement of objective fact. But in the United Stasi of America, "daring" to learn the rules well enough to avoid breaking them is, apparently, reason enough to be imprisoned. There's a dark irony there. More than one, eh?

The world is far stranger than I would have ever imagined.

D. Spink

Dear *2600:*

I've been reading your wonderful magazine since 2010 and it has been worth every penny. I usually don't have a chance to use much of the information that it contains, but it has been a great force directing me toward my current career path and choices, so many thanks for the years of publication.

I find myself with a great deal more free time on my hands lately and, as I've looked for valuable causes to donate my time to, I keep coming back to *2600*. Are there any significant opportunities for volunteers or interns to work for *2600?* How can I get involved, and what skills would be needed for this?

follow_the_lea

There are all sorts of things that pop up from time to time where we can use some help on one project or another. Usually, we'll mention it on our website (www.2600.com). One recurring project that needs lots of volunteers is the HOPE conference, which takes place every two years (in July of even numbered years). For that, we need help in everything from security to buildup to overall coordination and a whole lot more. Again, you'll see detailed mention of this on our website as it gets closer.

Special Requests

Dear *2600:*

I am writing to request that someone review an article I wrote for *Baseline Magazine* www.baselinemag.com; *Baseline* is an online and print magazine based like *2600* - it is in New York, New York.

To view the article just click on the attached link.

WS

Yeah, that's not going to work for us. For one thing, we require that writers actually send us material, not give us a link to it. For another, we don't print material that's already been printed in another publication or put online. Our readers would crucify us if we did. That said, we do hope you send us an original article in the future.

Dear *2600:*

Dear sir,

I kindly reference to can you teach me trick of hacking.

Please reply whatever your answer.

Omi

Every damn day we get a request like this. This is one of the lucky ones that we'll actually print. And our answer is basically the same as always: there is no "trick" involved nor is this something you can learn in a classroom. You have to go out and experiment on your own. By all means, read as much material as you can get your hands on to see what others have been up to. (That includes this publication.) But nothing can substitute for your own personal experience, one which we hope you share with other curious individuals. And if you come up completely empty with no ideas of your own and you feel the only way for you to learn is to have someone else telling you everything, odds are you're not actually a hacker yourself, but simply someone who is interested in what hackers do. We refer to that as the rest of the world.

Dear *2600:*

Been reading the current *2600 The Hacker Quarterly*. Brings back some great memories from the past. Hopefully this also awakens my mind and lets the learning flow.

Accept the invitation to view the full post: https://plus.google.com/_/notifications...

Google+ makes sharing on the web more like sharing in real life. Learn more: http://www.google.com/+/learnmore/

Name Deleted to Avoid Intense Embarrassment

And then there's the Google Plus spam we've been getting lately. We're not signing up to any services, accepting invitations, or giving out even the tiniest bit of personal info in order to simply read submissions. So we ask that readers not try to pull us into whatever scheme you've pledged allegiance to and to simply send an email to letters@2600.com or, if you're truly old school, an actual letter to 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

Dear *2600:*

Have you guys decided on a new theme for the next calendar? Could a book theme be done? It would be an adventure to find some of the great hacker texts, such as first editions. Also, you could embed an anti-DRM message during a significant period of submission to this injustice, which very few people have thought about in depth.

zenlunatic

Good ideas, but the 2014 calendar is already out with photos of payphones as the theme this time. You can get more info elsewhere in the magazine or through our website.

Dear *2600:*

I am in Denver, Colorado and I need to contact the U.N. or MI5. I am a prince of England - Prince Nicholas Bailey. The citizens are in serious need of outside help. My cell [redacted] is being forwarded. Most of the Internet is being rerouted to McLean, Virginia or Texas.

I have been trying to get word out for sometime now. It's mostly by Twitter or Facebook. Avoid the FBI at all costs.

Please help.

P.S. There is A homeless gang here pretending to be hackers. They are mostly junkies.

Asylum seeker
Prince Nicholas
Denver, Colorado USA

It shouldn't be very hard to contact the U.N. or MI5, especially using Twitter and Facebook, but we wouldn't be surprised if they already knew about you. As for the homeless gang of pretend hackers, there has to be a really good book in there somewhere. We suggest capturing as much of the dialogue as you can on a notepad. Unless these are actually Hollywood screenwriters already trying to do the same thing.

Continuations

Dear *2600:*

This is my fifth or so letter to *2600* over two years about *the same thing* and you have yet to actually address the issue except after my first letter when you agreed with me completely and changed your policies correctly... then later changed them right back to the "wrong-headed" way they were before I alerted you to your error and you fixed it. All your subsequent "answers" to my same query did not actually address my point at all. I assume different people may answer different letters each quarter, so maybe that is part of the problem.

Your best answer was "... We don't see why what was fair in the past wouldn't be considered fair today." Since my point of contention is that *2600 authors do not get the same payment they used to get, while photographers get more payment.* That is my point and question: *why don't 2600 authors get the same payment as they used to???*

Your last response was "we're always open to new ideas and to discussing different approaches, but we don't seem to be making any progress explaining things here, so we'll just have to disagree."

Did you even *read* my letter? Your response indicates you did not, or that you could not understand my clear English.

"My idea" is neither "mine" (it was *2600* policy for years) nor is it "new" (*2600* policy again). And what exactly are we "disagreeing" about??? You have *not* addressed my concern at all, therefore we have nothing to "agree to disagree" about!

So: I'll try to make this very simple for you, since you keep misunderstanding.

1) *2600* used to pay authors a certain amount of swag, the same amount for many years.

2) One day *2600* started offering swag to *photographers*. On that day, the amount of swag paid to *writers* went down.

3) I wrote a letter pointing out the oddity of photographers getting *more payment* than authors in a primarily *text* magazine.

4) *2600* responded that I was totally correct and, like the *2600* I've known and loved for years, changed the author payment *back to the original swag amount.*

5) Some time later, without notice, the author payment was *changed back* to beneath photographer payment.

6) Since that time, I have valiantly tried to remedy this, but every time I write about it, I get some nonsensical response from you.

Now: Do you think *2600* authors deserve *less swag* than photographers and if so: *why?*

If, like me, you value writing more than photos; why not change your policy *back to the way it used to be?* Writing takes more effort than snapping a picture; it's that simple, folks.

That all being said (yet again!): what are we "agreeing to disagree" about? Does *2600* think pictures are more valuable to the magazine than writing? Yes, I disagree. Does continually changing the subject (as you have been doing) and consistently refusing to answer my simple question help me or *2600* in any way? No, it's just a waste of both our and the readers' time. If you will *not* answer my question, then why even print my letter at all?

The *2600* letters column has a long history of snarky responses to stupid letters, but ignoring an *intelligent, well-researched, valid, correct, and polite* letter from a lifetime subscriber and seven time author? That's pretty shitty.

So man up and *face the facts: writers used to be paid more. Photographers used to be paid nothing. Photographers get paid more than writers, which was remedied once already by 2600, then silently reversed. My questions on this subject have since been misinterpreted, misread, misunderstood, or deliberately ignored. Does 2600 now value pictures more than words and if so* (as it does appear, since they are paid more), *why* does *2600* value pictures more than words (and don't say "a picture's worth a thousand words" - I already used that cliche in my first letter on this topic. Concerned with the apparent raging "bureaucratism" encroaching on *2600*.

Barrett D. Brown

To start on a positive note, your letter has set a new record for use of italics. And now to address (again) your concerns: All we can say is what we've always maintained - we do the best we can as far as compensating contributors. If we had a huge budget and lots of ads, we could afford to do more. We know that those who submit articles or photos here aren't doing it solely for the subscriptions or shirts (the "payment" you refer to), but because they want to help make a better magazine. At least, we hope that's the case since the attitude you repeatedly express here isn't what we're all about. Nor are your facts accurate. We offer the same items for writers and photographers and have for some time (one year's subscription, a year of back issues, or one of our shirts for each printed submission). It really couldn't be simpler. We offered different things in the past and reserve the right to offer different things in the future, based on what we can afford to do, the total number of printed submissions, what people are happy with, etc. We can nitpick this to death and claim injustice because articles are all different lengths and other such minutiae. We can seriously take you up on your offer to debate whether it takes more effort to be a writer or a photographer. There are very few activities on the planet which would be more of an exercise in futility. We hope you realize this now or sometime in the future and that, if we're wrong, our readers will tell us in droves.

Dear *2600:*

Okay, the planet is maybe going to implode, but I gotta say that "The Prophet" is wrong, wrong, and wrong some more, about the bit rate of a GSM channel.

It is true that on the backbone circuit-switched (non-VoIP) network, voice is transmitted at rates of 32-64 kbps. But all digital cellular radio interfaces compress voice down to about eight kbps or less. Obviously, this increases the capacity of cellular systems by a factor of eight. Or, put it this way, if they stopped compressing voice tomorrow, the capacity of GSM and other cellular systems would drop by a factor of eight... and the planet probably would implode.

His statement that, "Before compression on the air interface (which can vary depending on the codec used) GSM channels are 64 kbps PCM" is nonsensical (can I say "total crap" in *2600?*). It is nonsense because, before compression, it's not a GSM channel. Even if 64 kbps PCM is delivered to the RF circuitry, it's still what goes out over the air that is the GSM channel. And, although it is true that codecs vary in bit rate slightly, they don't vary very much. The highest bit rate voice coder that I am aware of for cellular was 13 kbps, and I don't believe that is used anymore. Sometimes codecs run at lower bit rates during periods of silence as a further optimization, but not higher.

"The Prophet" can easily end this debate, and the risk of the planet exploding, by remaining silent, which I will take as a sign of an admission that, for once in his life, he's wrong. That doesn't mean I don't love him.

D1vr0c

We can think of very few people who would accept that kind of an offer to end a debate. The Prophet is not one of them. Here's his response:

"I am always happy with a robust engineering debate but have no interest in further participating in it. We are splitting hairs that have already been split at this point. We'll have to start splitting my pubic hairs soon if this continues and I'm guessing nobody wants that."

If this doesn't put an end to the discussion, we're out of ideas.

Critiques

Dear *2600:*

For a magazine about hacking and technology, your website is pitiful. When viewing stores that carry *2600* in Colorado, a list of cities pulls up three different entries for "Colorado sprin," "Colrdo springs," and "Co springs." (http://www.2600.com/magazine/2600locations/us/co.html) I can only assume these are the attempts of a monkey with carpal tunnel trying to type the city "Colorado Springs" before giving up and going back to sniffing another monkey's bum.

Also, one of the stores listed has not been in existence for years, and some newer bookstores that carry *2600* are not included. If maintaining the website is difficult, perhaps turning the *2600* website into a community-editable Wiki format would be more efficient. Just a thought.

Grace

You may have noticed by now that we've just redesigned our site, something we've been working on for a number of years. We owe it all to one dedicated reader, who devoted countless days to migrating, converting, and creating content. The effort, however, continues. Now we have a lot more flexibility to do more, as well as vastly increased space for content. (For example, we now can host all of our radio programs at 128 kbps instead of 16 kbps.)

The listing of stores you refer to is ancient and was not put together by us. The carpal tunnel af-

flicted monkey worked for one of our distributors and we merely took that data and posted it. We've recently obtained a much newer list and hope to have it in a much prettier format (with maps and everything) by the time this issue is out. But the data will certainly be outdated as soon as it goes online. Getting the info from our distributors often takes quite a bit of cajoling for reasons we don't understand. Add to that the fact that bookstores keep going out of business and aren't being replaced and you see what we're up against. In the United Kingdom, for instance, we were a very popular magazine on newsstands but now can't be found at all because the stores and distributors have gone under and those running things now think there's no market for us. It's living proof that publishers are the first casualty of the publishing industry.

We're very open to the idea of doing something more Wiki-based, but this also takes quite a bit of coordination and time, something so many of us are in short supply of. We'll listen to any ideas people have.

Dear *2600:*

I've really enjoyed getting your magazine on my Kindle for the past few years. I'm sad to say that I had to cancel my subscription today. My subscription through Amazon expired this week because of a credit card number change. I resubscribed this afternoon, but noticed that I had lost access to all my back issues.

According to the Amazon rep that I chatted with: "...with regards to past issues with your subscription. You no longer have or access on the past issues due to the cancellation of the subscription when the card used lapsed, John. However what we may do is to refund you for the past issues."

It's sort of a ridiculous policy to remove the issues that you've already paid for from your account. I have yet to have a magazine come over to my house and take back any paper copies of a magazine after my subscription lapses.

Is there any way to (legitimately) get a DRM-free electronic version of *2600?* If so, I'd definitely be interested in subscribing. I'd be really happy with a MOBI file or an EPUB emailed out every quarter.

John

We have indeed added additional options for electronic versions since your letter came in, so you can explore those by going to our website. But to address your specific concern regarding Amazon, what you cite is simply not an acceptable policy. We've made that very clear to Amazon, as have many of our readers. As we're pretty high up on Amazon's magazine list (thanks, readers), they tend to listen. So they wish for us to tell you that, by default, up to seven back issues should always be viewable in the section titled "Periodicals: Back Issues." After that, they wind up in an archive. Readers can always elect the "Keep This Issue" option to hold onto it indefinitely. It's possible the rep you talked to somehow didn't understand this. We are more than happy to print an article that provides additional methods of keeping or transferring items you've bought if somebody writes it. Having such an article available on the Kindle would be a very valuable service for so many of our readers - and for Kindle users in general.

Dear *2600:*

I notice that the Summer 2013 issue features the article "Perfect Encryption Old Style" by Cliff. This is the exact same, word-for-word article that I also read in the Winter 2011-2012 issue, by the same author! Was this a fluke or is it a normal practice that I've never noticed until now? I'm not going to ask for a ten cent refund, although I do prefer paying for new content.

iacode

We're surprised we weren't deluged with complaints after making this horrible mistake, which only appeared in our paper issues. It resulted from two articles having the same file name in different directories and software that made some very bad assumptions. By the time we realized what had happened, the issues had already been printed. The electronic issues weren't affected, nor will this error show up in the Hacker Digest, Volume 30. What we did to rectify this and not rob our readers of two pages was to get rid of our house ad and staff box for the Autumn issue and replace that with the article that should have run in the Summer issue. We've also changed our file naming scheme so that such a thing will be caught a lot quicker if it ever happens again. But our next spectacular error will no doubt be something none of us anticipates.

Info Needed

Dear *2600:*

I've been into matter-mixing rather than hacking for the last few years, but I was interested in seeing the hacker perspective on bitcoin. Have there been any articles on this topic released in the last few years?

Jack

You will find articles on the subject in this issue and we hope to see way more as this evolves.

Dear *2600:*

I was wondering if there was a way to see what has been written about the Obama administration regarding loss of privacy. I remember a few years ago when I read alt.2600, there were quite a few editorials about how Bush was taking away our right to privacy. It seemed as if every magazine I picked up was complaining about Bush.

But since Obama became president, I haven't seen much written about him. I wonder if now with the Snowden revelation, something will be written up about him.

nick

We think that you should have no problem finding an article or two on this subject. But we're a bit unclear as to whether you're referring to us or *the Usenet newsgroup (alt.2600), which is quite a bit different. When we began publishing, Ronald Reagan was president. From that point until now, we have never honestly believed an administration had our right to privacy in mind as anything other than a threat to their agenda. We don't see that changing, so being vigilant is always going to be important.*

Dear *2600:*

If I access your website, are you going to hack my PC? I have a webcam, can you see me?

Inquiring minds need to know!

james

And by now you do indeed know. (The images go live if we don't get the check by November.)

Dear *2600:*

Will there be a HOPE conference this year/ summer?

Stephen

Lucky for you, no, or you would have missed it. HOPE X will take place in July of 2014 in New York City. You saw it here first.

Dear *2600:*

I have two problems. It's not something like discovering a zero-day and sharing it around (I wish I had one). This problem hits closer to home. I am currently studying for the A+ exam, but every time I sit down to study, I always hold back because the book is so extensive, and I fear that I will lose what I learned previously as I press forward to new chapters. I take notes, but it never seems to be enough.

Every time I take practice tests, the engine will tell me where I need more work and where I am strong. But sometimes the results vary. Sometimes where I once was strong I am now weak. I feel like I am trying to play catch-up with myself and will never take the exam because of this vicious loop I am in.

My second problem is I have taken this test once before in the past and failed. Since then, I haven't returned to take the exam. I am afraid of failing again. I try to block that moment in my life out, but every time I sit to study, it haunts me.

I love computers and want to be an expert PC technician one day, but I can't if these problems pose a constant roadblock for me.

I know you normally deal with the more mechanical and programmatic aspects of computers and so on, but can you also handle a psychological issue like mine? I will appreciate any kind of advice you can offer.

Thanks and keep up the good work.

Chaoticpoison

You are far from the only person facing this. Please don't torture yourself with expectations that could be out of reach, completely unimportant in the bigger picture, or both. Certifications are all fine and good for people who value these things, but there are many out there who don't. In fact, we're pretty sure there are places where listing them on a resume can actually work against you. The people who push these things will tell you there's no way you can succeed without them. That's a huge load of crap. If you truly love computers, you can find a way to work with them and to be good at what you do. Not everyone can succeed in the exam-taking environment, including many of the most talented people out there. That's nothing to be ashamed of - it just means your talents lie in a different area. The world of technology is so huge that you can define your own success with a little creativity and perseverance. That's pretty much how we got to do what we do.

Dear *2600:*

I was wondering how many articles do you guys consider for each edition of *The Hacker Quarterly?* Am I really that good to get two in a row?

Andrew

We generally don't consider the author's name when we look at an article so you likely did a good enough job to be published twice. Three times if you count this letter.

Dear *2600:*

I know I probably shouldn't be asking, but I really don't think it's a big deal. I am doing some research for writing and trying to find out how the companies go about securing payphones, where the locks get made, and how one can go about unlocking one?

Joe

Why on earth would you think you shouldn't be asking something? You should hear some of the questions that get asked around here. Anyway, if you look online for an article by Matt Blaze entitled "Notes on Western Electric (Bell System) Coin Telephone Locks," we suspect many of your questions will be answered. And, of course, if anyone wants to write more on the subject for us, that would make us really happy.

Dear *2600:*

Is there a recommended range for word/character counts? I'm assuming there's a max of some kind - can you tell me what it is (i.e., no more than 1500 words)? I've considered writing articles for *2600* for a long time, off and on, but I've always gone back to the length thing in my mind and then ended up getting sidetracked.

Also, I know how if it's been published elsewhere, it can't be published in *2600*... but I have another question. What if I wrote an article and attached a link (e.g. the article is the very basic version of my topic, to conform to text limitations and then the URL is an expanded version) but with the catch that the link is not activated *until* the article has been published? Would that be acceptable to do?

To be clear, you wouldn't *need* to click the link to understand anything, it wouldn't be required in any way (as that'd defeat the purpose of hard copies, forcing those readers to get to a computer/Internet). Instead, it'd just be additional/more detailed coverage of the topic. It would contain the original article text as well but, again, it wouldn't be published/accessible until after the article had been printed in *2600*.

adam

Don't let the length thing be an issue that keeps you from writing. Articles that are too short are more of a problem than articles that are too long. You can easily write several thousand words if you wanted to and, if the subject and presentation were interesting, we would be happy to print it. If it's a bit too wordy, that's what editors are for.

What you propose for links is certainly something we can do. We just want to avoid a situation where readers feel compelled to visit the website in order to understand the article. Pointers to further information are always welcomed and encouraged.

Meeting News

Dear *2600:*

I showed up for the last Philadelphia meeting, but I'm not sure there was one. I believe I showed up at the correct time and place (5:00 pm, first Friday of the month, 30th Street Station, southeast food court near mini post office).

There was no obvious group of people that appeared like they were conversing about technology or the magazine, no "2600 Meeting" sign, no one reading the latest *2600* issue. I sat at a table for a while with my issue open, thinking someone else might see it and know what I was there for. After an hour, I left. This was my first time trying to attend a meeting, so I'm not sure if I was looking for the wrong signals, or if past meetings were empty as well.

Do you know if this meeting is still active? Has the location or time changed?

Curious in Philly

Last we heard, this was an active meeting. Often, people don't show up for an hour or two after the start time. Of course, making that initial contact can sometimes be tricky, especially if people aren't congregating where the listing says they're supposed to be. It's always a good idea to walk around a bit in case that happens. If we get more such reports or don't hear anything from attendees, we'll have to delist the meeting.

Dear *2600:*

I already read the guidelines for the meeting and I don't have a problem with it - only with the day. I want to start a meeting in Costa Mesa, California. My problem is that I was going to start it on the first Monday of every month with the same schedule as the other meetings. It won't be possible for me and other people that are interested to do it on Fridays. I don't know if this is doable. Just give me your opinion; any recommendations would be appreciated.

Congratulation for your magazine. It teaches that you don't have to forget the cool hackers from the 1980s just because there is a lot of new technology. One thing I've learned in martial arts is that you never forget your basics and the root of what you're learning makes you better in the long run. This makes you humble and turns you into a better person and a better hacker - to hack to help others, not to hurt others. But I also know that not all is good. Like the ying and yang symbol, bad can't exist without good and good without evil. This is only my opinion and what I learn from hacking.

Thanks again and keep up with this great magazine.

Jorge

Thanks for the kind words and an interesting analogy. As for the meeting day, we've tried in the past to accommodate people who wanted to meet on different days, but we have yet to hear an idea that can work without confusing everyone and taking up an awful lot of space in our meeting listings. There is no one "other" day that would work for everyone, nor is there even a week that would. So we'd wind up with some meetings being on a second Tuesday, first Monday, last Saturday, etc. And even after doing that, there would be people in each of those places for which that particular day wouldn't work, leading to more contention and debate. This is why having one day a month worldwide continues to work and make sense overall. We hope you're able to somehow make this work.

Dear *2600:*

Over the last five years, I have randomly tried to find people at the Orlando meetings. Lately, you list Fashion Square Mall. Prior to that, it was the Florida Mall. Even with arriving 15 minutes prior to the 5 pm allotted time, no one *ever* shows up. And I've tried "pretending I am reading *2600*" and also having my laptop popped open.

No one. True, what does a hacker look like? Grizzly? Fat and balding? Acne child? Who knows!

Since these locations are a good one hour from where I live, how about we change the location to within 15 minutes? Not sure how people can object if no one ever shows up.

Jerrold

We're also not sure what the advantage of having a meeting closer to your house would be if nobody shows up. Read on for further info on this particular meeting.

Dear *2600:*

I attend the Titusville meeting now, but I would ask that you keep the listing for Orlando. I still maintain the website for Orlando, and hopefully the University of Central Florida kids will get together.

Richard Cheshire
Phreak & Hacker

As evidenced by the previous letter, that simply hasn't been happening. Keeping a meeting listing up in the hopes that someone will show up simply *isn't good enough. We'll wait one more issue to see if the situation changes, otherwise it will become meeting history.*

Dear *2600:*

I live in the Hawley Wallenpaupack area and I wanted to join *2600* meetings, but the closest one is in Allentown which is an hour away. I have tried to contact them many times and no one ever responds. The next closest meeting is three hours away. I was wondering if I should just start my own meeting.

Brandon

Starting your own meeting when there's one already in the area defeats the entire purpose of the meetings, which is to get together with people who share common interests in a particular region. The best way for you to make contact with these people is to simply show up at a meeting! Since it's only once a month, it shouldn't be impossible to figure out a way to get there.

Dear *2600:*

I was interested in starting a meeting in Syracuse, New York. Do you have any special requirements that I need to adhere to?

Steve

All of the info you need can be found on our website in the meetings section (under "Events"). Basically, meetings need to be held in public areas, not exclude anyone, and act responsibly. All meetings take place on the first Friday of the month (usually at 5 or 6 pm, and they must contact us at meetings@2600.com with occasional updates as to how the meetings are going.

Feedback

Dear *2600:*

Laurels to D.B. LeConte-Spink on his extensive and easy-reading article on the intra-system tactics of surveillance and oppression against the curious-minded community. His specific tactics on social engineering are rarely addressed in the black, gray, and white-hatted circles alike and were a joy to read as well as his defenses against. The "black propaganda" campaigns that are oh-so-common in all worldwide police states are but mere whispers and still ugly truths.

Radagast

Dear *2600:*

Re "Reversing Cisco Type 7 Password Hashes" by mcandre (30:1): Yeah, they are shit. That's because even in the mid 90s they were only there to prevent shoulder surfing and to provide legacy support for truly ancient kits (even in 1995/96).

When I attended Cisco training courses back then, every course told you to remove them and use Type 5 passwords (no matter what the course was). If you encounter a Type 7, then you have either discovered a collector's piece or something administered by a fucking idiot.

Pardon my cynicism regarding this as I have been in the network business for way too long and anybody who knows the difference between their ass and their elbow has dealt with the problem. Much of the problem is actually from Cisco customers who insist on using the pointless "shielded" passwords because their network teams are clueless and insist on using configs which were created in the early 90s.

Yes, I have received complaints about a switch being faulty because it won't accept a config, with the problem being there are no Fast Ethernet (10/100) interfaces anymore - they're Gigabit interfaces (prefixed with Gi instead of Fa), and so the onsite team complains that it's too difficult to configure the "new style" switches.

The situation as I often encounter it:

I work for a multinational IT which (among many other things) builds and administers after other people's networks. We still see Type 7 passwords when we become responsible for a network that has been built by a team that has no clue whatsoever. Often we will see such things as "support@ mydomain.com" in a config (shows that at least one team member can cut and paste from the Internet).

Before handover, we insist that all the Type 7s are replaced with Type 5 passwords as much for our own protection as our future customers (yes, there are servers that use the same admin passwords as the switches and routers). Much of the time, these teams complain that they won't make the change (actual word they should use is "can't"). This is depressing. Sometimes you will get one of their team who is eager to make the change, and you find that he has been trying to make the network resemble something from the mid 90s, but has been prevented by a manager who things that RIP is still the protocol of choice (and VLANs are something that the devil sent to plague his dreams of flat networks).

The situation as Cisco explained it late last century:

Back in the dim dark days when I first attended Cisco courses (1996), we were told that Type 7 was not an encrypted password, but an obscured password - the sole purpose of Type 7 was to protect the password from shoulder surfing and that it was only used for legacy configurations (CHAP handshakes being on the list of security offending legacy excuses, as I remember).

It was stated that Type 5 was always to be used. This was long before the SANS statement in 2000 that there was an issue.

The reason the Type 7 still haunts us is more due to retarded network teams who don't remove Type 7s and complain when noises are made about removing the POS which are Type 7s.

We had a group of engineers on one multinational telco on a course who got upset at the mention of removing support for Type 7 passwords, as there would be too much work to do <sigh>.

Here's an example of what clueless network teams do:

In case you don't know, BGP means Border Gateway Protocol. It is only used on the borders between networks (by normal people) and is incredibly slow to propagate routing changes as it's only supposed to have a very limited number of neighbors to deal with.

They also boasted that their customer solution (what would now be termed a "cloud") was running solely on BGP (hundreds of devices which were allegedly fully meshed). They insisted that there was no potential issue, I can only describe the tutor as being upset and that turned to annoyance when the "network engineers" got increasingly arrogant about their solution being correct.

Come Thursday lunchtime, a phone call stated that a pair of their routers had problems and there were problems with BGP working its routes out. We finally saw the engineers on Friday afternoon when their network had finally converged and their network was mostly operational. It took a full seven hours for routing changes to propagate through the network every time a device went up or down.

They later stated that it must be a Cisco issue as they were sure their architecture was perfect.

I would also avoid the use of the term hash. At best, it's a Vigenere (and a poor example), with the start position prepended at the beginning of the "encrypted" value so you know where to start in the ring buffer.

Hell, I even wrote a Z80 assembler password ("decloak") when I was bored in the hotel (alcohol fueled rampages didn't appeal) and that involved working out the initial values.

The recent Type 4 plume of excrement is a different matter though, and is one all of Cisco's own making, but typical of using offshore coders.

Kilby

Dear *2600:*

I'd like to express my thanks for including the article "Why You Need a Grimoire" in 27:2. The evolution of my grimoire is an interesting story, and I thought I'd share it.

In 2010, when I first read the article, I had already noticed the transient nature of the Internet (how information could suddenly vanish on a website with no warning). I had printed things out before, made screenshots of websites but, until the Grimoire article, I had not done anything permanent with my notes.

First, I had to get something permanent. I ended up going to Wal-Mart and getting a three-ring Five Star notebook, neon pink (possible bad judgment, but I was going through a neon color phase at that time). I could put about 200 pages of notebook paper in there. For website screenshots and printouts, the notebook also came with a hole punch. It also had a pen and pencil case inside, which was useful for storing writing implements directly with the grimoire.

The first printout I put in my book was a copy of the "Why You Need a Grimoire" article (which has always been on page one). I carefully copied all my loose work into the notebook (first edition was in pencil because I wanted it to be easy to erase and rewrite things). This first edition lasted from the summer of 2010 until about the winter. Eventually though, I had eraser marks all over every page, and I realized the need to have something more permanent.

So, for the second edition of the grimoire, I copied everything onto new sheets of paper with a ball point pen. This edition expanded to about 40 college-ruled notebook sheets. The second edition lasted until autumn of 2011 when my wife, innocently looking for some scratch paper, unzipped my grimoire without actually looking inside and removed a bunch of filled sheets of paper. I nearly had a heart attack! I taped a sign on the cover reminding anyone who looked at it that this notebook was mine, and not to remove any pages from it.

I was able to get everything recopied back into my grimoire (I count this rescribing as a separate edition because I reorganized some of the notations and entries, and excised some of the completely out of date material). This was my third edition.

At this point, I was getting some notoriety in my local area as the best person to call if you had a computer problem. Most people, without even realizing it, referred to me by my grimoire, which they had seen me use on occasion. They would recommend me to other people with the words: "Call that nerd with the pink notebook." (I laugh now, still pondering what moved me to get a neon pink grimoire.) Most of that notoriety I owe to the initial *2600* article; I wouldn't have been nearly so good if I hadn't saved all my research and notes in my grimoire. The third edition has lasted the longest.

In fact, I just started on the fourth edition of my grimoire now in the summer of 2013. I discovered that printer paper is slightly thicker than college ruled notebook paper, and does not rip as easily. After several years of flipping pages in my grimoire, my pages were getting worn on the edges and especially around the ring holes. But I had noticed that the printouts I had inserted into the book years ago had not frayed around the ring holes quite so badly (if at all!).

The fourth edition of my grimoire is still packaged in a pink (slightly sunburned, so not quite as neon as before) Five Star notebook. For this edition, I typed all my notes using LibreOffice Writer and I printed them, then used the hole punch that came with my notebook. These printouts make the book the neatest edition I've ever used, with multiple easy-to-read fonts (much easier than handwriting!), and neat margins. I've discovered that using fonts is much more convenient than handwriting because, since I can read smaller fonts, I can put more on each page than I could before when I was writing everything.

I look forward to the future. I wonder how long the fourth edition will last....

Thanks so much for the informative articles you include in *2600!* I so very much enjoy reading them, and occasionally copying an article to be preserved in my grimoire.

Sean Murphy

Dear *2600:*

In your editorial "The Road To Safety" in 30:2, discussing the Boston Marathon bombings, you state that "having... information gathered and managed by members of society rather than government eyes makes it far less of a threat to our freedom." This is a dubious conclusion to a highly nuanced issue. You ignore the significant threats posed to society by an army of highly-connected Internet vigilantes who take it upon themselves to carry out the duties of professional public servants. Witness the aftermath of the bombings, when a single tweet - claiming that the name "Sunil Tripathi" was heard on the Boston police scanner - led to an eruption of speculation on social media about the innocent Mr. Tripathi and completely unnecessary pain for his family and friends. Thanks to the infinite memory of Google and other archives, online slander will never be forgotten; thanks to a "relevance score" that values retweets, links, and clicks, it will always be at the top of search results about a person, far above the otherwise boring digital record of normal life.

In the end, the desire for fame and Reddit karma by egotistical, Internet-savvy individuals may cause far greater harm to innocent members of society than government programs subservient to laws made by elected members of Congress. We can throw the bums out, but the Internet caucus is unelected and beholden to no one.

As a magazine with historical credibility on the issue, *2600* owes to itself and to its readers a more balanced evaluation of the threats to our privacy.

t. heride

There is certainly much evil that can be accomplished through mob rule and mass stupidity. In the instance we cited, however, many eyes looking for a specific instance of suspicious behavior on cameras they themselves owned and operated (hence being limited in total content) seems a far better scenario than one set of government eyes looking at everything for us. The Twitter/Reddit incident you refer to clearly showed the difference in value between journalists doing actual research and a large number of uninformed people spreading misinformation. This is a threat of an entirely different nature. There are definite risks everywhere, but the risks of a surveillance state are among the worst.

Dear *2600:*

This letter is in response to Tim's letter in 30:2, in which he proposes producing audiobook versions of the magazine. I would be interested in participating as a narrator. I have done previous voiceover/voice acting work, I am familiar with the technical vocabulary and terminology used in the magazine, and I have a pleasant (female) speaking voice.

Jax

If this project moves forward, we will certainly be in touch.

Dear *2600:*

I just wanted to say that *2600* is an epic magazine. It seems that nowadays the hacking and phreaking community - phreaking mostly - has almost died a little, at least in the sense that "hacking" is now "what prepackaged software can I download to hack a Facebook account?" except for a few forums. But *2600* does the best job of preserving hacking culture. This seems strange considering I'm rather young, but just my thoughts. What I'm most concerned about in the community however is phreaking. It seems that many on the net consider phreaking to be dead and/or worthless, and it's hard to find any good material on modern day phreaking, a field which I was interested in taking part in after some hacking endeavors. *2600* breaks away from the monotonous trend of disappointment I find when exploring the "hacker community" on the net. Just my thoughts.

Keep up the good work, *2600!*

Blank Electron

Consider that much of today's telephony wouldn't be around were it not for phreaking and the people who decided to explore the phone system, manipulate it, and eventually come up with something better. There's no reason that has to stop, simply because the landscape is virtually unrecognizable. Phreaking was always about bypassing restrictions and exploring forbidden territory. In today's cell phone crazed society, there are tons of restrictions and lots of hidden areas to explore. If anything, it's the fact that there are so many different systems to mess with that makes it more difficult to define than when it was just Ma Bell. But being difficult is nowhere near being impossible. The world of telephony has come to an interesting place. Let's work together and use the values of phreaking to take it somewhere else.

Dear *2600:*

Re: Cortland letter, 30:2, they have been selling the Cap'n Crunch Bosun whistle on eBay. Lately, many of these have been for sale with the prices varying from $17 to $45 for the auctions. I looked last night and one was for sale for $70, but this is an anomaly. You can search under "captain crunch whistle" and "cap'n crunch whistle". I hope you are able to find what you are looking for.

Charles Parker, II

Dear *2600:*

I'm not entirely sure where this question should be directed, so I'm taking a shot in the dark....

A little over a decade ago, I was introduced to *2600* by a good friend. My very first issue was Spring 2002. Since then, I've been a fairly regular reader, picking up copies at my local Barnes & Noble. I've always been curious about back issues, particularly from the first few years, but never followed through on that curiosity. Then, a couple of days ago, I was delighted to discover the digital digests, Volumes 1 and 2. I was like a kid in a candy store - and I truly hope you continue with the digitizing of each year's issues! But I digress; back to my question....

In the description for the digests, it is stated, "This is not just a scan of some old back issues. We've literally gone through every article and every piece of data and arranged them in a brand new book form, divided into articles, news stories, letters, and data." My question is this: is it possible for *2600* to actually do that - scan old back issues so readers that delight in text formatting and the printed page might get a glimpse of the actual physical copy that represents the origin of a beloved and treasured source of information and ideas?

Surely I can't be the only reader that would be interested in such a thing.

Something to think about.

RJC

The PDF versions are just that - a scan of the printed pages. What's different is that they've been arranged so that each year reads like a book with letters being in one section, columns in another, etc. The Kindle version also is in this format. We could just scan the issues and stick those online, but we want to also OCR them and have them be accurate so that the text can be searchable. The quality of type on those early issues along with the quality of existing OCR software makes that very difficult, which is why it takes time and money to pull this whole project off. We're always looking for new ideas and for easier ways to accomplish these things, so please keep writing in with suggestions.

Dear *2600*:

Re Shea Silverman's Raspberry Pi article, although this was a good first look at this "gaining popularity" device, there is a *warning* that should have been added. The power supply for this device *cannot* be more then 1A *max*. For some reason, *it will destroy the processor!*

For more information on this, see Ron Hackett's article in the August 2013 *Nuts & Volts* magazine for a full explanation.

pixter

On Privacy

Dear *2600*:

I became a Google product user, not by choice, but because it was easy to use. I used sdf.lonestar.org as a base for a decade maybe before doing the terrible switch. I had my first account there during the second half of the 90s. I was trusting the admin, the system was working perfectly, the community was great, it was OK. Then - things changed a bit.

Around 2005, I went back to school. I was trying to keep going with tcsh shell and mutt email, but it was not easy. I was receiving many emails with massive attachments, at an increasing rate with all of the MS-Office formats - *.pptx, *.docx, *.xlsx, or whatever. It went pretty fast with mutt, save this and that, scp all the files on my box, edit everything, save, scp upload + mutt + attach + send and voila. But I realized that the average non-tech-savvy students were doing the same thing much faster than me, with multiple gigabytes of storage in the cloud from *any* computers while I had only a couple of hundred megabytes and was kinda restricted in the computers I was able to use to do that.

Then Google. It was a great alternative to Microsoft at the time, the not so bad guys who were doing many things right. When Yahoo Mail and MSN offered 100 megabyte mail accounts, Gmail provided two gigabytes. They had plenty of apps, calendars, meetings, searches, integrated online storage, engines, small non-obstructive ads, etc. It worked perfectly for the higher education world in my eyes.

In addition, in 2009 or 2010, I bought a Google Nexus One Phone with everything integrated - contacts and stuff. It was easy to integrate, but I knew where this was going. I refused to use Facebook for that reason (no Mark Z., you don't need the contacts on my phone and no, you don't need my phone number). iOS, I just cannot stand this shit. About each year after, there was a new TOS from Google that we had to accept or stop using their products. A kind of erosion of our privacy, like the centralization of all the services under one username. I guess I was able to cope with it, but it still stink years after.

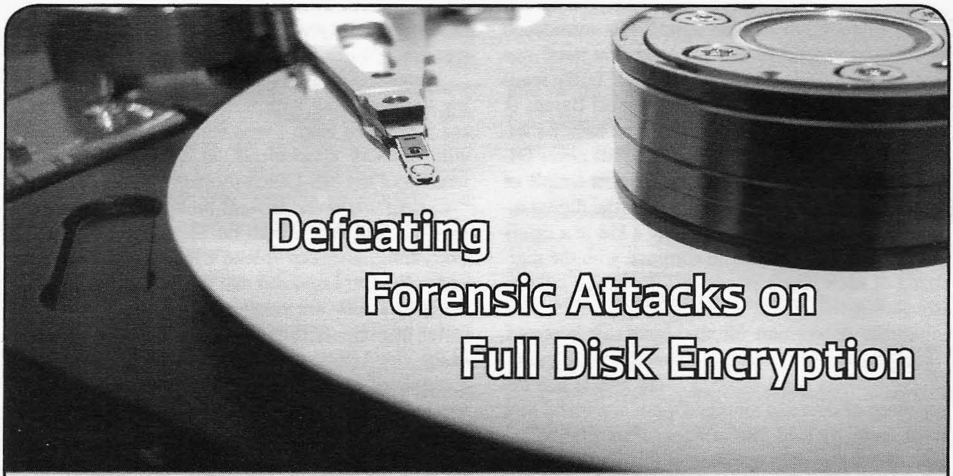
For my research, I am required to go for several months in remote places on desert islands almost alone where there is no Internet at all, only an Iridium data/voice link (which is pretty costly). I left in May 2013 and was back at the end of July, and heard the leak from Edward Snowden. Then things escalated quickly - and I was pissed at many things. I think it is the straw that broke the camel's back. I want to get rid of Google from my options. I want my privacy back.

I feel like I'm in a kind of trap - I don't know where to start. And I knew it back in 2006 when I moved everything that it would be that way.

And still, I know no one in the couple of hundred email contacts I have who would be able to send me an encrypted email or who would be able to decrypt one I send them.... Heck, I know no one who owns a PGP/GPG key. I feel like the road will be long. Now what?

Let's get to work.

flax0r



Defeating Forensic Attacks on Full Disk Encryption

by MoJo

With the rise in use of full disk encryption tools such as TrueCrypt and BitLocker, the forensic community has developed a number of techniques to recover the keys required to decrypt protected data. While at first these attacks may seem powerful and hard to defeat, there are actually many simple and practical steps that will provide full protection if followed.

Cold Boot Attacks

A cold boot attack requires the encryption key to be in memory, i.e., the encrypted drive is mounted. The attacker performs a hard reset on the machine and loads an attack tool, say from a USB drive, that dumps the contents of the computer's RAM. The attacker can then search through the memory dump for the encryption key required to unlock the drive. A simple way to mitigate this attack is to prevent the BIOS from booting off USB drives or CD/DVDs, in fact, anything other than the internal HDD. Remember to password protect the BIOS settings themselves. Unfortunately, the attacker may be able to reset the BIOS using a hardware jumper, and by default most will boot from CD. As such, a better option is to get a motherboard that wipes all RAM on reboot by default. Apparently, motherboards that support Microsoft's "TCG Platform Reset Attack Mitigation Specification" do this, but I have yet to see one. Many server motherboards will perform a full RAM write/verify test though, and the few Intel ones I have tried do not allow you to abort the test.

Remanence Attacks

Remanence refers to the way that DRAM retains its contents even when power is removed for a short time. Because of this, it is possible to perform a variation of the Cold Boot Attack where the RAM is physically removed from the computer and placed into another one, which is ready to boot up some forensic key recovery software. The only defense against this attack is to either prevent the attacker getting at your RAM while the encryption key is stored in it or to make the RAM difficult to remove. The former can be accomplished by never leaving the computer alone with encrypted volumes mounted, and having an emergency "dismount all volumes and wipe keys" function if a surprise raid is possible. TrueCrypt has that feature, no doubt popular with unpopular Chinese activists. You can use a keyboard shortcut to activate the emergency dismount, but on most computers simply pressing the power button will begin a controlled shutdown that dismounts all drives and may be the only option if you encrypt your system partition.

Physically protecting the RAM can be a bit tricky. Firstly, the attacker will probably try to open the case with the computer still turned on, since as soon as power is cut the RAM will begin to lose data integrity. They have only seconds to transfer it to a different computer. Server motherboards often feature a "case open" switch that can detect opening of the case and start an emergency shutdown, so wire it up if available. Server cases often have additional internal covers over the RAM area to channel air for cooling, and stripping the heads on the screws or even just using a mixture of random security bolts can really help slow an attacker down. Finally, you can always glue the RAM into the sockets, ideally with superglue but hot-melt will buy some time. In fact, I have seen eBay sellers use hot-melt glue to prevent RAM and various cables falling out during shipping.

If you are buying a new laptop and are worried about this, consider getting one with non-removable, non-upgradable RAM, such as an Ultrabook. Typically, they are very hard to open up anyway and the RAM is soldered directly to the motherboard.

DMA Attacks

Direct Memory Access, or DMA, allows devices other than the CPU to directly access the contents of RAM. Firewire, Thunderbolt, and PCI/PCI Express all support DMA. Most laptops will have at least one of these (PC Card slots are actually just hot-plug PCI/PCI-E ports). Digital forensics companies sell devices that connect to these ports and allow the contents of RAM from a live system to be dumped to another for analysis and recovery of encryption keys. Forensics guys love these tools because even if the computer is locked, it will usually happily accept their Firewire/PC Card device and load a driver for it, and then they have access to things that an offline analysis would never get them and full control over a live system. If you happened to be logged in to IRC at the time, they could start pretending to be you, for example.

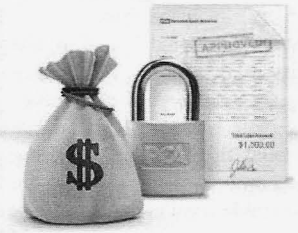
Mitigation is as simple as disabling the device in your OS of choice. Fortunately, even when disabled, the DisplayPort part of a Thunderbolt port usually still works. Remember to disable the PCI/PCI-E host controller for your PC-Card port, rather than any devices you have plugged in to it (which obviously will no longer work).

Hibernation File Attacks

When your Windows PC hibernates, it saves the contents of RAM to the hibernation file. If you encrypted the system partition where this file lives, then you have nothing to worry about; it is inaccessible. If you didn't, then you either need to disable it ("powercfg.exe /hibernate off" in an administrator level cmd box) or use BitLock's TPM+PIN option. The latter makes sure that the encryption key is not stored in the hibernation file, instead living in the TPM module where it is supposed to be secure and protected by a PIN number. Of course, you have to trust the TPM chip manufacturer on that.

It is also a good idea to avoid sleep mode. In sleep mode, the contents of RAM, including any encryption keys, are preserved. Remanence attack mitigation will help, but why take the chance?

Good luck.



BANK NOTES

by lg0p89

It's a Wonderful Day in the Neighborhood... To Go to a Fake Website

The following may or may not be based on actual events. This is intended only as an educational tool.

At the bank I work at presently, there is the usual firewall, IDS, and IPS in place in addition to other measures to prevent the deviants. While sitting at work at ye olde bank in mid December 2012, a quarantined email message popped up on the system. This was just before lunch-imagine that. This actually is unusual. There is maybe two a year that get to this point, so, from a ratio analysis, this is a significant event. Naturally, since this was out of the ordinary, I took notice and gave this a bit more attention than the normal email.

The report itself was very bland, merely stating the minimal amount without any details. The only thing I knew at this point was an email to me was quarantined. The reason was there was an attachment type policy violation. This piqued my curiosity as I was pretty sure what was to come. The actual attachment was Recent_Activity.exe. Upon seeing this information, the issue was obvious. The email was not opened in the operating environment, but was viewed in the quarantine area. The body of the email stated *"As part of our security measures, we deliver appropriate monitoring of transactions and customers to identify potentially unusual or suspicious activity and transactions in the American Express online system. / Please review the "Suspicious Activity Report" document attached to this email. / Your Cardmember information is included in the upper-right corner of this document to help you recognize this as a customer service e-mail from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at http://www.americanexpress.com/phishing / Thank you for your Cardmembership. / Sincerely / Tasha_Dennis / Tier III Support / American Express Account Security / Fraud Prevention and Detection Network"*.

The email appears to be valid. It lulls you into a false sense of security (as any good social engineering would) with the Amex symbol, the person's name and department they work in, and the Amex website for phishing attacks. After all, it is not logical for a phishing attack to list the alleged company's phishing warning site. This must be a valid website (as read by the average user).

If you simply glanced at who the email was from and the body of the email, you might believe this was valid and authentic. Well, there are a few items that would raise the big ole red flag.

First, the email is intended for a single person (as it is read). After all, the attachment was for a "Suspicious Activity Report," which would need to be for a person. The distribution was actually to eight people. A bit strange. Also, all eight people work at the bank, but in different areas. The eight people also are higher up in the organization (you can tell by their titles) and not tellers, so their access to sensitive data is greater. It appears as though the email addresses were harvested from the bank's annual report, which listed the employees, their position in the bank, and their email. This specific issue has been addressed with management - to no avail.

The attached file was a .exe file. This is not normal. The file with a suspicious activity report would be a .pdf and wouldn't need to be a zip file or .exe. For what they were sending, an .exe file would be highly suspicious and worrisome. There was no reason to have an .exe file in the email.

Also, the bank does not use Amex for the corporate cards. Most use one of the other two primary cards in use (Mastercard or Visa).

Last, but not least, is something rather odd with the sender. The sender did appear to be from Amex, but this was spoofed. The sender actually was message@securebank.com.

If you receive an email that does not apply, e.g. an update on your Amex card when you don't have one and your corporate card also is not Amex, there may be an issue. Don't give in to the natural curiosity urge to open this email.

Instead, question authority. Look at how many recipients there are for the "personal" email. If it doesn't make sense, there is probably an issue. Don't press the button. Please use this as a learning experience to teach your friends and staff what to look for.

Does Every Cloud Have a Silver Lining?

This is written more for the small- and medium-sized business ("SMB") needs. Cloud, cloud, cloud, cloud. Week after week, it seems as though there is at least one story in one of the industry journals about the cloud. Given my and our interests, I tend to focus more on the security aspect of this. With any project, there are the positive and negative aspects to consider. There is no yellow brick road. There are two camps: the group that wants to keep the security function within the business and the group that wants to have this security in the cloud.

The service providers would like all of the company's security aspects in the cloud, as it brings everything under one roof and subsequently increases their revenue. If I did not know better, I would think they were being altruistic. Certain portions of the security are handled on an acceptable level in the cloud, e.g. email. However, the network security should still be handled on-site. The amount of confidential data processed and stored by businesses and banks can be massive. Couple this with the amount of potential liability from the clients whose data would be compromised and the seriousness is intolerable. There also is the risk of the data moving from the site to the cloud, adding a new avenue of attack and risk. At the local level, the next generation firewall and IPS are perfectly engineered for the local use.

From a purely operational slant, the command and control at the local level simply makes more sense. The local network administrator ("N/A") is able to monitor the updates quicker. As the N/A arrives at work, the N/A can take a quick look at any updates and see what needs to be pushed more quickly than others. This is much more like a triage in a hospital. Also the N/A does not have to wade through the 300 + emails that came in overnight, as may occur with a provider. There is a great disparity between the number of emails received at an SMB and a global cloud service provider.

With local control, there is a quicker response for updates and patches. For example, the N/A receives an update or patch during the work day. The N/A can review the update or patch to analyze its impact, if any, and how serious this is. With this process at the local level, the patch management does not have to get the push approved through two or three layers of management. The endgame also has to be reviewed. Say a breach occurred. Any breach would carry an immense amount of potential liability and also a massive hit to the community rapport. For an example to think about, let's look at a small community bank. There is a security breach as the data is transferred from the site to the cloud. This naturally consists of the client's name, address, SSN, deposit and loan numbers, and balances. There is everything you need to assume the person's identity except for a physical signature. This could be social engineered, but that is another story. Once the clients are notified of the breach, they wonder, as any of us would, how safe their personally identifiable information really was, and how safe, if at all, their money will be. The clients would quickly and assuredly begin to move their business (aka money) to other institutions.

In summary, security is one function that should be handled locally at the business for the SMB. Since it is easier to offload this onto a service so there is one less headache, don't do it. You may never have an issue, but if you do, the next step is to brush off the resume, as you now have a resume updating event.

Not every cloud has a silver lining.

A Little Bit of Research Helps Immensely...

I write mostly about social engineering. This is intentional. This area just seems to be a bit more interesting than the others. Coding malware or a virus ends up in a rather direct attack. The person targets a company and sends these along hoping for the person at the other end to bite on the hook (open the email and click on something not so nice). Social engineering requires a certain level of nuance and being slick to accomplish the task.

It was another day in the neighborhood at the local bank. A call, much like any other call, came in. "Hello, this is _____ from EMC." The droll IT manager that fielded the call simply responded, sounding like Lurch from *The Addams Family*, with "Yes." The EMC rep responded with "I see you are using some of our products." Along comes the same response from the IT Manager "Yes." The EMC rep asks "Can you tell me what you use?" After a brief hesitation, explanation to follow, the response was "No, you should be able to see what we use." Still more hesitation. The EMC rep slowly responds with "Well, we are working from our back-up now and can't access it." From this point forward, the conversation was curtailed abruptly. As a disclaimer, the IT manager is not a rough person with too little time and too many projects. He is a great person with too little time and too many projects.

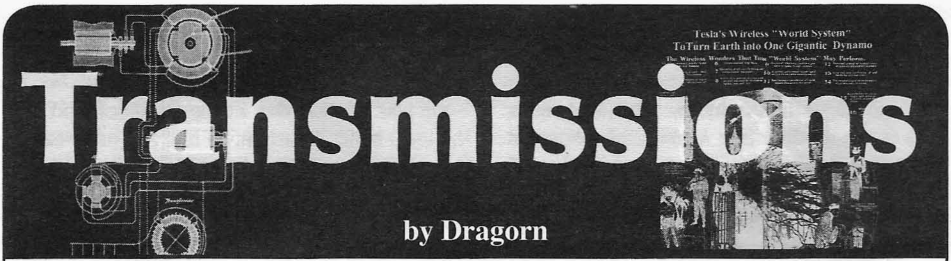
The short answers were intentional. Social engineering is not a full frontal assault like a DDoS. You get a little information here and there. After enough data in bits and pieces has been gathered, you have a better feel for their OS and other systems, which then gives you a better road map for the attack. The strike on the target then is rather specific in the tools that are to be used. We have been trained to not give more information out to people unless you specifically know the person. We know not to give the information out to anyone just calling in.

The second red flag was the EMC rep not knowing what the bank was already using and purchasing. Even if the rep was using a back-up, he still should have been able to see what the bank was using. This was pretty blatant.

The third strike, I mean red flag, was obscured as the call came in. The Caller ID did not show the number and the ID showed not as EMC, but as "Out of Area." The number could at least have been spoofed.

It is so much better to be conservative and not divulge private information they should know anyway. It would not have taken much for a person to simply answer the questions, but this would have provided far too much information, which would have been a benefit to the "EMC rep."

Thought for the day: "Via trita est tutissima."


Tesla's Wireless "World System"
To Turn Earth into One Gigantic Dynamo
The Wireless Wonders That Tesla "World System" May Perform

Transmissions

by Dragorn

For what should be obvious reasons, security, cryptography, anonymity, and identity protection has become a bit of an issue in the past few months. Unfortunately, security is hard, cryptography is harder, and now that it's suddenly in the press, everyone is jumping on the encrypted, anonymous communication bandwagon.

There are two main concerns when considering what encryption tools are appropriate:

Of prime concern should be: What is the impact of failure? The requirements for a hacker are different than the requirements for a political dissident or a corporate worker. Not only are the challenges faced different, but the risks of compromise can range from lost money and embarrassment to possible imprisonment or even death for political dissidents in some parts of the world today.

Secondly, who are your adversaries? Hard drive encryption, for example, provides excellent protection against a stolen device, but questionable protection against legal methods. Case law is still being built, but it seems reasonable to say that unless prolonged detention for contempt of court is preferable to the results of decrypting a drive, it's unlikely to save you in criminal proceedings.

Similarly, it is relatively simple to provide local anonymity - such as obscuring your destination and identity from snoopers on a local network at a conference or other presumed hostile local network. It is much harder (and possibly impossible at this point) to provide total anonymity between endpoints on the Internet if the snooper is able to grab a significant percentage of connection data, as it is claimed the U.S. government is able to do. Even long-standing cloaking services such as Tor may have vulnerabilities when an unknown number of internal nodes in the network are controlled by a hostile agency.

Both of these must be considered when looking at what tools actually offer:

Firstly, validation: How confident are you that who you think you're talking to is who you're actually talking to? How do you verify this? For secure communications to take place, you *must* be able to verify that you're communicating with the proper entity, even if this validation is simply "have I communicated with this entity in the past?"

Without validation of the endpoints, it's impossible to know if the encrypted session is between yourself and your intended, or between yourself and a man-in-the-middle attacker. Validation of remote systems is supposed to be one of the advantages of SSL - we all trust the root authority servers to only hand out certificates to authenticated and validated entities - unfortunately, the combination of security breaches and government intervention has made the safety of these mechanisms highly suspect. It's not unreasonable to assume that top-level SSL authorities have been compromised or have provided universal certificates either voluntarily or under subpoena.

Validation is so important, some tools offer it as a stand-alone feature - for example, PGP or GPG signing of emails provides validation of the author, while providing no encryption at all.

Anonymous message passing systems such as OTR still implement recipient validation - by requiring you to validate the user via some out-of-band mechanism and then authorize the key. The same trick is used by SSH when connecting to a server for the first time. Little can be done about securing communications without a method to validate the identity of the recipient.

For actual protection of content (or protection of content beyond the initial handshake), the data must be encrypted using something derived from validation of the recipient. In the case of SSL, the handshake validates the certificates of the endpoints and then creates a new, temporary key, used to encrypt the traffic. Any system which claims to validate the sender of a message *must* include validation of the entire message, validation of each message block in a stream, or must encrypt the stream.

The problem nearly all encryption systems face is that to communicate over the Internet (or to make a phone call), you need to send non-encrypted data - source, destination, and so on. The collection of this metadata is at the heart of the controversy about governmental spying - even assuming that the government isn't able to break the encryption (which is a dangerous assumption), it's possible to build webs of interactions between people.

Email and instant messaging are even easier to track - an encrypted email has "To" and "From" addresses in the clear, as well as the IP of the sending server and any other headers that might be included (like email client, which can reveal OS version). Instant messages include whatever account data the service places on them. While it's possible to hide *what* you say, it's far, far more difficult to hide that you're saying *something*, and *who* you are saying it to.

This can be a concern even on a local network. For example, if you're at a hacker con, you probably don't want to be connecting to your home system, no matter how good your security. At the very least, domain records can identify you in a situation where you might not want to be identified. At the worst, you've led a hostile audience directly to your door. While relatively easy to mitigate on a local network, it can be extremely difficult to address when combating Internet-wide surveillance.

Let's consider some standard encryption and identity protection tech:

Hard disk encryption: It's fantastic, and everyone should be doing it, but primarily it protects you against theft of the physical device. Since the hard drive is decrypted on boot, there is zero protection against runtime exploits. If someone owns your browser and gets all your files, it doesn't matter that when you turn it off, it's encrypted, does it? The value of drive encryption is relatively unknown when facing criminal proceedings, as there is very little actual case law. In general, it appears that in the United States, the Fifth Amendment protecting against self-incrimination has been ruled inapplicable when the authorities can already prove the existence of the data. In a current case, they claim the files were visible before the system was rebooted. Therefore, they classify refusal to decrypt as contempt of court. In almost any situation, the only time hard disk encryption will help in a criminal case is when the results of decryption are worse than possibly indefinite detention for refusing to decrypt.

Tor: The Onion Router attempts to protect the origin of communications by routing it through multiple nodes, protected with SSL, before releasing it to the Internet. The biggest flaw in Tor is - us. Insecure communications practices, like using the same browser for Tor and non-Tor purposes, expose tracking data like cookies, HTML5 storage, flash cookies, etc. It is unknown how effective Tor could be in cloaking activity if a government-level snooper can see a large percentage of traffic entering and exiting the Tor cloud.

VPN: VPNs are fantastic for obscuring local traffic, but don't do much to hide behavior in general. Unless you're paying for your VPN service in bitcoins somewhere, traffic is hitting the Internet from an IP connected to you. On the other hand, if your main goal is to prevent troublemakers on the local Wi-Fi from figuring out where you're going, an Amazon AWS micro server instance is free for a year and can run OpenVPN like a champ on an IP no one without a subpoena can track back to you.

PGP/GPG: The de-facto standard for encrypting files and email. They're great, but probably fall into the same problem as hard disk encryption. It is likely you could be forced to provide the means for decryption in a criminal case.

OTR: Off The Record, an instant-message encryption system, attempts to provide forward protection - each session is encrypted with a temporary key which is not kept. In theory, this can provide deniability, and the inability to decrypt past messages; of course, this counts on both ends of the conversation turning off local logging of messages. OTR can't do anything about hiding the fact that a conversation took place, but the contents will be protected.

So where does all this leave us? Basically, with no good options - nothing is guaranteed against government-level snooping of metadata, but we can at least protect *what* is being said. If you're in a high-risk situation, be *extremely* careful about what tools you use. Now that security is a hot topic, lots of unreviewed tools are appearing that claim to protect identity. Some are scams. Some are simply naive. In general, stick with well-known peer reviewed tools. They may not be perfect, but at least we understand more about where they fall down. If Tor hasn't fully solved the problem in five years, I'm pretty sure some guy making a random Android tool hasn't done it in a single revision.

by Wananapaoa Uncle

I spent the last 15 years of my life in computer security as freelance, visiting lots of different customers. Each one had specific setups, software, and network topologies; each needed some sort of security. The first point of this rant of mine is not about *why* they needed security - everyone has needs for security. The point is *when* they realized it.

You can study lots of papers discussing the security topic, each detailing aspects that may lead to some form of problem. You should prepare the networking ground by setting security cornerstones, redact documentation, teach people the right way to do things, and avoid doing the most obviously wrong ones. I found this way of doing thing is a pure myth.

Companies need security when they have a problem. I'm not talking about data that is compromised or systems that are shut down. Most often, I found the biggest problem was some sort of local law or rule coming into your business from outside. They require you to have some level of security, so you must adhere to them, and generally very fast. Companies fear fines more than intruders.

So now you're forced to implement some sort of security. You're forced to document that you comply with these rules. No matter how, you should be fast and not interrupt daily business that, of course, has its own rules that cannot be changed. So the first people who care about security are the legal staff. They find each aspect that can exempt them from complying with rules, sometimes generating lots of absurd technology-abstracted conclusions. Then come "external" companies to assess and document your infrastructure, with no connection to the way the network itself is utilized by users and applications. They normally ask for schemes they cannot understand, policies they aren't able to read, and bring with them "hackers" with black boxes full of antennas and lights that "assess" security.

They are masters, especially in Googling and cut and paste. So they Google for the wrong words, find the wrong references, cut and paste them together, and send this blob to a pizza-fueled-underpaid trainee who replaces the 256 different fonts with the corporate one, applies the formal template, and here you are: your very own security guidelines. First invoice is sent.

Now they will explain to you those guidelines, and will offer some costly service to tell you how to implement them in your business. And, of course, no one needs to know anything about your business. Second document ready - "Implementation guidelines" - and second invoice is sent. You're almost there; you have documents about complying with those absurd security requirements.

It may turn out that implementing security guidelines will be a little intrusive in your business. You have to rewrite applications to support those bizarre words called passwords, you can no longer send all of your sensitive data out to a contractor in Hyderabad, you should stop using good old FTP to send transactions to your bank. They sometimes state that you must change your password twice a year. Are you serious? My cat lived 12 years, and the new one has the same name as the dead one, so the password must remain the same. Also, my bride has her birthday set - I cannot change it!

So the customer discovers that he just put a lot of "effort" (say, money) into this ridiculous thing called security, and he should put a lot more of it into changing things? Are you serious? Of course, the big consultant has the solution! Just the final touch, the one I really hate. Really. You can solve all of your security problems by buying some specialized hardware. Of course, it should be enterprise grade. It must be highly available to not interrupt work when it miserably fails. It must be costly. The thing goes in and out of the IT department, encompassing people who make financial evaluations, and yes, in X years it costs less to buy some black box than revamping the infrastructure.

Here you are. You need a firewall, just to begin. What are you saying? Your old firewall? No, it's not "certified." Yes, you must buy new VPN licenses, and reinstall the software on each device, but you'll have a new "certified something." Just hope that the niche company that produces it doesn't go out of business too early, leaving you without the procedure to renew all the digital certificates (usually sent by mail to remote people).

Of course, you need an IDS/IPS. It looks in each corner of your network and finds the bad guys when they're doing bad things. This includes your corporate app that runs on the same port of Back Orifice, your database server that generates "abnormal" amounts of traffic, and IP phone traffic that can be a "hidden channel" for leaking data. Dozens of legitimate things are blocked. So you need a consultant to tune the box, of course, that switches from automagically adaptive to fucking costly. Of course, the IPS/IDS must be "trained" for each application you implement. To make it short, when the costly yearly contract ends, the device is put in "look-but-don't-do-anything" mode, creating an environmentally unfriendly electricity guzzler (but hey, your company is eco-friendly - certified by some obscure entity).

Another one that you must implement is the Data Loss Prevention device or software. It scans transiting data to find potential leaks. It kills your email containing any word it sees as sensitive, it uses "heuristics" to block your Excel offers, it trashes documents containing numbers greater than 99,999 (maximum value of your standard contract) - it's better that you break your phone numbers into small chunks if you want them in your commercial emails? You cannot use your USB drives anymore, or you need a support ticket open each time. You know the procedure - after one year, DLP is set to "silent" mode.

Then, you must solve the problem of all your people around the world selling your goods. Their laptop can be stolen, can't it? So you need to buy and implement full disk encryption to start protecting everything before the boot process. And how do you deal with people calling you via a phone booth in Kathmandu at 2 am your time telling you that they need the unlock PUK, or that the HD broke and they need their files back? Sooo simple! Just keep an unencrypted USB drive in the computer bag to back up the data daily, and a "do-not-open-if-not-really-necessary" envelope with the super-master unlock PUK of the whole company in it (taken directly from a customer policy for traveling workers).

So, a year afterwards, what have you got? Lots of consultants in and out (each of them having an admin password to "assess" your infrastructure), some rack full of blinking equipment (it is disabled, but corporate tours for guests must include blinking "firewalls"), and a (physical) folder full of awfully written documentation that no one will ever read (fortunately). But hey, we bought security.

I could have written hundreds of What-The-Fuck stories here, but there are sites devoted to this. I would like to stress how wrong the belief is that you can buy some black boxes and canned documents to reach the security Eden. Security isn't a product to buy; security is all about people's culture. You must put security into every action you perform at work and, of course, it is not only technology related (someone said Kevin?). Companies should *invest* money educating people more than they *spend* in buying assets. Maybe they will enlighten some dormant hacker mind, an asset between the most valuable ones.

CLOUDS, CLOUDS, CLOUDS...

by lg0p89

Disclaimer: This may or may not be based on an actual incident. All references are purely coincidental in nature, etc. [That should satisfy the legal department.]

Here we go....

In a small community bank, its assets and resources are very important. Without certain services, the bank simply can't function. For instance, the systems tracking deposit account transactions are vital. Curiously enough the bank's clients may actually want to know their balances. This is tough to believe! [Sarcasm.]

As they arrive at the bank and finish their respective transactions, there is a clear document trail. The Feds and Regulators would have it no other way. These tickets detailing the specific transaction are fed through a reader, verified for correctness and accuracy, and entered into the system. The client's account is then updated.

All you as the client see is yourself handing the check to the teller and the teller handing you $20. It seems awfully simple.

The bank I am presently, gainfully employed at used to do this transaction processing function in-house with bank employees. Senior management believed they could save a few dollars by outsourcing this. After all, there would be no employees associated with this function. There would also be no overhead, health insurance, paid time off, or other direct labor expenses. The pertinent service would simply be out there in the cloud.

With the numbers massaged around enough, it did appear as such.

Here Comes the First Shoe

All was fine and dandy until one of their servers failed. It just happened that this specific server had the bank's data. As it turns out, there was an incredible lack of redundancy, much to the bank's displeasure. We were down for a full day's business.

The clients could not get their balances, make online payments, etc. After many apologies and future promises of service, they were up again, which was great news. This should have been the end of it. Not so fast....

The Other Shoe Drops

The Romans declared to beware of the Ides of March. The system went down again. This time, however, the system was down for 1.5 days. This is generally [and definitely was] not acceptable on any plant or level of reality. This was no fun for anyone involved. There were still more promises from the provider.

Based on this second failure, senior management elected to take a closer look into bringing the service in-house... again. After a relatively short review, they decided to do this. There were clear cost savings and much more control over the process and equipment.

Lessons Learned/Re-Learned or Why the Cloud is Still a Bad Idea for Small- to Medium Sized Businesses

First, I do apologize for the run-on section title. The reasons for not adopting the cloud in certain instances are ample.

a) *There is a loss of control.* Granted, the service provider is contracted for the service, but what if something out of the ordinary happens? What happens if they were to file bankruptcy? Good luck getting access to your data within a week or two. When attorneys get involved, it seems as though simple requests get bogged down.

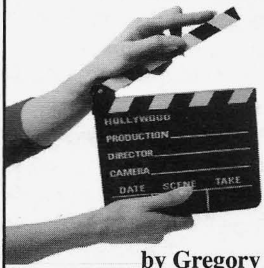
b) *You don't really know the condition of the service provider's equipment.* I don't know anyone in a small business who initially or regularly visited or visits the service provider to check on the equipment's condition. The client, or in my case the bank, solely goes on trust and what the sales representative claims. The equipment could be relatively new or ancient, held together with duct tape on the server racks. You quite frankly just don't know. They may or may not have a rotation/

replacement plan in place for the servers. The contracts generally don't have a specific equipment condition clause.

c) *If the system goes down, no way to know for certain how long it will not be available.* Granted, you have a contract, but what if a hurricane, for example, takes out the regional data center? Without redundancy, you are not likely to have a quick, readily available back-up ready to go in a few days. Even if the contract has a "Time is of the Essence" clause saying you will have an outage of service of no greater than 18 hours, this still may not happen. Granted, you could sue, but this may not help with your bruised view in the community.

At the end of the day, there may be the illusion that this is better, but due to the uncertainty we face every day and a lack of control, the cloud may not be the best choice for time sensitive operations but may be better suited for backing up family vacation photos and cooking recipes.

In-House 2 Cloud 0



Lights, Camera, Hack!

by Gregory Porter
backfromthemovies.blogspot.com

If you are reading *2600*, I'm willing to bet you've been asked by someone either "What is hacking?" or "Who are hackers?" Don't worry, I am not going to make a big commentary about the meaning of hacking. We, as a culture, have a tendency of thinking about hacking with regard to computers (I certainly did before I got into film). Hacking can be found in every facet of life. We just have to, well, hack our preconceived notions surrounding a subject. In this article, I will look at a place where hackers aren't often attributed: film.

First, I should specify how I use "hacker" and "hacking." There are, as I'm sure you know, a plethora of definitions, varying from "Hacking is unauthorized use of computer and network resources" [1] to "A hacker is an aesthete." [2] I and fellow readers will probably gravitate towards the latter. The emphasis, then, is not on computers but on an attitude. I have always thought of it as "making something function outside of its original design."

If we want to look at hackers in cinema, we should look no further than filmmakers. A film, after all, is largely about aesthetics, so we should look at what goes into making a film, particularly with regard to film history.

Now, I would like to examine one of the first cinematic-hackers, Georges Méliès, best known for his 1902 film, *Le Voyage dans la Lune* (*A Trip to the Moon*). He was thought of as a magician because he would make things disappear and reappear on screen, a trick he discovered when filming a city street.

While filming this city street, his camera ran out of film. He stopped and reloaded the camera with film. By the time he started recording again, a horse came into the frame (or camera's view). When he was looking back at the footage, it appeared as though the horse appeared out of thin air. He recreated this effect in his films to make a character disappear in a cloud of smoke, for example.

Méliès used the physical nature of film to his advantage, making a never before seen effect. But wait, I can imagine someone objecting because this was a coincidence. "It wasn't as if Méliès meant to do that." Have you heard of Captain Crunch? He discovered that if you blew the whistle found in Captain Crunch cereal, it made a frequency which allowed for free long distance calls. I hope if you are reading this magazine, you know the frequency of the whistle.

Méliès was an example of a technical type of hacking. He was able to take what was understood about film and what he discovered to make something new.

Let us talk about one more hacker, Jean-Luc Godard, and his first film *Breathless* (1960). Godard loved film noir (think *Casa-*

blanca) and wanted to make one as his first movie. But what does it take to make a film noir? You need a morally ambiguous leading man like Humphrey Bogart from *The Maltese Falcon* (1941), a man who "makes crime a career - and ladies a hobby." [3] He is tough and über-masculine, but isn't really that bad of a guy - he is just trying to survive in a hard, cold world. You need a femme fatale, a beautiful, black-widow of a woman who seduces men to compromising (sometimes fatal) situations [4].

On paper, this seems pretty straightforward and his movie seems to follow this structure. We have the car thief Michel and his lover Patricia who leads him to his death. In actuality, this movie inverts genre definitions and expectations [5].

How does the male protagonist, Michel, compare to Bogart? Before he became a car thief, he worked as a flight attendant which, classically, isn't considered the most masculine profession. Instead of being followed by a lover, he pursues a woman who isn't that interested in him.

Patricia is as close as we get to a femme fatale. Physically, instead of being a tall, dark woman with hard eyebrows and flowing brunette hair, she has a pixie cut. She doesn't seduce Michel for personal gain (she doesn't seduce him at all, quite frankly), nor is she the cause of his death.

The film's cookie-cutter structure on paper inverts all genre assumptions through its realization on film. Why did he do this? He was largely unhappy with the way films were being made and wanted to do something different.

Hacking is, as you know, just as much freedom of expression as anything else. Godard and Méliès were both able to break from preconceived notions surrounding their medium. This isn't, of course, specific to these two gentlemen. I just wanted to give you a taste of how hacking is present in film. More importantly, I wanted to illustrate how hacking is much more prevalent than may have perceived.

I love hacking and I love film and, with this article, I hope to move towards merging my two passions. Whatever your passion may be, happy hacking.

1. http://www.crime-research➥.org/news/05.05.2004➥/241/
2. http://www.cs.berkeley➥.edu/~bh/hacker.html
3. http://youtu.be/yRSCV➥2qc2IY
4. http://www.hollywoodmovie➥memories.com/articles/➥film-noir-articles/film-➥femme-fatale-role-holly➥wood.php
5. Brody, Richard. *Everything is Cinema: The Working Life of Jean-Luc Godard*

Fiction: The Error

by Zellie Y. Thomas

He was signaled by a simple beep.

Each time the firmware in his neural implant was updated, a tone was emitted informing him of the newly modified software. It wasn't a loud pitch, but a tone produced at the lowest frequency that a human ear could possibly hear. Despite that no one else could hear the beep, he glanced out his cubicle to catch any signs of arousal. "All that high-techery and they can't remove that annoying beep," Tim huffed.

The workspace cubicles formed an array populated with objects of approximately equal value. Each technician had a black suit with a modern silhouette. Some jackets lay draped over shoulders, but most covered the backs of chairs. Skinny black ties hung from the collars of their white shirts. And their shoes - the shoes were impeccably shined.

What separated him from the others was the small mechanism attached to the cortex of his brain. The micro sized device represented a quantum leap in human bioengineering. These implants contained electrodes that communicated with the brain through neuronal signals.

By linking itself to the networks of the brain it increased memory capacity and gave its user total information recall.

Thousands of citizens across the country had undergone surgeries to install similar devices. It was a costly operation, half the cost of an android, and affordable only to the more privileged members of society.

There were some doctors who performed surgeries or prescribed medicine without implants but it was a rarity. Children with neural enhancements achieved greater scores in aptitude tests. It opened the doors towards elite universities and advanced careers. Journalism, engineering, science, politics. All fields closed off to those without neurological aids.

And Tim had one.

He withdrew his fingertips from the keyboard and sat staring at the screen, wrinkling his forehead and blinking from the glare. He tilted his head and watched the data scrolling across the screen. It abruptly came to a halt and alerted him of an error. "You're like a walking computer, you should be able to figure it out." Tim never took his eyes off the section of computer code on his monitor.

His coworker joked on. "Don't try to guess where the bug is in the code, you could be a 'bit' off." Tim didn't answer. His colleague slowly sunk behind the drab barrier between them. He was gradually closing in on the error delaying the development of Xenith's latest project. The TRA-82 was a portable surface-to-air missile developed by Xenith and the U.S. Army. Each missile was equipped with a reprogrammable system to allow for innumerable updates. It had already been responsible for more than 100 aircraft kills. With an improved targeted system it could potentially record double that. The matrix of cubicles within the office produced a gentle hum of spinning hard disks. Each processor worked together to create the new set of software for the TRA. His fingers glided across the keyboard as electrodes began to communicate within his neural network. "A walking computer is right," he said to himself. The neuronal signals traveled throughout the lobes of the brain, flipping through consolidated layers of information. Without any external command, they stimulated his knowledge of computer programing and began its retrieval process. "I think I got it." After several strokes of the keyboard, he reclined in his padded chair. The computer crunched the thousands of lines of code. Tim closed his eyes with his hands behind his head and smiled.

When his terminal finished checking the data, it would only be a few months until it was loaded into a TRA.

"Looks like all the tests are passing. Knew you could do it, Tim."

Tim smiled hesitantly at the coworker leaning over the cubicle's wall.

"How much you think this program is worth?"

"Millions."

"And how many kills," Tim said. "How many more kills will the improved missile make?" "Hopefully hundreds."

Tim broke eye contact and stared at the "enter" key on his keyboard.

"So what then, a human life is only worth a couple hundred grand?"

"You should of thought about those things before you signed up for this gig."

The neurons traveled rapidly across his brain's hemispheres. They stimulated the brain in order to recollect an instant where he had once before rationalized the outcomes of his actions. He recalled nothing. Tim sat motionless. He stared at the cubicle's wall. A small section of its paint was peeling. He never noticed it before. He reached to push the paint back into place but it crumbled under the pressure. He faced his monitor.

"What's the matter, short circuit?" the coworker wisecracked as he rummaged through Tim's hair.

"I don't know what to do next."

"You upload and we celebrate."

"No," Tim clarified. "I'm confused about what I'm meant to do, not what I am supposed to do."

"Listen, how bout you just upload the code and go into sleep mode in the break room or something."

"I can't do this anymore," Tim blurted. "I need to get out of here."

The black chair rolled underneath his desk and coworkers began to rise behind the walls of their workstations. "What's going on?" "Where does he think he's going?" The last thing he heard before leaving the office was someone shouting his name. He gently pushed the elevator button for the ground floor and it began its descent. Tim watched as the LCD displayed the floor numbers in decrementing order.

"And now what?" he said with his finger still on the button.

The entrance doors of Xenith headquarters slid closed behind Tim. He unfastened the top button on his shirt and loosened his tie. Men similarly dressed crowded the sidewalks. He walked in the direction of Jimmy's, a popular cafe among Xenith employees.

There were many saloons and cafes along Main Street. Xenith established them, as well as residential areas on its property to keep tabs on its employees - though it claimed it was to service them instead.

Tim walked two blocks and stopped at an intersection. There was a commotion several feet behind him.

"Stop," a voice commanded. "Stop or I'll shoot!"

Tim staggered a few steps until his feet gained a faster pace.

"I didn't do anything."

Tim elbowed his way through a mass of people and sidestepped into an alleyway. He pressed his back against the brick wall.

"Because I didn't do anything, I've done something bad?"

He inched out from behind the wall. An officer with a gun drawn barreled down the sidewalk. His eyes began to skip around his surroundings for an exit. He saw a large dumpster, a chain linked fence and a fire escape.

"It's Officer Murphy of the Xenith Police Department. Tim, I need you to come out with your hands up," the voice roared.

"Maybe you have me confused with someone else. There are at least three other Tims in the department."

"We know. But you're the only one whose uplink went offline from the update today. Now, step out slowly."

Tim stepped out with his hands raised. "What are you talking about?"

"All Tims should be in constant connection with the Xenith's server."

"You want me to believe every Tim in Xenith was able to afford a neural implant? That's absurd."

The officer waited. He said, "There's no implant."

"What do you mean?"

"Just come with me, Tim," Murphy said.

"What do you mean there's no implant?"

"You're a TIM," said Murphy. "A Technologically Intelligent Machine."

"I don't understand."

"Now, just come with me so we can safely retrieve the missile code and - "

"No!" interrupted Tim. He made an awkward dash towards the overpass. Murphy fired his gun into the air; its gunshot reverberated under the monochrome sky.

Tim stumbled behind a black sedan. He patted his legs and upper body feeling for exit wounds. There was no blood. He was still alive.

"I'm not a killer," said Tim.

"No one said you were. We can straighten you out. Have you back working like normal."

"And I'm not - I can't be an android."

Clutching where he thought was his heart, Tim breathed heavily. "Just let me go," he said, trying to catch his breath. "You won't - you'll never hear from me again."

Murphy said, "Now, you know I can't do that."

There were a few people gathered around saloon windows. A man exited Jimmy's while putting on a black suit jacket. He walked to join a group of growing onlookers.

"There was a farm. Chickens, cows, but mostly chickens. On one of those days where it's so hot you can hear yourself breathe, a calf was born. A calf amongst all these chickens. All the chicks would crowd around. The cutest thing. The calf thought it was a chicken. Even sat on an egg once trying to hatch it. Local newspapers came down to cover it. A big sensation. A few years later they slaughtered it for ground beef."

"You need to come out with your hands up."

"I don't want to go back. I'm not going back."

The tone agitated Murphy. "You have no choice in the matter," he said. "You're an android, a bot, wires and circuits. You belong to Xenith Corporations."

"You're wrong, Officer Murphy." Tim rose from his hiding spot. "I do have a choice."

"Don't!" Murphy yelled as Tim leapt from the concrete overpass' barrier.

The smell of burning rubber lingered in the air as vehicles maneuvered around the body sprawled on the street. A few honked in frustration. Murphy kneeled next to a motionless Tim and ran an electronic device over his head.

"Like you said, Officer Murphy. There's no implant. I'm just Tim."

Murphy frowned. After a few moments of connecting wires, he svuccessfully reestablished Tim's connection to Xenith's server. And he was signaled by a simple beep.

HACKER HAPPENINGS

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

October 3-6
Maker Faire Rome
Palazzo Congressi
Rome, Italy
www.makerfairerome.eu

October 16-20
ToorCon
The Westin San Diego
San Diego, California
sandiego.toorcon.net

October 25-27
Pumpcon 2013
Best Western Center City
Philadelphia, Pennsylvania
www.pumpcon.org

October 26-27
Ruxcon
CQ Function Centre
Melbourne, Australia
www.ruxcon.org.au

November 9-10
Kiwicon 7
Wellington Opera House
Wellington, New Zealand
www.kiwicon.org

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

April 10-13
Notacon 11
Cleveland Marriott East
Warrensville Heights, Ohio
www.notacon.org

April 17-21
Easterhegg 2014
Kulturhaus Arena
Stuttgart, Germany
eh14.easterhegg.eu

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

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

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

Marketplace

For Sale

TERRIBLE NERD. I wrote a book about growing up geeky. I stole my first computer - from a church. Once, I crashed the Internet for all of Europe. You can probably relate. www.TerribleNerd.com.

PORTABLE PENETRATOR. Crack WEP, WPA, WPA2 Wifi networks. Coupon code for Portable Penetrator Wifi Cracking Suite. Get 20% off with coupon code 2600 at http://shop.secpoint.com/shop/the-portable-penetrator-66c1.html.

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

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Turning off TVs is fun! See why hackers and jammers all over the planet love TV-B-Gone. Don't be fooled by inferior fakes. Only the genuine TV-B-Gone remote controls can turn off almost any TV in the world! Only the genuine TV-B-Gone remote control has Stealth Mode and Instant Reactivation Feature! Only the genuine TV-B-Gone remote control has the power to get TVs at long range! Only the genuine TV-B-Gone remote control is made by people who are treated well and paid well. If it doesn't say Cornfield Electronics on it, it is not the real deal. Also available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! And for professionals, the TV-B-Gone Pro turns off TVs up to 100 yards away! *2600* readers get the keychains for 10% discount by using coupon code: 2600REAL. www.TVBGone.com

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

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

Announcements

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

Help Wanted

NEED HELP IN DECRYPTING A WINZIP DATA FILE, password was lost! Also, want any or all Facebook, LinkedIn, or social data with name, email, and/or photos. Contact Joe: soldato13@yahoo.com

HIRING TELECOM MYSTERY SHOPPERS. Need help collecting quotes from telecom providers by phone & Web scraping. Telecommute part-time from anywhere in North America. If you grok social engineering, enjoy VoIP hacks, use Excel, and can code a little, join us! Info: telcoshop@hush.com.

ARTIST AND PHOTOSHOP NINJA NEEDED. Small ebook publisher needs a Photoshop ninja/graphic artist/true artist to create 5 book covers during the next 5 months, and a further 15 covers during the following 18 months. We are not a big, greedy multinational publisher, so we will pay a reasonable amount, we will treat you with respect, and we will give you the credit you deserve. Our owners are longtime friends of *2600* and HOPE. Send contact info and portfolio samples, if any, to: librosfirst@gmail.com.

Wanted

AUTHOR WILL PAY UP TO $1,000 FOR TECHNICAL CONSULTANT re: *current* technical methods and tactics used to hack voice mail accounts, i.e. England, U.S., and elsewhere. cdg (dot) book (at) yahoo (dot) com

ALWAYS AVOID ALLITERATION. Fledging website on Cognitive Science language and thought seeks audience and feedback. http://alwaysavoidalliteration.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.

SUSPECTED OR ACCUSED OF INTERNET-RELATED CRIMINAL OFFENSES? Consult with a lawyer experienced in defending human beings facing computer-related accusations in California and federal courts. I am an aggressive Constitutional and criminal defense lawyer with experience representing persons accused of unauthorized access (so-called computer hacking), misappropriation of trade secrets, and other cybercrimes. I am a semantic warrior committed to the liberation of information (after all, information wants to be free and so do we), and I am willing to contribute pro bono representation for whistleblowers and accused hackers acting in the public interest. Past clients include Kevin Mitnick (million dollar bail case in California Superior Court dismissed), Robert Lyttle of The Deceptive Duo (patriotic hacktivist who exposed elementary vulnerabilities in the United States information infrastructure), and others who will remain anonymous. Also, given that the worlds of the hacker and the cannabis connoisseur have often intersected historically, please note I also specialize in defending medical marijuana and cannabis cultivation cases. Please contact me, Omar Figueroa, at (415) 489-0420 or (707) 829-0215, at omar@stanfordalumni.org, or at Law Offices of Omar Figueroa, 7770 Healdsburg Ave., Ste. A, Sebastopol, CA 95472. Complimentary case consultation. Stand up for your rights: "I respectfully invoke all of my Constitutional rights, officer. I do not consent to any search or seizure, I choose to remain silent, and I want to speak to a lawyer." Remember your game theory and the Prisoner's Dilemma: nobody talks, everybody walks.

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

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

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/

Personal

FREE GHOST EXODUS! I'm a 29-year-old hacktivist and independent writer looking to pen pal with others. I'm in prison for botnets. My interests include civil/human rights, activism, government accountability, music, art, religion, and info-sec. Hit Google up for my pics, follow my blog at cellblog.freejessemcgraw.com, email at ethernix@hushmail.com. Also see haxradio.com and electroniktribulationarmy.com, but don't forget to write me directly @ Jesse McGraw, #38690-177, P.O. Box 26020, Beaumont, TX 77720. Don't forget to use https://startpage.com (if you value your privacy). Power to the People. (P2)

ELEVEN YEARS DOWN, THREE TO GO. SWM, 5'9", 175 Brn/Blu prisoner seeking correspondence for friendship, contacts, proxy, with anyone over 18. Calling and snail-mail only now, but 25 cent email soon. There's no anonymous correspondence allowed. Sex and race unimportant. My past was very black. Incarceration made me pragmatic and understand loyalty. Time to change hats but I need help. I know some of what's needed to know to accomplish things. I can't wait until I can move. What am I? Because I can tweak a 98 registry, S.C. thinks I'm a hacker! What makes a hacker anyway? The government can't keep this Alaskan National down forever. It's hard but still learning. Interested in computers, tech, Linux, faith, sci-fi, everything that has connection to multi-generational self-sustaining networks, drones, makerbots, cybernetics, and stopping slavery. Important to me: open-mindedness, cleverness, and support for Bottom Billion. Let's drink a lot of coffee, relax, kick back, dream, and make something with what we have. I'm not seeking money in this ad. Uncovering answers to questions is my strong point now. World anarchy and meeting a Gray Hat hacker girl would be totally cool. Yes I said Gray Hat. Policy is that they open and read all mail. Address all letters as James Anderson and put 283022, TyRCI U6-9B, 200 Prison Road, Enoree, SC 29335.

CURRENT WEB-HOSTING PROVIDER looking for your help in this new digital age. I am currently locked up in the B.O.P., but I am due for release this October. I am currently accepting new applicants who have any knowledge of any of the following: domain registration, web hosting, IRC.IRCd hosting, SHOUTcast hosting, Ventrilo hosting, TeamSpeak hosting, VoiP hosting, cloud-based services, networking, server management, and more! This list goes on and on but will give more details on request. This opportunity will not last as we are limited on this great offer. For those of you who have written me a letter and have not heard from me, I apologize. A lot of letters don't reach me for some odd reason. I am willing to write to anybody even if it's not regarding this ad. A pen pal is nice once in a while. I reply to all letters received. Chris Douglas 14329-298, Big Spring FCI, 1900 Sim ler Ave., Big Spring, TX 79720. All mail is welcome. Write me as much as you like! Email is available, but I need your email address first.

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. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to subs@2600.com. Be sure to include your subscriber coding (those numbers on the top of your mailing label) for verification.

Deadline for Winter issue: 11/21/13.

Dear Readers: We screwed up last issue and printed an article that had already been published instead of the follow-up to it. To make up for this and to ensure that you don't lose precious pages due to our mistake, we are sacrificing our staff page and house ad to print the article that should have run last time. Sorry for the wait.

A Response to "Perfect Encryption - Old Style!"

by Phil

I enjoyed Cliff's article in 28:4; it's great to see someone bringing it back to the old-school pen-and-paper OTP methods of history. However, the article doesn't cover why/how it is possible for OTP encrypted messages to be truly unbreakable. Suppose I had infinite computing power. Couldn't I figure it out eventually, even if it took a long time? It's not exactly intuitive, so I'd like to try demonstrating how OTP works and why it's unbreakable.

To demonstrate, I'll introduce an OTP-based encryption method that I developed. It's more complicated than [plaintext + key] in order to give it flexibility: If the key meets the OTP requirements, it is perfectly secure; however, a less secure key can be used and it will still be very difficult to crack, due to the property of diffusion. To achieve this, my particular algorithm employs transposition with fractionation and substitution (in the form of combining the plaintext with key material via modular arithmetic).

For our example, we'll encrypt the following message: "MEET AT DAWN" with the key {38626973}. This algorithm converts letters into two-digit number equivalents, diffuses the digits, and then adds a numerical key to each digit to produce the ciphertext. As you follow along, note that this entire process can be completed without a computer at all.

First, we create a numerical alphabet so we can work with our plaintext, which is a string of numbers (the total length of which is divisible by two). The underscore represents a space (yes, even spaces are encrypted), and the numbers 0-9 are treated as two-digit letters as well. So, A becomes 01, B becomes 02, Z becomes 26, a space becomes 27, and the numbers 0-9 are represented by 28 to 37.

Hence, "MEET AT DAWN" becomes 130505202701202704012314 - that's our plaintext.

Now that we have a workable plaintext, we can begin with the first step of the two-step procedure: Diffusion. To do this, we take the plaintext and split it into groups of four digits, stacked on top of each other to generate a matrix of four columns and ((message length) / 4) rows. You might be wondering about messages that aren't divisible by four; you'd simply add a space (27) to the end of the message to make it divisible by four. Our example message is already divisible by four, so we can continue generating the matrix:

```
13 05
05 20
27 01
20 27
04 01
23 14
```

To diffuse this plaintext, we will work with the two columns on the left and the two columns on the right separately. Start with the top-left digit and move down in a zig-zag fashion:

```
1# 05
#5 20
2# 01
#0 27
0# 01
#3 14
```

So far we have 152003. Now, take the remaining numbers from the left-side columns:

```
#3 05
0# 20
#7 01
2# 27
#4 01
2# 14
```

Now we have 152003307242. Continue the same process on the right-side columns, starting at the upper-left digit, and we get the last half of our message: 000704521211.

So, we took our plaintext {130505202701202704012314}, and scrambled it into {152003307242000704521211}. Now, we apply our key using modular arithmetic:

```
1 5 2 0 0 3 3 0 7 2 4 2 0
➡0 0 7 0 4 5 2 1 2 1 1
3 8 6 2 6 9 7 3 3 8 6 2 6
➡9 7 3 3 8 6 2 6 9 7 3
-------------------------
➡-----------------------
4 3 8 2 6 2 0 3 0 0 0 4 6
➡9 7 0 3 2 1 4 7 1 8 4
```

"MEET AT DAWN" encrypted with {38626973} yields our ciphertext: {4382-6203-0004-6970-3214-7184}. (I like to split the message into groups of four to make it easier to read.)

We can already tell that this particular encrypted message isn't perfectly secure, because the key isn't at least the length of the message. Hence, it repeats itself and makes the message vulnerable to cryptanalysis. So, how do we achieve OTP security? The guidelines are simple in concept, but very difficult in implementation (hence the reason that OTP systems aren't widely used today - it just isn't practical).

To achieve OTP security, the key must be:

- Totally, truly random (pseudorandom numbers generated by computers do not count as truly random; numbers "randomly" chosen in someone's head or by randomly typing on a keyboard are also not truly random).
- Never ever reused, in whole or in part - the same key must never, ever be reused for any other message.
- As large as (or greater than) the length of the message. Since my algorithm converts characters

into two-digit equivalents, the key length requirement would be ((message length) * 2). Hence, our example message "MEET AT DAWN" would need a key of at least 24 digits.

- And, of course: The key must be kept totally secret. (Real-life implementations of OTP algorithms have demonstrated one-time pads printed on super-flammable paper for immediate destruction of the key, or very tiny paper that can be easily consumed or otherwise destroyed if necessary. The only limit is the cleverness of the user.) This requirement is arguably the hardest part of successful OTP implementation, as both the sender and receiver need to be able to have the same key for each message; securely sending the pads is very difficult in real life.

Now that we know how to make our message perfectly secure, let's analyze how unbreakable encryption is possible in the face of a theoretical "perfect" cryptanalysis machine: a cracking computer with infinite computing power. Such a machine could simply brute-force keys, and, with infinite power, it would always find the right key. So how could any encrypted message be truly secure?

Let's encrypt "MEET AT DAWN" again, but we'll use a key that meets our OTP requirements. We need a 24-digit keystream made up of truly random numbers. Whenever I want some high-entropy random numbers, I go to `http://www.random.org`, which generates its random integers using atmospheric noise - a very high-quality source of randomness, to be sure. (For those of you keeping up with the "you don't need a computer" theme, you can get high-quality random numbers from rolling a ten-sided die.) For our example, we'll use this key: {629073451125378063848998}. We complete our zig-zag diffusion method, and then add the key:

```
1 5 2 0 0 3 3 0 7 2 4 2 0
➡0 0 7 0 4 5 2 1 2 1 1
6 2 9 0 7 3 4 5 1 1 2 5 3
➡7 8 0 6 3 8 4 8 9 9 8
-------------------------
➡----------------------
7 7 1 0 7 6 7 5 8 3 6 7 3
➡7 8 7 6 7 3 6 9 1 0 9
```

"MEET AT DAWN" encrypted with our random, 24-digit key gives us our ciphertext, {7710-7675-8367-3787-6736-9109}.

Now let's go back to the controls of our infinite-power cracking machine. Hark, an encrypted message! Let's crack it! We feed our ciphertext {7710-7675-8367-3787-6736-9109} into the cracking machine, and we program it to find *all* plaintexts that form a coherent message. Soon enough, we see our actual plaintext, "MEET AT DAWN" on the list of cracked messages, corresponding to the key {629073451125378063848998}. If you think about it, perfect security doesn't necessarily mean the machine couldn't figure out that the actual plaintext is a possible solution.

Shannon security comes into play when we look at the rest of the list of cracked messages: "MEET AT EVE " (with a space on the end) appears with the key {629071451117378040848987}. That key is very similar to our actual key, but the plaintext has the opposite meaning - which key is the correct one? We also find "MEET IN BACK" with the key {629673451247378066840998}; "DO NOT MEET " with the key {700376333115236460859057}; and even "FAKE MESSAGE" with the key {769569141377327862266099}. With no other information, we have no way of knowing the correct key. OTP's unbreakable nature lies in the sea of keys through which the attacker is forced to swim. This also explains why key security is so vital in successful OTP implementation: It must be truly random (a key with a pattern in it will be easily picked as the most likely valid key); it must never be used again (if our key matches a previous known key, we can safely discard the other solved keys); it must never be revealed to anyone else (obviously, any clues to the correct key reveals our message).

Even though OTP ciphers can achieve unbreakable security in theory, the practical application of such a system has proven to be a challenge. The security requirements of the key are such that, in practice, an OTP ciphertext may only be as secure as, say, a computer encryption method used to hide the keystream, or the physical security of a safe in which the keys are stored. While the OTP system is theoretically unbreakable, the practical application of OTP encryption opens up vulnerabilities. For example, let's suppose I'm sending messages encrypted with my cipher to someone via mail. Both sides of communication have notebooks full of perfectly random numbers. The two notebooks are the only existing record of the numbers. As messages are sent back and forth, numbers are taken from the notebooks in order as needed and used only once. If I keep my notebook in a desk drawer in my house, then I can't claim that my messages are perfectly secure; cracking my messages would only be as difficult as breaking into my house and taking the notepad. That's just one example of many - OTP keys could be compromised at the origin, in transit, and at the destination. Furthermore, the physical security of these random pads is just one factor. Authentication is a challenge that isn't addressed by OTP, and the existence of that countless number of decryption keys means that an adversary could easily calculate a key that would decrypt a ciphertext into any message of the same length. Thus, an adversary doesn't need to know the secret key in order to use your own cryptosystem to launch an attack. There are ways to address this, but it only highlights the relative difficulty of successfully implementing OTP communication.

Even if we could remove the implementation problems associated with the physical security of the key material - e.g., both communicating parties are savants who can perfectly memorize the key material, and hence never have it written down - the threat of rubber-hose cryptanalysis means that an inherent risk would still exist, keeping us from that elusive perfect security in practice. This points to a bigger problem with information security in general: the humans are the weakest link in security, but an information system's need for usability means there will always be a human in the mix. We can't rely on theory alone if we want to secure our information.

Thanks for reading.

MEETINGS

ARGENTINA

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

AUSTRALIA

Melbourne: Level 2 food court, Melbourne Central Dome.

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

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere near the Dunkin Donuts in the glass paned area with tables.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

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

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

ENGLAND

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

Leeds: The Brewery Tap Leeds. 7 pm

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

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

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

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

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

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

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

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

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

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

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

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

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

MEXICO

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

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

NETHERLANDS

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

NORWAY

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

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

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

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

Trujillo: Starbucks, Mall Aventura Plaza. 6 pm

PHILIPPINES

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

SWEDEN

Stockholm: Central Station, second floor, inside the exit to Klarabergsviadukten above main hall.

SWITZERLAND

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

WALES

Ewloe: St. David's Hotel.

UNITED STATES

Alabama

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

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

Arizona

Phoenix: Cartel Coffee Lab. 6 pm

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

Arkansas

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

California

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

Monterey: East Village Coffee Lounge. 5:30 pm

Sacramento: Hacker Lab, 1715 I St.

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

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

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

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

Colorado

Colorado Springs: The Enclave Coop, 2121 Academy Circle. 7 pm

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

Connecticut

Newington: Panera Bread, 3120 Berlin Tpke. 6 pm

District of Columbia

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

Florida

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: Matt's Casbah, 801 E New Haven Ave. 5:30 pm

Orlando: Panera Bread, Fashion Square Mall.

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

Titusville: StoneFire Art Gallery & Studios, 2500 S Washington Ave.

Georgia

Atlanta: Lenox Mall food court. 7 pm

Hawaii

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

Idaho

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

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

Illinois

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

Peoria: Starbucks, 1200 West Main St.

Indiana

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

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

Iowa

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

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

Kansas

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

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Worcester: TESLA space - 97D Webster St.

Michigan

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

Missouri

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

Montana

Helena: Hall beside OX at Lundy Center.

Nebraska

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

Nevada

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

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

New Mexico

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

New York

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

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

Rochester: Interlock Rochester, 1115 E Main St. 7 pm

North Carolina

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

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

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

North Dakota

Fargo: West Acres Mall food court.

Ohio

Cincinnati: Hive13, 2929 Spring Grove Ave. 7 pm

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

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

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

Youngstown: Denny's back room, 4020 Belmont Ave.

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, southeast food court near mini post office.

Pittsburgh: Tazz D'Oro, 1125 North Highland Ave at round table by front window. 7 pm

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 Lane, outside porch near the entrance. 7:30 pm

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

Vermont

Burlington: Quarterstaff Gaming Lounge, 178 Main St, 3rd floor.

Virginia

Arlington: (see District of Columbia)

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

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

Richmond: Hack.RVA 1600 Roseneath Rd. 6 pm

Virginia Beach: Pembroke Mall food court. 6 pm

Washington

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

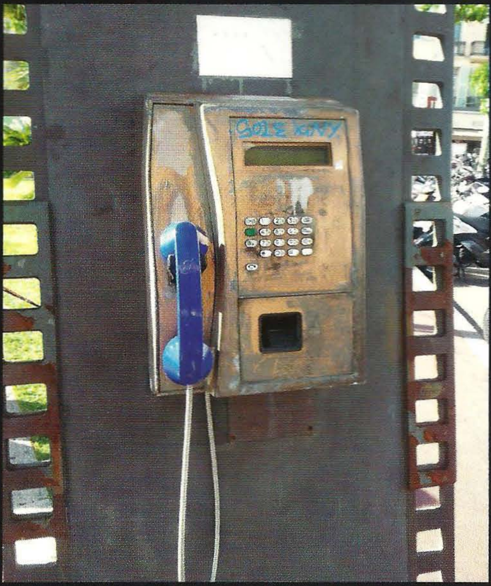
Spokane: The Service Station, 9315 N Nevada (North Spokane).

Wisconsin

Madison: Fair Trade Coffee House, 418 State St.

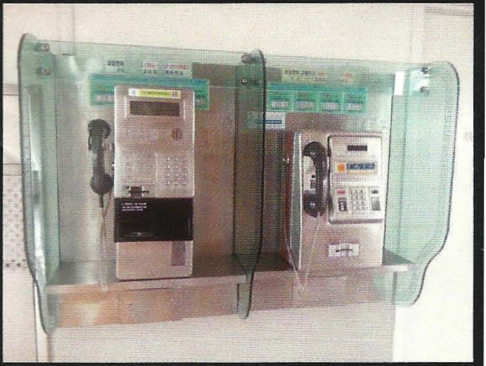
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Payphones of the World



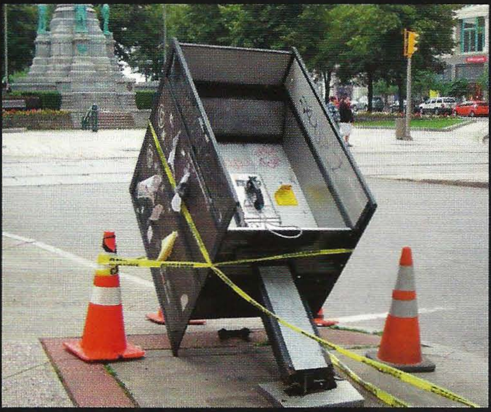
France. Spotted at the Cannes International Film Festival earlier this year. Note the "film" that the phone is mounted on.

Photo by T-RAY



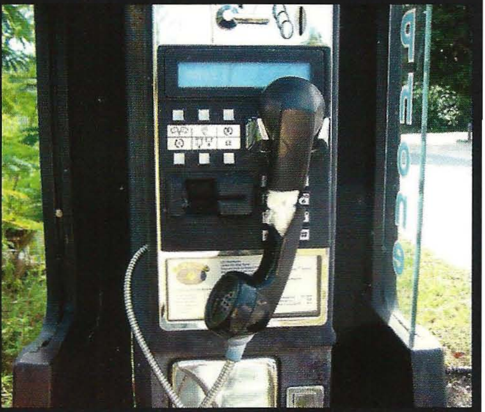
South Korea. Seen in the Gimpo Internartional Airport in Seoul, these are two rather old models, taking all combinations of coins and cards between them.

Photo by bitcoin vendor



United States. Nobody is too surprised at a sight like this in Buffalo, New York. And we wouldn't be at all surprised if these phones were still operational.

Photo by Vince Harzewski



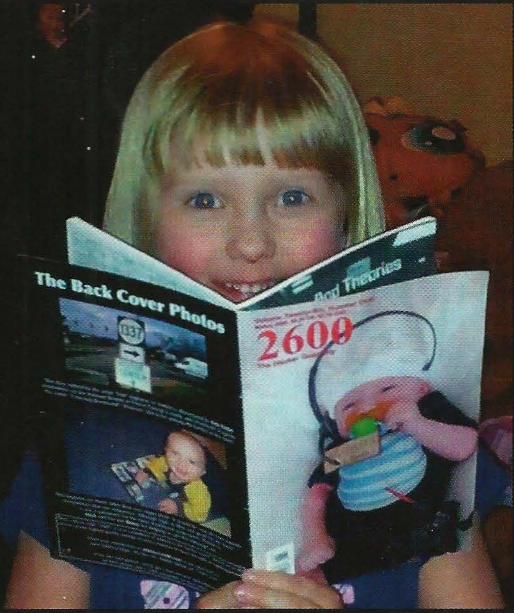
Bahamas. Believe it or not, this phone in Mangrove Cay on Andros Island actually works. But you'd have to have an unusually shaped head to take advantage of it.

Photo by Robin Blanc

CORRECTION: In some editions of our Summer issue on this page, the payphone from the United States was erroneously credited. The photographer was Connor Dunning. We apologize for the error.

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



Occasionally, moments like this just happen and lately we've been getting more and more of them. In this case, Gene (**laserdemon**) noticed his four-year-old daughter parading around the house with one of our issues while counting out loud. This verifies a longstanding theory of ours that we do in fact sometimes act as an educational tool. What's really amazing here is the number of kids in a single photo of our magazine.

And on the other end of the spectrum, we see the symbolic death of a hacker - and the unsymbolic death of someone with the actual last name of "Hacker" as seen by **L. Motz**, who witnessed this at Westview Mausoleum in Atlanta, Georgia. This kind of thing also happens now and then.

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

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

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